Financial Intelligence Units:

An Overview

International Monetary Fund

World Bank

2004

Revised version of July 23, 2004

Editing: Paul Gleason and Glenn Gottselig
Composition: Glenn Gottselig and Sarah Underwood
Cover Design: Martina Vortmeyer

Cataloging-in-Publication Data

Financial intelligence units : an overview -- Washington, D.C. : International Monetary Fund, Legal Dept., Monetary and Financial Systems Dept. : World Bank, Financial Market Integrity Div., 2004.

p. cm.

ISBN 1-58906-349-X
Includes bibliographical references.

1. Money laundering—Prevention. 2. Commercial crimes—Prevention. 3. International Monetary Fund. Legal Dept.
HV8079.M64F35 2004

The term "country," as used in this publication, does not in all cases refer to a territorial entity that is a state as understood by international law and practice; the term also covers some territorial entities that are not states, but for which statistical data are maintained and provided internationally on a separate and independent basis.

Price: $23.00

Please send orders to:
International Monetary Fund Publication Services
700 19th Street, N.W. Washington, D.C. 20431, U.S.A.
Tel.: (202) 623-7430 Telefax: (202) 623-7201
E-mail: publications@imf.org
Internet: *http://www.imf.org*

CONTENTS

Tables

Figures

Boxes

FOREWORD

Recent efforts to develop effective strategies for anti-money laundering and combating the financing of terrorism (AML/CFT) bring together several distinct but related aspects of financial systems and criminal law. Financial intelligence units (FIUs) constitute an important component of these strategies. An FIU is a central national agency responsible for receiving, analyzing, and transmitting disclosures on suspicious transactions to the competent authorities. Combating the crimes of money laundering and financing terrorism is essential to the integrity of financial systems but, if these efforts are to be successful, traditional law-enforcement methods need to be supported by the contribution of the financial system itself, in particular by implementing know-your-customer principles and reporting suspicious transactions to an FIU. Financial institutions hold critical information on transactions that may hide criminal schemes. Although this information is covered by necessary confidentiality regimes, it has to be made accessible to law-enforcement agencies to enable them to trace criminal money channels.

FIUs have now been in existence for over ten years, and more than 90 have been admitted into the Egmont Group, the informal international association of FIUs. Many more countries are planning to establish an FIU; and in many countries, the authorities are endeavoring to improve the effectiveness of existing ones. Yet, up to now, no overall presentation of FIUs was available to help these authorities in their efforts. As a result, considerable time and effort was needed to find relevant information about FIUs and their operations. It is this gap that the present handbook attempts to fill.

The handbook covers a wide array of topics relating to FIUs, beginning with the key steps necessary for establishing them and the various forms they can be given in a government structure. The core functions of FIUs (receiving reports of suspicious transactions, analyzing them, and disseminating the resulting intelligence) are analyzed in detail, with examples taken from a number of different countries. Some of the most important additional functions assigned to certain FIUs, such as monitoring compliance of the reporting institutions with AML/CFT requirements, are also discussed. Finally, international assessments of FIUs, done in the context of assessments of overall AML/CFT frameworks, are described.

Rather than providing definitive statements on what an FIU should be, the handbook strives to bring to the reader as many examples as possible of existing FIU settings and arrangements, in order to provide policymakers and legislators with the widest palette of country experiences worldwide and help them design financial intelligence units that best serve the purposes of their own jurisdictions.

François Gianviti
The General Counsel
IMF

Stefan Ingves
Director
Monetary and Financial Systems Department
IMF

Cesare Calari
Vice President
Financial Sector
World Bank

ACKNOWLEDGMENTS

The handbook is a joint effort of the International Monetary Fund's Legal Department and Monetary and Financial Systems Department as well as the World Bank's Financial Market Integrity Division. It was written and edited by Louis Forget with the assistance of Vida Šeme Hočevar, both of the IMF Legal Department, under the direction of Jean-François Thony, Assistant General Counsel. Contributions and comments were received from Maud Bökkerink and Ernesto Lopez, IMF Monetary and Financial Systems Department; Eric Robert, Nadim Kyriakos-Saad, Cheong-Ann Png, Peter Csonka, and Ross Delston, IMF Legal Department; and Alain Damais and Bess Michael, World Bank. The support and encouragement of the members of the Egmont Group Committee is gratefully acknowledged and, in particular, the useful comments of William Baity, Chair of the Egmont Committee and Deputy Director, FinCEN; John Brewer, FinCEN; and Boudewijn Verhelst, Deputy Director of CTIF-CFI (the Belgian FIU).

1

INTRODUCTION

Since the mid-1980s, the need for a modern anti-money-laundering strategy has become widely accepted internationally. The negotiations of the 1988 United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances can be seen as the starting point of this trend. Depriving criminal elements of the proceeds of their crimes has increasingly been seen as an important tool to combat drug trafficking and, more recently, all serious crimes. Progress in this area is becoming a critical element in fighting organized crime, corruption, and the financing of terrorism, and maintaining the integrity of financial markets.

As countries developed their anti-money-laundering strategies and found that law-enforcement agencies had limited access to relevant financial information, it became clear that the strategy required them to "engage the financial system in the effort to combat laundering while, at the same time, seeking to ensure the retention of the conditions necessary for its efficient operation."[1] Countries also found that implementation of a system requiring disclosures of suspicious transactions on the part of financial institutions created the need for a central office or agency for assessing and processing these disclosures.[2]

The first few financial intelligence units (FIUs) were established in the early 1990s in response to the need for a central agency to receive, analyze, and disseminate financial information to combat money laundering. Over the following ten years, the number of FIUs increased to the point where the Egmont Group, the informal international association of FIUs, had 94 members in 2004. In 2003, the Financial Action Task Force (FATF) adopted a revised set of recommendations on combating money laundering that, for the first time, included explicit recommendations on the establishment and functioning of FIUs.[3] In recent years, recognizing the importance of an FIU in the anti-money laundering/combating the financing of terrorism (AML/CFT) framework, the International Monetary Fund and the World Bank, as well as a number of their

---

[1] William C. Gilmore, 1999, *Dirty Money: The Evolution Of Money-Laundering Counter-Measures*, 2nd ed. (Strasbourg: Council of Europe Press), page 103.

[2] Egmont Group, 1995, *The First International Meeting of Organizations Devoted to Anti-Money Laundering* (Brussels), page 1.

[3] FIUs have been included in the methodology used to assess AML/CFT frameworks since 2001.

member countries, have provided technical assistance to countries in the establishment and strengthening of FIUs.

Although the FIU members of the Egmont Group share the same core functions of receiving, analyzing, and disseminating financial information to combat money laundering and financing of terrorism,[4] they differ in many ways. Authorities intending to establish an FIU or improve an existing FIU's effectiveness face a number of choices concerning how the FIU is to be established and function. Similarly, providers of technical assistance regarding FIUs need access to a wide array of information as to the various aspects of FIUs. Thus, it is opportune to provide FIU officials, country authorities, and providers of technical assistance with an overview of the range of experience countries and FIUs have had up to now.

Moreover, FIUs currently face a series of unique challenges. The scope of their responsibilities is being widened to include dealing with the financing of terrorism, in addition to money laundering and the related predicate offenses. Financial information related to the financing of terrorism is, in many ways, different from financial information regarding other crimes, thus raising issues of methods of information analysis and of training for FIU staff. The range of reporting entities is also being widened to include nonfinancial professions, such as casinos, company service providers, and legal and accounting professionals. As a result, the nature of reports received has become more varied, and here again, issues of methods of analysis and staff training arise.

The purpose of this handbook is to respond to the need for information on FIUs. The information provided includes references to the relevant FATF standards wherever appropriate. It should be emphasized, however, that this handbook is neither an assessment tool nor a synthesis of the assessments of FIUs completed so far. The handbook does not contain a systematic exposition of the standards used in the assessment of AML/CFT frameworks as they relate to FIUs. Authorities wishing to ensure that the arrangements they put in place to combat money laundering and the financing of terrorism, including their FIU, meet international standards should refer to the FATF 40 Recommendations and the Methodology adopted by the FATF and the other bodies that perform AML/CFT assessments. Technical assistance on establishing and strengthening FIUs is available from the International Monetary Fund, the World Bank, and other sources.

Throughout the handbook, reference will be made to the Egmont Group of FIUs. The Egmont Group was established in 1995 "to encourage and

---

[4] Egmont Group, June 2004, *Statement of Purpose of the Egmont Group of Financial Intelligence Units* (Guernsey).

assist in the exchange of financial intelligence between countries."[5] More specifically, it is "an informal organization to provide a forum for FIUs to improve support to their respective national anti-money-laundering programs." "This support includes expanding and systematizing the exchange of financial intelligence information, improving expertise and capabilities of personnel of such organizations, and fostering better communications among FIUs through application of technology."[6] (See Box 6 for more details.)

The text is organized as follows. Chapter 2 discusses the issues involved in establishing an FIU, including a description of the types of FIUs. Chapter 3 discusses the core functions of an FIU: receiving suspicious transaction reports and other reports, analyzing them, and disseminating financial intelligence to the appropriate authorities. In Chapter 4, other functions exercised by some FIUs are discussed. Chapter 5 discusses the enhancement of the effectiveness of FIUs. Chapter 6 discusses the process of international assessment of FIUs. In Chapter 7, some conclusions are offered.

---

[5] Egmont Group, 2003, audiovisual presentation.

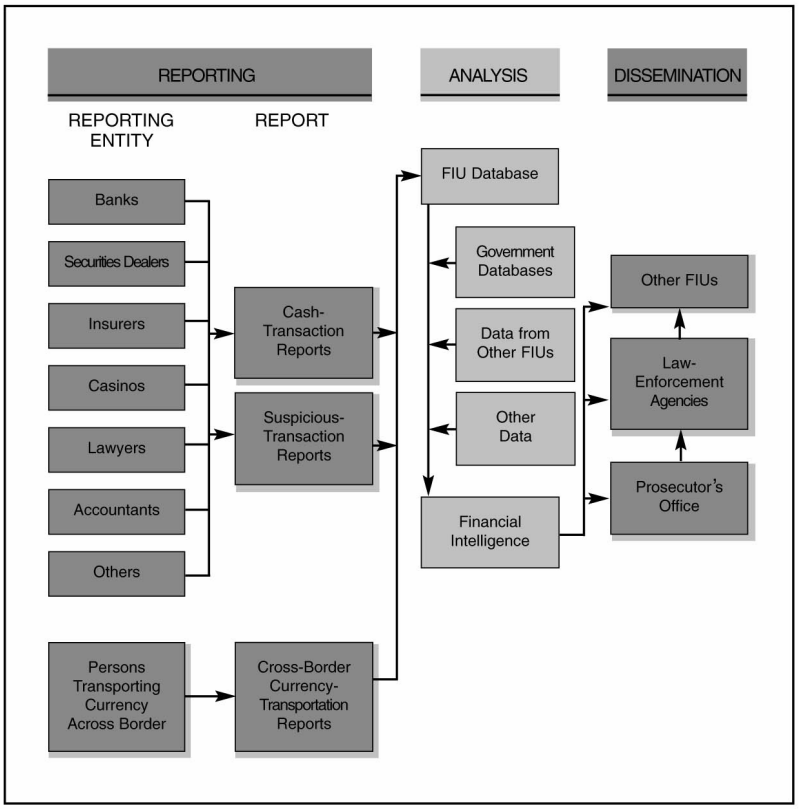
[6] Egmont Group, (undated), *Information Paper on Financial Intelligence Units and the Egmont Group*, page 3.

2

ESTABLISHING AN FIU

In their simplest form, FIUs are agencies that receive reports of suspicious transactions from financial institutions and other persons and entities, analyze them, and disseminate the resulting intelligence to local law-enforcement agencies and foreign FIUs to combat money laundering (see Figure 1).

Figure 1. Typical FIU Information Flow



Source: Adapted from FINTRAC (Canada) *2001 Annual Report*, Appendix III.

Establishing an FIU is an important step in combating financial crime. As such, it should be based on criminal policy considerations specific to each country, and the basic features of the FIU should be consistent with the super-

visory framework of the country, as well as with its legal and administrative systems and its financial and technical capabilities. The process of establishing an FIU is discussed in the next section. The establishment of an FIU also responds to international norms and standards, and these are discussed in the section on "International Considerations." As a government agency, the FIU must be given the degree of autonomy necessary to fulfill its responsibilities while being accountable for the results it achieves. This is discussed in the section on "Institutional Autonomy and Accountability." Organization and staffing issues are discussed in the following section.

Steps in Establishing an FIU

The establishment of an FIU signals the determination of country authorities to heighten the priority they accord to combating financial and other crimes in the country, and to cooperating with other countries in this regard. An effective FIU can make a significant contribution to combating these crimes nationally and internationally.

Although, in establishing an FIU, authorities may feel the need to respond to the calls of the international community, their decisions as to the FIU's functions and the modalities of its operations need to be based on the country's own crime-fighting policy objectives, resources, and priorities. The responsibilities of the FIU also need to be harmonized with those of existing national agencies involved in the fight against financial crime, including law-enforcement and supervisory agencies and policy-setting government bodies.

Moreover, the establishment of an FIU will entail the use of budgetary resources. As a matter of good public administration, the objectives pursued by the establishment of the FIU need to be defined; and the FIU must be given the means to successfully pursue these objectives, for which it will become accountable. Care should be taken not to give the FIU more responsibilities than it can cope with, given its expected resources. In some cases, other agencies that have resources and experience may be in a position to exercise certain functions, such as the supervision of AML/CFT requirements, in a more effective way that an FIU. Overlapping functions should be avoided to the extent possible, and to the extent such overlap is unavoidable, coordination mechanisms should be established to minimize conflicts and maximize cooperation between the concerned agencies.

It follows that the establishment of an FIU and the determination of its functions and resources should be based on an analysis of the country's situation with respect to money laundering, the financing of terrorism, and serious crime in general. In this connection, it is useful to note that one of the critical functions of an FIU is the exchange of information with other FIUs. In addition to the contribution the FIU can be expected to make in combating

domestic crime, it will also be called upon to respond to requests for intelligence from other FIUs.

Also to be considered are the general features of the country's legal system, and the existing strengths and weaknesses of the government agencies where the FIU could be located. As will be seen in the next section, some arrangements with regard to the placement of the FIU in the government structure are tailored to the particular features of the legal and administrative systems of a country. Similarly, relative strengths and weaknesses of the agencies where the FIU may potentially be located need to be assessed, since it may not be prudent to establish an FIU within an administration that does not enjoy the trust of those under its authority. The challenges countries face in establishing FIUs are often considerable. In the small developing island economies, these challenges can become daunting. (See Box 8.)

Key Decisions

Political support is necessary to ensure the success of the FIU. Such support is needed not only to secure the adoption of the law establishing the FIU but also, on a continuing basis, to ensure that the FIU receives sufficient budgetary resources to achieve its objectives.

The analysis of the issues that a country faces in terms of financial crime and the role the FIU will play in meeting the country's criminal policy objectives will make it possible to sketch the FIU's broad outlines, status, and functions. Among the key elements of this outline are the following:

- The basic objectives to be pursued by the FIU;
- the authority and functions necessary to achieve its objectives;
- any functions the FIU will be required to exercise in addition to the core functions (such as, for example, the supervision of reporting entities' compliance with reporting or other obligations, and the freezing of transactions);
- the means to ensure the operational autonomy and the accountability of the FIU;
- the basic transaction reporting requirements: who reports and what is reported (for example, suspicious transactions, cash transactions, cross-border movements of cash);
- the general size of the FIU (after a start-up period) in terms of budget or staff, in relation to the expected flow of information to and from the FIU and any additional responsibilities assigned to the FIU;
- the role of the FIU in relation to other national agencies and government bodies and to other FIUs, including the exchange of information; and
- the location of the FIU in the administration, its autonomy and accountability, and the means to make it operational.

After these key issues have been decided, an executive team may be formed to start the process of establishing the FIU. At this stage, drafting of the law may be initiated, incorporating the decisions on the above topics.

Consultations with Private Sector

In many countries, it has been found productive to discuss the proposed FIU and the draft law with the representatives of the segments of the private sector that will be most directly affected by the establishment of the new AML/CFT regime. Most of the information to be provided to the FIU will come from the private sector, and most of the latter will come from the financial sector. Consulting the representatives of the most directly concerned sectors before the draft legislation is presented to parliament can have a number of advantages.

First, consulting the private sector offers the government an opportunity to build confidence in the proposed agency on the part of the institutions that will be required to send suspicious transaction and other reports to it. Second, such consultations should facilitate understanding of the new obligations to be imposed on the financial and other sectors, and thus facilitate discussion in parliament. Third, for the FIU, the consultations may help the planners, and later the FIU itself, in developing requirements for reporting transactions that can realistically be expected to be followed by the reporting entities. And fourth, for the reporting entities, the advance consultations will serve to make the concerned institutions aware of their future obligations and the related need to develop the necessary programs to fulfill their obligations.

Early consultations with the private sector will also provide an opportunity for the authorities to highlight the benefits of the new system to financial and other institutions that will have to begin reporting transactions to the FIU. The adoption of an AML/CFT framework can reduce the risks of the sector being negatively affected by instances of fraud, money laundering, and other financial crimes perpetrated through their institutions. The fact that the framework would be based on international standards reflecting worldwide practice that would protect the financial and economic environment of the country can also be highlighted.

Financing an FIU

To be able to achieve its objectives, an FIU needs resources commensurate with its size and the amount of data it is expected to receive, process, and disseminate.[7] This, in turn, is a function of the size and variety of financial and

[7] The 2003 FATF Recommendations set the following standard: "Countries should provide their competent authorities involved in combating money laundering and terrorist financing with *(continued)*

nonfinancial entities that will provide reports to the FIU, and the scope of the reporting obligation. Other responsibilities that may be assigned to the FIU also need to be taken into account in determining its resource needs. The location of the FIU in a ministry or government agency may reduce some of its operational costs somewhat (for example, if personnel management and building maintenance costs are either absorbed centrally or shared with others parts of the same ministry or agency). Some costs specific to the FIU, however, such as those for specially trained staff or high-level computing facilities, may be substantial and should be factored into the preparation of the FIU budget.

Most FIUs are financed directly from the state budget. For example, most administrative-type FIUs[8] that are part of a ministry of finance have their own budget within the budget of that ministry (for example, Korea's KoFIU, Monaco's SICCFIN, Slovenia's OMLP, and the United States' FinCEN). Law-enforcement-type FIUs are usually financed by the police, the ministry of interior, or the prosecution service (for example, Estonia's RA, Jersey's FCU, and Hungary's ORFK).[9] (See Appendix III for definitions of abbreviations of the names of countries' FIUs.)

Some FIUs are cofinanced by different state authorities or ministries. For example, the MOT in the Netherlands and the MOT in the Netherlands Antilles receive their financing under an arrangement between the Netherlands' Ministry of Finance and the Ministry of Justice. A small number of FIUs are partly or wholly financed by the central bank or the financial sector supervisory agency of the country (for example, Bolivia's UIF, Italy's UIC, Spain's SEPBLAC, and Venezuela's UNIF). Some FIUs are placed directly under the government, outside the budget of any other agency, and are financed as a separate budgetary unit (for example, Colombia's UIAF, Panama's UAF, and Romania's ONPCSB).

In all countries, the reporting institutions and professionals must absorb their own costs of implementing the AML/CFT laws, including the costs of setting up systems for detecting and reporting suspicious and other transactions. In countries where the FIU's budget comes from the financial sector supervisory agency, the FIU may be indirectly financed by the contributions, levies, and fines imposed on the supervised institutions. In Belgium, the re-

---

adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of those authorities are of high integrity" (Recommendation 30).

[8] See the next section for a discussion of the various types of FIUs.

[9] In Bulgaria, 25 percent of the annual amount of fines levied under the AML law reverts to the FIU to be used to fund salaries, and 30 percent reverts to the FIU to be used for "capital investments for improvement of the equipment, training and participation in international events" (Law on Measures Against Money Laundering, article 17a, paragraphs (2) and (3)) [Bulgaria].

porting institutions contribute directly to the financing of the FIU's operations. The Belgian FIU's operational expenses are paid without any contribution from the federal budget.[10] The budget ceiling is set annually by agreement between Belgium's Ministers of Finance and Justice.[11] The bulk of the contributions is provided by credit institutions, insurance companies, and stock market brokers and dealers, while the central bank, the postal service, and other reporting entities and professionals pay a small portion.[12] The main advantage of this arrangement is that the FIU is shielded from the political vagaries of budget making, which contributes to the FIU's independence. It is noteworthy, however, that no other country has adopted this approach. It may be that the idea of financing the operations of a public agency with funds levied directly from the private sector entities subject to its jurisdiction does not fit well in the public finance framework of most countries or that this arrangement does not necessarily guarantee that the FIU will receive a sufficient amount of resources over time.

Types of FIUs

Over the years, countries have established FIUs for the general purpose of combating money laundering and have generally given them the three core functions that are part of the accepted definition of an FIU. The administrative arrangements by which these functions are carried out, however, vary considerably from country to country. These variations arise from different country circumstances, together with the lack of an internationally accepted model for the functions of an FIU in the early 1990s, when the first such units were established. For example, in some countries, the function of the FIU as an additional tool for law-enforcement organizations in combating money laundering and associated crimes was emphasized, and this led to the establishment of the FIU in an investigative or prosecutorial agency. Other countries emphasized the need for a "buffer" between the financial institutions and the police, and consequently their FIUs were established outside these agencies.

---

[10] Law of January 11, 1993 on Preventing Use of the Financial System for Purposes of Laundering Money, Article 11, paragraph 7, and Royal Decree of June 11, 1993 on the Composition, Organization, Operation and Independence of the Financial Intelligence Unit, amended by Royal Decrees of May 30, 1994; February 23, 1995; and February 4, 1999, Chapter X [Belgium].

[11] Royal Decree of June 11, 1993 on the Composition, Organization, Operation and Independence of the Financial Intelligence Unit, amended by Royal Decrees of May 30, 1994, February 23, 1995, and February 4, 1999, Article 12, paragraph 1 [Belgium].

[12] For the fiscal year ending December 31, 2003, out of an operational budget of about €2,360,000, contributions from credit institutions, insurance companies, and stock market brokers and dealers represented about 72 percent of the total, while the other reporting entities and professionals, together with the central bank and the postal service, contributed about 27 percent (see C.T.I.F., *10e Rapport d'Activités, 2002–2003*, page 150).

The wide variety of arrangements for FIUs may be summarized under four general headings: the administrative-type FIU, the law-enforcement-type FIU, the judicial- or prosecutorial-type FIU, and the "mixed" or "hybrid" FIU.[13] It should be emphasized, however, that such classification is, to a certain degree, arbitrary and that other ways of classifying FIUs are possible. Nevertheless, these categories illustrate the wide variety of administrative arrangements under which FIUs are established. While these are not exhaustive lists, advantages and disadvantages of each type of FIU are summarized in Boxes 1, 3, and 5, respectively; and, by way of examples, the main features of an administrative-type FIU (the OMLP of Slovenia) and a law-enforcement-type FIU (the National Criminal Intelligence Service (NCIS) of the United Kingdom), are set out in Boxes 2 and 4, respectively.

Administrative-type FIUs

Administrative-type FIUs are usually part of the structure, or under the supervision of, an administration or an agency other than the law-enforcement or judicial authorities. They sometimes constitute a separate agency, placed under the substantive supervision of a ministry or administration ("autonomous" FIUs) or not placed under such supervision ("independent" FIUs). The main rationale for such an arrangement is to establish a "buffer" between the financial sector (and, more generally, entities and professionals subject to reporting obligations) and the law-enforcement authorities in charge of financial crime investigations and prosecutions. Often, financial institutions facing a problematic transaction or relationship do not have hard evidence of the fact that such a transaction involves criminal activity or that the customer involved is part of a criminal operation or organization. They will therefore be reluctant to disclose it directly to a law-enforcement agency, out of a concern that their suspicion may become an accusation that could be based on a wrong interpretation of facts. The role of the FIU is then to substantiate the suspicion and send the case to the authorities in charge of criminal investigations and prosecutions only if the suspicion is substantiated.

The actual administrative location of such FIUs varies: the most frequent arrangements are to establish the FIU in the ministry of finance, the central bank, or a regulatory agency. A few have been established as separate structures, independent of any ministry (CTIF/CFI in Belgium, for example). In most cases, the decision to establish the FIU outside the law-enforcement

---

[13] On the "typology" of FIUs, see generally J.F. Thony, 1996, "Processing Financial Information in Money Laundering Matters, The Financial Intelligence Units," *European Journal of Crime, Criminal Law and Criminal Justice, Brussels*, pp. 257–82; B. Verhelst, 2002, *The Financial Intelligence Units in the International Context*, paper available from the Egmont Group; and P.A. Schott, 2003, *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* (Washington: World Bank and International Monetary Fund), Ch. VII.

system also leads to the decision that the FIU's powers will be limited to the receipt, analysis, and dissemination of suspicious transaction and other reports, and that they will not be given investigative or prosecutorial powers. Similarly, the powers of the FIU to disclose the information contained in transaction reports is usually defined narrowly, to preserve the confidential character of the information provided to it.[14] Administrative-type FIUs may or may not be responsible for issuing AML/CFT regulations or for supervising compliance with AML/CFT laws and regulations on the part of reporting institutions.

Box 1. Administrative-Type FIUs

Advantages

- The FIU acts as an interface between the financial and other sectors subject to the reporting obligation, on the one hand, and law-enforcement authorities on the other hand, thus avoiding the creation of direct institutional links between these institutions and law-enforcement agencies while bringing disclosures to the attention of law-enforcement agencies.
- Financial institutions are more confident about disclosing information if they know that dissemination will be limited to cases of money laundering and financing of terrorism and will be based on the FIU's own analysis rather than the reporting institution's limited information.
- The FIU is a "neutral," technical, and specialized interlocutor for the reporting parties.
- If the FIU is placed in a regulatory agency, it is the natural interlocutor of the financial institutions.
- Information can be easily exchanged with all types of FIUs.

Disadvantages

- Because the FIU is not part of the law-enforcement administration, there may be a delay in applying law-enforcement measures, such as freezing a suspicious transaction or arresting a suspect, on the basis of financial disclosures.
- The FIU usually does not have the range of legal powers that law-enforcement agencies and judicial authorities have to obtain evidence.
- The administrative-type FIUs (unless they are truly independent) are more subject to the direct supervision of political authorities.

Examples of countries with administrative-type FIUs include Andorra, Aruba, Australia, Belgium, Bolivia, Bulgaria, Canada, Colombia, Croatia, the Czech Republic, France, Israel, the Republic of Korea, Liechtenstein, Malta, Monaco, the Netherlands, the Netherlands Antilles, Panama, Poland, Romania, Russia, Slovenia, Spain, Ukraine, the United States, and Venezuela.

[14] These FIUs are sometimes referred to as "closed-box" FIUs.

By making an administrative authority a "buffer" between the financial institutions and law-enforcement sectors, authorities can more easily enlist the cooperation of reporting institutions, which are often conscious of the drawbacks vis-à-vis their clients of having direct institutionalized links with law-enforcement agencies. Administrative-type FIUs are often preferred by the banking sector. They may also appeal to other institutions and professionals that have been added to the list of reporting entities for the same reasons.

Box 2. Example of an Administrative-Type FIU: Slovenia's Office for Money Laundering Prevention (OMLP)

Structure

- fully integrated as an office of the ministry of finance;
- director appointed by the government;
- reports to the minister of finance and the government; and
- structured in six services and the management: service for prevention and supervision (three employees), section for suspicious transactions (four employees and one administrative assistant), Analysis Service (one employee), Information Technology Service (two employees), International Cooperation Service (one employee), management (two employees), and main office (one employee and one administrative assistant).

Budget for 2003

Approximately $670,000—more than 80 percent of which is used for personnel charges.

Staff

The director, two administrative staff (one with an undergraduate degree, one with a graduate degree), and 14 professionals with at least a bachelor's degree in law, computer science, or economy.

Functions and Powers

Policy functions

- represented on the national governmental committee responsible for countering the financing of terrorism, the national security council, and various working groups (for example, on the amendments of the Criminal Procedure Code and the Penal Code, corruption, economic crime, national strategy for combating crime); and
- proposes to the competent bodies changes and amendments to the regulations concerning the prevention and detection of money laundering.

Operational functions

- centralizes and analyzes mandatory reports:

  - reports on cash transactions (CTs) above approximately $25,000 (31,217 reports received in 2003);
  - reports from customs authorities on transfers of cash or securities above $25,000 (2,423 reports revised in 2003); and
  - reports on suspicious transactions (79 reports received in 2003: 72 from reporting institutions, the rest from other FIUs and other state authorities);
- analyzes and disseminates reports (with documentation) on money laundering to competent authorities (police and Prosecution Service);
- disseminates information (without documentation) to the competent authorities when there are reasons to suspect that a serious criminal offense (for which the law prescribes a prison sentence of five or more years) or a corruption criminal offense was committed.
- trains employees of reporting institutions;
- keeps a centralized database of all information related to money laundering in the Republic of Slovenia;
- participates in the preparation of indicators for the recognition of suspicious transactions;
- trains law-enforcement officials and supervisors; and
- publishes statistical data on money laundering and informs the public about money-laundering issues.

Other legal powers

- freezes transaction (for up to 72 hours);
- gives obligatory instructions (when conditions for freezing exist);
- requests that reporting entities provide additional or new information when there is suspicion of money laundering;
- asks or directly obtain any other data on legal or individual persons or transactions from state authorities or institutions with public authorization; and
- serves as the appointed Central Authority under Council of Europe Convention No. 141 on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime.

Website: *http://www.sigov.si/mf/angl/uppd*

Law-enforcement-type FIUs

In some countries, the emphasis on the law-enforcement aspects of the FIU led to the creation of the FIU as part of a law-enforcement agency, since this was the easiest way to establish a body with appropriate law-enforcement powers without having to design from scratch a new entity and a new legal and administrative framework.

Operationally, under this arrangement, the FIU will be close to other law-enforcement units, such as a financial crimes unit, and will benefit from their expertise and sources of information. In return, information received by

the FIU can be accessed more easily by law-enforcement agencies and can be used in any investigation, thus increasing its usefulness. Exchange of information may also be expedited through the use of existing national and international criminal information exchange networks.

Box 3. Law-Enforcement-Type FIUs

Advantages

- built on an existing infrastructure, so there is no need to set up a new agency;
- maximum law-enforcement use can be made of financial disclosure information;
- quicker law-enforcement reaction to indications of money laundering and other serious crimes;
- information can be exchanged using the extensive network of international criminal information exchange networks (such as Interpol); and
- easy access to criminal intelligence and to the intelligence community at large.

Disadvantages

- tends to be more focused on investigations than on prevention measures;
- law-enforcement agencies are not a natural interlocutor for financial institutions; mutual trust must be established, which may take some time, and law-enforcement agencies may lack the financial expertise required to carry out such a dialogue;
- the FIU usually does not receive data on currency transactions above a fixed amount;
- gaining access to the financial organizations' data (other than the reported transactions) usually requires the launching of a formal investigation;
- reporting institutions may be reluctant to disclose information to law enforcement if they know it could be used in the investigation of any crime (not just money laundering and the financing of terrorism); and
- reporting institutions may be reluctant to disclose information to law enforcement on transactions that are no more than "suspicious."

Examples include Austria, Estonia, Germany, Guernsey, Hungary, Iceland, Ireland, Jersey, Slovakia, Sweden, and the United Kingdom.

Also, a law-enforcement-type FIU will normally have the law-enforcement powers of the law-enforcement agency itself (without specific legislative authority being required), including the power to freeze transactions and seize assets (with the same degree of judicial supervision as applies to other law-enforcement powers in the country). This is likely to facilitate the timely exercise of law-enforcement powers when this is needed.

Box 4. Example of a Law-Enforcement-Type FIU: United Kingdom's National Criminal Intelligence Service (NCIS)

Structure

- The NCIS is a nondepartmental public body operating under the NCIS Service Authority;
- the NCIS Service Authority reports to the Home Secretary;
- the head of the NCIS is appointed by the NCIS Service Authority and reports to it;
- within the NCIS, the FIU functions are discharged by the Financial Intelligence Division; and
- the Financial Intelligence Division has three components: the Data Management Center, the Liaison Unit, and the Intelligence Development Unit.

Budget and Staff (2004, Financial Intelligence Division only)

Approximately £4 million, more than 88 percent of which is used for personnel charges (staff: 120).

Functions and Powers

Operational functions

- centralizes and analyzes disclosures of suspicious activity (approximately 100,000 disclosures were received in 2003, 95 percent of which were from reporting institutions, with the rest from national financial investigation and intelligence units and foreign FIUs);
- provides consent to carry out reported suspicious transactions under the Proceeds of Crime Act 2002 (may withhold consent for up to seven days);
- analyzes and disseminates reports and witness statements (with documentation) on money laundering in prosecutions and on request;
- keeps a centralized database on money laundering in the United Kingdom;
- participates in the preparation of indicators for the recognition of suspicious transactions;
- trains other law-enforcement officials and supervisors; and
- publishes statistical data on money laundering and informs the public about money laundering and other threats.

Other legal powers

- request additional or new information from reporting entities when there is suspicion of money laundering; and
- request or directly obtain any other data on legal or individual persons or transactions from state authorities or institutions with public authorization.

Website: *http://www.sigov.si/mf/angl/uppd*

Judicial or prosecutorial-type FIUs

This type of FIU is established within the judicial branch of the state and most frequently under the prosecutor's jurisdiction. Instances of such an arrangement are found in countries with a continental law tradition, where the public prosecutors are part of the judicial system and have authority over the investigatory bodies, allowing the former to direct and supervise criminal investigations.

Disclosures of suspicious financial activity are usually received by the prosecutor's office, which may open an investigation if suspicion is confirmed by the first inquiries carried out under its supervision. The judiciary's powers (e.g., seizing funds, freezing accounts, conducting interrogations, detaining suspects, and conducting searches) can then be brought into play without delay. Judicial and prosecutorial FIUs can work well in countries where banking secrecy laws are so strong that a direct link with the judicial or prosecutorial authorities is needed to ensure the cooperation of financial institutions. It may be noted that the choice of the prosecutor's office as the location of an FIU does not exclude the possibility of establishing a police service with special responsibility for financial investigations. Also, in many countries, the independence of the judiciary inspires confidence in financial circles.

The principal advantage of this type of arrangement is that disclosed information is passed from the financial sector directly to an agency located in the judiciary for analysis and processing.

Box 5. Judicial or Prosecutorial-Type FIUs

Advantages

- usually have a higher degree of independence from political interference;
- disclosure information is brought directly to the agency authorized to investigate or prosecute; and
- allows the judiciary's powers (e.g., seizing funds, freezing accounts, conducting interrogations, detaining people, conducting searches) to immediately be brought into play.

Disadvantages

- generally has the same disadvantages as are listed in the first five bullets of Box 3 on law-enforcement-type FIUs; and
- may have difficulty exchanging information with nonjudicial or prosecutorial FIUs.

Examples are Cyprus and Luxembourg.

"Hybrid" FIUs

This last category encompasses FIUs that contain different combinations of the arrangements described previously. This hybrid type of arrangement is an attempt to obtain the advantages of all the elements put together. Some FIUs combine the features of administrative-type and law-enforcement-type FIUs, while others combine the powers of the customs office with those of the police. For some countries, this is the result of joining two agencies that had been involved in combating money laundering into one. It may be noted that in some FIUs listed as administrative-type, staff from various regulatory and law-enforcement agencies work in the FIU while continuing to exercise the powers of their agency of origin. Among the countries that have established "hybrid" FIUs are Denmark, Jersey, Guernsey, and Norway.

International Considerations

Although the international community quickly developed standards on combating money laundering in general, mostly through the work started by the FATF in 1989, formal recognition of the FIU as a crucial element in anti-money-laundering strategy is more recent. In the 1990 FATF Recommendations, mention was made of the need for financial institutions to report suspicious transactions to "the competent authorities," but these "competent authorities" were not defined, and could be any government agency designated for the purpose. It is only with the issuance of the 2003 Recommendations that the FATF Recommendations recognized the need for an FIU in the sense defined by the Egmont Group.

The FATF Recommendations

The 1990 FATF Recommendations mentioned "competent authorities" for receiving and processing suspicious transaction reports.[15] The recommendations touched upon the main roles of "competent authorities" and alluded to some of the functions and attributes that could be vested in such authorities (without requiring that FIUs have all of them): receiving suspicious or currency transactions above a certain limit; giving instructions to financial institutions; having a computerized database, compliance control and supervision powers, and regulatory powers; issuing guidelines; and carrying out international information exchange. Some of the rules governing suspicious transaction reports were also set out in the recommendations, such as the immunity enjoyed by those who make reports to the FIU in good faith and the rule

[15] Recommendations 16, 18, 24, 26, 27, 28, and 32 mention "competent authorities" in this context.

against "tipping off."[16] At about this same time, the first national FIUs were being established. The 1996 FATF Recommendations did not introduce major changes in the manner in which the recommendations referred to "central authorities" in the context of reporting suspicious transactions.[17]

Box 6. Egmont Group of Financial Intelligence Units

In 1995, a group of FIUs meeting at the Egmont Arenberg Palace in Brussels decided, in view of the benefits inherent in the development of a FIU network, to establish an informal group for the stimulation of international cooperation. Now known as the Egmont Group, these FIUs meet regularly to find ways to cooperate, especially with regard to information exchange, training, and the sharing of expertise.

Countries must go through a formal procedure established by the Egmont Group in order to be recognized as meeting the Egmont definition of an FIU. The Egmont Group as a whole meets once a year. Since the Egmont Group is not a formal organization, it has no permanent secretariat. Administrative functions are shared on a rotating basis. Aside from the Egmont support position, working groups and the newly established Egmont Committee are used to conduct common business.

FIUs, at a minimum, receive, analyze, and disclose information on suspicious or unusual financial transactions provided by financial institutions to competent authorities. Although every FIU operates under different guidelines, most FIUs, under certain provisions, can exchange information with foreign counterpart FIUs. In addition, many FIUs can provide other government administrative data and public record information to their counterparts, which can also be very helpful to investigators. One of the main goals of the Egmont Group is to create a global network by promoting international cooperation among FIUs.

The ongoing development and establishment of FIUs exemplify how countries around the world continue to intensify their efforts to focus on research, analysis, and information exchange in order to combat money laundering, terrorist financing, and other financial crimes.

Source: Adapted from "The Egmont Group Financial Intelligence Units (FIUs)," at *http://www.egmontgroup.org/about_egmont.pdf.*

The FATF Special Recommendations on Terrorist Financing, adopted in October 2001, broadened the scope of the reporting obligation to include transactions suspected of being related to terrorist financing.[18] The issuance of

[16] Recommendations 16 and 17 (1990).
[17] Recommendations 15, 18, 23, 26, 27, 29, and 32 dealt with "competent authorities."
[18] FATF Special Recommendation on Terrorist Financing IV (see Appendix VIII).

the revised 40 FATF Recommendations in June 2003 marks an important milestone in the evolution of the FATF's approach to FIUs. Largely on the basis of the work of the Egmont Group, the recommendations, for the first time, explicitly mention the FIU as the recipient of reports of suspicious transactions and specify that countries should establish FIUs.[19] With the FIU firmly established as one of the "competent authorities" in the AML/CFT system, Recommendation 30, which specifies that competent authorities should have adequate financial, human, and technical resources, clearly applies to FIUs. Similarly, Recommendation 40, which specifies that countries should ensure that their competent authorities provide "the widest possible range of international cooperation to their foreign counterparts" and that "exchanges should be permitted without unduly restrictive conditions," also applies to FIUs.

International Conventions

In the last few years, a number of international conventions have recognized the usefulness of FIUs in modern anti-money-laundering systems and have encouraged the states that are parties to these conventions to establish FIUs. These are (in the order in which they were opened for signature), the Convention for the Suppression of the Financing of Terrorism (1999), the United Nations Convention Against Transnational Organized Crime (2001), and the United Nations Convention Against Corruption (2003).

The first of these conventions requires the criminalization of the financing of terrorism; the second requires the criminalization of participation in organized international criminal groups, corruption, money laundering, and obstruction of justice. The third requires the criminalization of various forms of corruption, money laundering, concealment of the proceeds of crime, and obstruction of justice. One common element in the three conventions is that each one requires states that are parties to criminalize money laundering and to adopt measures to prevent it. The preventive measures are, in large part, inspired by the FATF recommendations and include references to the reporting of suspicious transactions to competent authorities.[20] In the two most recent conventions, the references to the FIU are explicit. For example, the United Nations Convention Against Transnational Organized Crime requires states that are parties to "ensure that administrative, regulatory, law-enforcement and other authorities dedicated to combating money-laundering ... have the ability

---

[19] FATF Recommendations 13 and 26 (2003); the methodology developed by the IMF, the World Bank, and the FATF in 2001 mentioned FIUs specifically.

[20] Convention for the Suppression of the Financing of Terrorism, Article 18 (b) (ii); United Nations Convention Against Transnational Organized Crime, Article 7, paragraph 1 (a); and United Nations Convention Against Corruption, Article 14, paragraph 1 (a).

to cooperate and exchange information at the national and international levels ... and to that end, shall consider the establishment of a financial intelligence unit to serve as a national centre for the collection, analysis and dissemination of information regarding potential money-laundering."[21]

The institutions of the European Union (EU) have taken a number of significant initiatives to combat money laundering and international organized crime. The norms adopted by the EU form part of the legal framework for the fight against money laundering in the members of the European Union, whose membership was expanded from 15 countries to 25 as of May 1, 2004. In addition, because they are elaborated with a view to being implemented in countries with differing legal systems, these norms and standards are of interest to countries outside the membership of the European Union. The main instruments bearing directly on the work of FIUs are briefly described in Box 7.

Box 7. Norms and Standards on FIUs in European Union

1991—Council Directive on prevention of the use of the financial system for the purpose of money laundering (91/308/EEC)

The Council Directive on prevention of the use of the financial system for the purpose of money laundering of 1991 embodied the basic requirements of sound anti-money-laundering programs, including customer identification, record keeping, and the blocking of suspicious transactions. With respect to FIUs (which were not mentioned as such but were included among the "authorities responsible for combating money laundering"), the directive contained three basic principles: (i) full cooperation of financial institutions with these authorities by furnishing to them, on their own initiative, information on any fact that might be an indication of money laundering and furnishing to them additional information on their request; (ii) blocking suspicious transactions until the responsible authorities had been notified; and (iii) furnishing information to the FIU whenever, as a result of an inspection or otherwise, supervisors or regulators of financial institutions discover facts that could constitute evidence of money laundering.

1997—Amsterdam European Council Meeting: EU action plan to combat organized crime

This action plan, which was endorsed at the Amsterdam European Council in June 1997, stated that "money laundering is at the very heart of organised crime." Although the action plan was directed mainly at cooperation among law-enforcement agencies, it also included preventive

[21] United Nations Convention Against Transnational Organized Crime, Article 7, paragraph 1 (b). The United Nations Convention Against Corruption contains similar language (Article 58).

measures; and, in particular, it recommended the establishment of a system for exchanging information concerning suspected money laundering at the European level (which was followed by Council Decision of October 17, 2000—see below).

1999—Tampere European Council Meeting: creation of an area of freedom, security, and justice

The 1999 European Council meeting in Tampere, Finland was devoted to "the creation of an area of freedom, security and justice in the European Union." One of its pillars is an EU-wide fight against organized and transnational crime in which special actions against money laundering are called for. One of these actions attempts to remove the remaining legal obstacles to the exchange of information among member states' FIUs. The Presidency Conclusions state that "regardless of secrecy provisions applicable to banking and other commercial activity, judicial authorities as well as FIUs must be entitled, subject to judicial control, to receive information when such information is necessary to investigate money laundering."

2000—EC Council Decision of October 17, 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information

Council Decision of October 17, 2000, which followed the Action Plan to Combat Organized Crime mentioned above, sets out detailed requirements to improve the exchange of information between FIUs. The decision endorses the Egmont Group definition of an FIU and requires that performance of their functions (including the exchange of information) not be affected by their internal status, "regardless of whether they are administrative, law-enforcement or judicial authorities."

2001—Directive 2001/97/EC of the European Parliament and the Council of December 4, 2001 amending the Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering

The 2001 amendments to the 1991 Directive reiterate the basic obligation of full cooperation and reporting of suspicious transactions set out in the 1991 Directive and extends its scope beyond financial institutions to a number of activities and professions susceptible to money laundering.

Core Principles of Financial Sector Supervision

International standards regarding the prudential regulation or supervision of financial institutions include AML/CFT compliance among the aspects of financial institutions that are subject to the powers of the regulators or supervisors.[22] The standards regarding AML/CFT are set out in general terms and directly or indirectly refer back to the FATF Recommendations.[23] For their part, the 2003 FATF Recommendations state, as a general matter, that financial institutions should be subject to adequate regulation and supervision and that they effectively implement the FATF Recommendations. For financial institutions subject to prudential supervision based on the Basel Committee, IOSCO, or IAIS standards, the AML/CFT regulatory and supervisory measures that are applied to financial institutions as a matter of prudential regulation are also applied as a matter of implementation of the FATF standards under the 2003 Recommendations.[24] The three groups of supervisors coordinate their own efforts to combat money laundering and terrorist financing, using the FATF common standards as the basis of their work.[25]

This system of cross-references minimizes the possibility of conflicts between the anti-money-laundering standards applied by prudential regulators and supervisors and those set out in the FATF Recommendations.

Model Laws

Although they do not constitute norms or standards, model laws prepared by experts may help authorities wishing to tap international experience on the establishment of FIUs. Among relevant model laws are the United Nations Model Bill on Money Laundering, Proceeds of Crime and Terrorist Financing (2003) (for common law countries), the United Nations Model Legislation on Laundering, Confiscation and International Cooperation in Relation to the Proceeds of Crime (1999) (for civil law countries), the Commonwealth Model Law for the Prohibition of Money Laundering (1996) (for common law countries), and the OAS (Organization of American States) Model Regulations

---

[22] Basel Committee on Banking Supervision, 1997 *Basel Core Principles for Effective Banking Supervision*, September, Principle 15; International Organization of Securities Commission (IOSCO), 2002, *Objectives and Principles of Securities Regulation*, February, paragraph 8.5; and International Association of Insurance Supervisors (IAIS), 2003, *Insurance Core Principles and Methodology*, October, ICP 28.

[23] In the case of the Basel Committee and the IAIS Core Principles, the standards contain an explicit reference to the FATF Recommendations; in the case of the IOSCO Principles, the substance of the standard also leads back to the FATF Recommendations.

[24] FATF Recommendation 23, second paragraph (2003).

[25] The "Joint Forum" of the three associations of supervisors has issued a note on *Initiatives by the BSBS, IAIS And IOSCO to Combat Money Laundering and the Financing of Terrorism*, June 2003.

Concerning Laundering Offenses Connected to Illicit Drug Trafficking and Other Serious Offenses (December 2002).

All of these model laws put the FIU at the center of the suspicious transaction reporting system and contain useful suggested provisions on the functions and powers of the FIU. It may be noted in this connection that, in general, the model laws suggest legal provisions for a wide range of functions that may be exercised by the FIU but do not provide guidance as to which functions should be given to an FIU in a particular case; nor do they provide guidance on the linkages that need to be established between the FIU and other agencies. Thus, although they provide useful guidance to the drafters of legislation and regulations, model laws do not replace a careful consideration of a country's own characteristics, objectives, and resources through its political and technical decision-making process.

Institutional Autonomy and Accountability

The core functions of an FIU call for objectivity in decision making, the timely processing of incoming information, and strict protection of confidential data. As the exchange of information between FIUs is based in large part on trust, building an FIU that inspires trust from its counterparts is key to effective cooperation. To ensure that these requirements are met on an ongoing basis, FIUs need to be given enough operational autonomy to allow them to carry out their assigned tasks without undue interference.

At the same time, as government agencies, FIUs are accountable for the way in which they carry out their mission. The means by which FIUs account for their actions and the person or body to which they are formally accountable will vary from country to country. Accountability mechanisms, however, need to ensure that the special powers entrusted to the FIU are not abused and that the public resources put at its disposal are used efficiently for the intended purposes.

A number of factors enter into the definition of the autonomy and accountability of the FIU. One is the placement of the FIU in the national administration and, in particular, whether it is established as part of an existing government ministry or agency, or outside any existing structure. The law may also protect the independence of the FIU by defining the manner in which its head is appointed and replaced. Specific reporting arrangements may be set out. These factors are often intertwined, and decisions about the degree of autonomy and accountability of an FIU should take all of them into account. In addition to these legal factors, other factors may affect the autonomy of the FIU, such as the local conditions related to the relations between the political power and the administration, and the actual budgetary resources provided to the FIU.

Placement in Administration

Some FIUs are established as autonomous bodies outside any preexisting government structure (see the previous discussion of autonomous or independent FIUs), while others are established as components of existing ministries or agencies. A body that is not part of a preexisting government structure is likely to enjoy a greater degree of operational autonomy than would a department within a ministry. Also, an FIU placed in an independent government agency, such as the central bank, is likely to be more independent of the government than one placed in a ministry.

Even among the FIUs established within an existing government structure, however, there are variations as to the degree of autonomy each FIU enjoys. Some FIUs are established as departments of a ministry or agency. For example, in the Czech Republic, the powers of the FIU are given to the ministry of finance and are exercised by a department of the ministry.[26] In other countries, the FIU is located in a ministry, but is given a high level of autonomy. In the United States, FinCEN was originally established as an agency of the U.S. Department of the Treasury and was elevated, after September 11, 2001, to a bureau, a more autonomous status within the department.[27] Even for FIUs located in a ministry or agency, special provisions on the appointment and dismissal of the head of the FIU or on reporting arrangements may affect the autonomy of the FIU.

Appointment and Dismissal of FIU Head

In the absence of specific provisions in the law, the head of the FIU would be appointed in the same manner and would be subject to removal and dismissal in the same way as other civil servants of comparable rank. In an FIU located in a ministry, this would normally entail appointment by the responsible minister (or the cabinet) and removal at the discretion of the appointing authority.[28] The laws of many countries contain special provisions that tend to protect the autonomy of the head of the FIU. In some cases, the appointment is given more solemnity by being made by the president of the country on the recommendation of the concerned minister or ministers. This is the case, for example, in Brazil[29] and Colombia.[30] In other countries, the prime minister is

---

[26] Act No. 61 Coll. of February 15, 1996, on Selected Measures against Legitimization of Proceeds from Criminal Activities and on the Amendment of Related Legislation, Article 7, paragraph (2) [Czech Republic].

[27] *FinCEN Strategic Plan for the fiscal years 2003–08*, page 1 [United States].

[28] As a civil servant, the person would normally be protected from arbitrary demotion and firing by civil service rules, but he or she could be transferred to another position at the minister's discretion.

[29] Law No. 9613 of March 3, 1998, Article 16, paragraph 1 [Brazil].

[30] Law No. 526 of 1999 establishing the Financial Information and Analysis Unit, Article 2

(continued)

involved in the appointment of the head of the FIU. In Bulgaria, the head of the FIU is appointed by the minister of finance "with the approval of the Prime Minister."[31]

The autonomy of the head of the FIU may also be enhanced by provisions limiting the power of the appointing authority to remove him or her from office. A restrictive set of conditions on the removal of the head from of the FIU would help to strengthen the person's independence by preventing other officials from exerting undue influence or interference. Such restrictive provisions are set out in the Bulgarian law, for example, where the head of the FIU is appointed for a term of five years and can only be removed from office, with the approval of the prime minister, for one of the reasons stated in the law.[32] In Antigua and Barbuda, the head of the FIU, who is appointed by the prime minister on the advice of the cabinet, may be removed from office only for the reasons set out in the law, and only on the recommendation of a select committee of the house of representatives.[33]

Oversight of FIUs

In some countries, the relations between the FIU and the minister to whom it is responsible are left unstated in the law. In such cases, these are similar to those between any similar entity or department and the responsible minister. In some cases, the law specifies an aspect of the relationship. In particular, some laws set out the kind of direction a minister may properly give to the FIU, thus excluding direction that would constitute improper interference. For example, the Canadian law specifies that the responsible minister "may direct the [FIU] on any matter that, in the Minister's opinion, materially affects public policy or the strategic direction of the [FIU]."[34]

The most usual vehicle through which the FIU enables the responsible authority to exercise its supervisory function is by issuing a periodic report on its activities. Most laws on FIUs provide that the FIU issue such a report on an annual basis, but the structure and contents of the report is left to the FIU. Most FIUs provide a narrative account of the past year's activities, as well as statistical data on reports received, files sent for investigation or prosecution, and exchanges with foreign FIUs. Some FIUs (Australia, for example) organize the report along the lines of their broad qualitative objectives and provide their own assessment as to the extent to which they have achieved

---

[Colombia].

[31] Law on Measures Against Money Laundering, Article 10 (4) [Bulgaria].

[32] *Id.*, Article 10 (8).

[33] Office of National Drug and Money Laundering Control Policy Act, 2002, Section 6 [Antigua and Barbuda].

[34] Proceeds of Crime (Money Laundering) and Terrorist Financing Act, Section 42 (2) [Canada].

these objectives. This organization facilitates the assessment of the performance of the FIU on the part not only of the responsible minister but also of the general public.

Most often, the responsible minister exercises his or her supervision of the FIU directly. In a few countries, however, a high-level committee is placed between the FIU and the minister. The functions of such committees vary from country to country, but some of them have a clearly defined supervisory role with regard to the FIU.

In Italy, a "guidance committee" was established in 1997 to make an annual "overall examination of the activity [of the FIU in implementing the anti-money-laundering law] in order to evaluate the progress and the results of the activity and to formulate proposals aimed at enhancing the effectiveness of anti-money laundering action." The committee is chaired by the director general of the treasury and includes high-level representatives of the Bank of Italy and the ministries of interior, finance, justice, and foreign trade. The FIU is required to provide half-yearly reports on its activity to the committee, including all the information to the committee needs to carry out of its functions.[35]

Similarly, in the Netherlands, an "assistance committee" made up of representatives of the concerned ministries, law-enforcement, and prosecution agencies; financial sector supervisors; and the sectors to which the AML law applies is charged with "assisting the [FIU] in its functioning, offering its knowledge and expertise to it," and "advising [the FIU's supervising ministers] on the way the FIU carries out its duties and on the effectiveness of the disclosure obligation."[36]

In South Africa, a "money laundering advisory council" advises the supervising minister on "policies and best practices to identify the proceeds of unlawful activities and to combat money laundering activities, and the exercise by the minister of his powers under the AML act, to advise the [FIU] concerning the performance of [its] functions, and act as a forum in which the [FIU], associations representing categories of accountable institutions, organs of state and supervisory bodies can consult one another."[37]

---

[35] Decree Law 143 of May 3, 1991, as amended by Legislative Decree 153 of May 26, 1997, Article 3-*ter* [Italy].

[36] Act of 16 December 1993 containing regulations on the disclosure of unusual transactions relating to financial services, Sections 15 and 16 [Netherlands].

[37] Financial Intelligence Centre Act, 2001, Sections 17–20 [South Africa].

As these examples show, committees established to supervise the work of the FIU may also advise the responsible minister more broadly on ways to improve the AML/CFT framework. These committees may provide an institutional basis for responding to FATF Recommendation 31, which states that "[c]ountries should ensure that policymakers, the FIU, law-enforcement and supervisors have effective mechanisms in place which enable them to co-operate, and where appropriate coordinate domestically with each other concerning the development and implementation of policies and activities to combat money laundering and terrorist financing."

Organization and Staffing

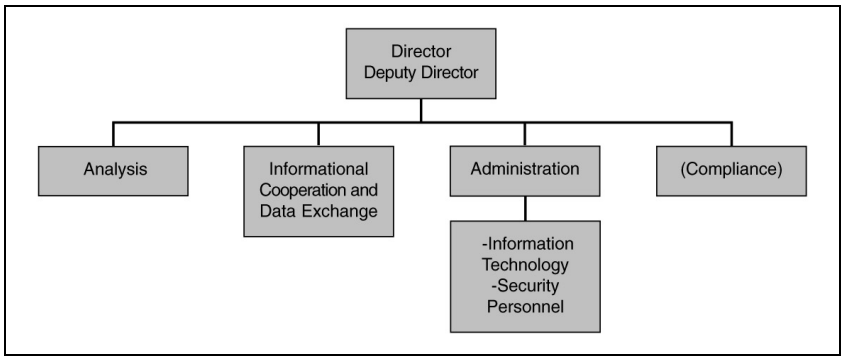
Internal Organization

The internal organization of an FIU varies depending on the functions entrusted to it and on its size. In countries with a limited financial infrastructure, the FIU is likely to be small, and its structure may be very simple. In larger jurisdictions, where the FIU will be larger and have more complex responsibilities, a sound internal organization will be essential to efficiency and success. In such countries, most FIUs will, for example, have a department dedicated to the receipt and analysis of transaction reports, since this is a core function of all FIUs. Exchange of information may be dealt with in the same department or become the responsibility of a separate department if the volume of exchanges warrants it. Similarly, once an FIU reaches a certain size, administrative matters may be entrusted to a separate department. An administrative-type FIU that is responsible for supervising the compliance of reporting entities with AML/CFT requirements (a function that requires additional resources) will normally have a department dealing with supervision.[38] Beyond this, organizational arrangements vary.

A typical FIU may be organized as shown in Figure 2. It should be emphasized that such a structure is shown strictly as an example to illustrate the links between the functions entrusted to the FIU and the possible organization of the corresponding tasks inside the FIU—other arrangements are certainly possible. Also, in very small FIUs, such a formal organization may not be necessary.

[38] Examples are the AMLD in Croatia, the FIA in Bulgaria, and the OMLP in Slovenia.

Figure 2. Typical FIU Organization Chart



The department responsible for receiving and analyzing reports (the analysis department) is the key department in an FIU, since it receives suspicious transaction and other reports and analyzes them. The analysis department may also communicate with the compliance officers or other authorized representatives of reporting entities on individual cases. Staff of the analysis department usually manage the internal databases on suspicious transactions and on freezing orders issued (if applicable), unless the information technology function becomes so important as to be made the responsibility of a separate department. Staff of this department may be authorized to request information from other FIUs or may initiate the requests if they are sent by the international cooperation department. The department may also prepare typologies for purposes of training and sharing of information on trends in criminality.

A department for international cooperation and information exchange usually covers multilateral and bilateral cooperation matters. Typically, the international cooperation department maintains a database on information exchanged with other agencies and FIUs that is shared with the analysis department. The international cooperation department may be authorized to communicate directly with counterpart FIUs and other foreign bodies dealing with money laundering in individual cases.

FIUs with regulatory or supervisory responsibilities often establish a separate department to carry out these functions. This department monitors compliance with AML/CFT requirements and initiates the sanctions mechanism in cases of serious failures to report transactions. If the FIU has the power to apply administrative sanctions, the department would be responsible for this as well. This department also cooperates with primary supervisory bodies of the reporting institutions and exchanges information with them (if legally possible) on compliance matters. The department also works with professional associations in improving sector compliance and offers training to improve reporting.

In many FIUs, sophisticated data storage, retrieval, and analysis technologies are employed, and the maintenance of the supporting computing infrastructure becomes a vital component of their operations. A group of highly skilled information technology (IT) staff is needed for this purpose. In some FIUs, these staff are located in the analysis department, where most of the computing is done, although the IT staff serve the entire FIU. In other FIUs, a separate department is established to denote the importance of information technology to the FIU as a whole and facilitate the work of the organization.

Staffing

Human resources are usually part of the central management functions, except in the larger FIUs, where a separate human resources department may be established. An organization chart describes the tasks and required qualifications for each position. An FIU may need expertise in a wide range of fields, especially when the scope of the reporting obligation is broadened beyond financial institutions. Economists, bankers, lawyers, law-enforcement officers, information technology engineers, securities brokers, insurance specialists and gaming specialists, are among the experts who may be needed to analyze reports. In addition to sector knowledge, staff in the analysis department will also need good analytical skills. Security is of paramount importance in an FIU, and thorough background checks (involving a review of criminal, financial, and personal records) must be performed on candidates for employment. In many cases, the staff of FIUs can be composed of experts seconded by administrations or departments concerned with financial crime (such as justice, police, finance and customs departments, and supervisory authorities).

Liability of Staff and Confidentiality of Information

In most cases, FIU staff will be civil servants, subject to the laws and regulations governing the status and conduct of civil servants and protected by the general rules governing suits against them. In many countries, these rules include a general duty of discretion with respect to the matters staff deal with and general protection against claims of liability for actions taken in the course of their employment.

The very special nature of the work of an FIU often leads, however, to inclusion in the legislation of strict rules regarding the confidentiality of the information handled by its staff and immunity from liability for disclosure of the information to authorized persons (such as the prosecutor's office or a foreign FIU). Some countries may also have rules barring the use of suspicious transaction reports in court proceedings and shielding FIU staff from compulsory testimony in court cases. In addition, most FIUs have internal confidentiality regulations that describe in detail the procedures for handling

the information and data available in the FIU. Controls over the uses made of FIU information is exercised on a regular basis.

Security Issues

Along with confidentiality of information, security issues are most important in an FIU. Staff are informed (and often reminded) of the security procedures they must follow. The premises of the FIUs are protected (by alarms and security officers). Access of visitors is limited. Special protection is often arranged for the rooms where data on suspicious transactions and other FIU databases are located.

The separation of the FIU's databases from the outer electronic world is an important element in maintaining the security and confidentiality of FIU information. In many FIUs, the computer system consists of an internal network with limited connection to the outside. Special software for data protection is installed, and message-encrypting systems are used in all exchanges of sensitive data with the outside.

Box 8. FIUs in Very Small Developing Island Economies

In the very small developing island economies, such as some of those in the Caribbean and the South Pacific, the challenges in establishing an FIU can be daunting. These economies are the size, in terms of population, of a small town in most other countries, and their revenues per capita are very low.

Finding suitable staff is the first challenge. Persons skilled in financial investigations, forensic accounting, and other AML/CFT tasks are less likely to be locally available, and it may not be easy to attract such persons from elsewhere.

Second, since the conventional banking system does not usually cover as much of the population in these jurisdictions (since operational costs are usually high in relation to the number of persons served), their FIUs need to focus their efforts on the informal banking or funds-transfer networks, which pose the additional challenge of lack of documentation, thereby adding to the FIU's costs.

Third, FIUs in these jurisdictions may find that it is not always easy to obtain financial intelligence and information from other FIUs, because they tend to be less well known outside their regions. Many of them are not members of the Egmont Group, a situation that may raise concerns among other FIUs as to the safeguards available to protect the confidentiality of data held by them.

Finally, the establishment and operation of an FIU involves a level of financial commitment that is proportionately much greater for the very small and developing jurisdictions than for other economies. Operating even the

most basic FIU entails certain costs, in terms of staffing, training, equipment, and secure facilities, and these costs are proportionally higher in these jurisdictions.

Would a regional FIU provide the solution to these problems? Studies were carried out to explore the possibility of setting up regional FIUs in the Caribbean and South Pacific subregions. In October 2003, the Caribbean project, which related to an FIU that would have coexisted with national FIUs, was "laid to rest in light of the fact that the Caribbean Financial Action Task Force (CFATF) members from the subregion have not responded enthusiastically with regard to taking this matter forward" (CFATF, *Annual Report 2002–2003*, p. 23).

After a number of studies, including a feasibility study by the IMF Legal Department, the concerned Pacific island countries, together with the Pacific Forum Secretariat, the APG Secretariat, the IMF Legal Department, and the Egmont Group (Oceania Region), decided in September 2003 that "(a) the notion of a regional approach for supporting [Pacific island countries] in addressing their needs in relation to financial intelligence information be approved; and (b) the IMF Legal Department will produce a proposal to advance the development and implementation of the regional approach." Work toward this objective is under way. What is envisaged is an organization to support national FIUs in the subregion, rather than a regional FIU. Under the definition of an FIU endorsed by the Egmont Group and the FATF, FIUs are *national* entities.

3

CORE FUNCTIONS OF AN FIU

Although they vary in many ways, FIUs share a common definition, which refers to their basic function: serving as a national center for the collection, analysis, and dissemination of information regarding money laundering and the financing of terrorism. These three functions are the core functions shared by all FIUs recognized by the Egmont Group. The definition of FIUs based on their core functions was first formalized by the Egmont Group in 1996.[39] Similar definitions, also based on the three core functions, have now been incorporated in the revised FATF Recommendations of June 2003[40] and in two global conventions.[41]

Given their different status and history, it is not surprising that in some countries the FIU is entrusted with additional functions. For example, some FIUs monitor the compliance of certain entities with AML/CFT rules and standards. Other FIUs have the power to block reported suspicious transactions for a limited time. The FATF recommendations set a standard that countries should establish an FIU with the three core functions and contains other provisions that relate to the exercise of these functions. In contrast, no international norm or standard deals with the noncore functions of FIUs. In this chapter, the core functions will be discussed in some detail, while some of the most significant noncore functions exercised by FIUs will be described in Chapter 4.

---

[39] "A central, national agency responsible for receiving, (and as permitted, requesting), analyzing and disseminating to the competent authorities, disclosures of financial information: (i) concerning suspected proceeds of crime and potential financing of terrorism, or (ii) required by national legislation or regulation, in order to combat money laundering and terrorism financing." For a detailed discussion of each of the terms used in the definition, see Egmont Group, *Interpretive Note Concerning the Egmont Definition of a Financial Intelligence Unit* (Appendix IV).

[40] "Countries should establish a FIU that serves as a national centre for the receiving (and, as permitted, requesting), analysis and dissemination of STR and other information regarding potential money laundering or terrorist financing [....]" (Appendix VII)

[41] Two conventions require that States Parties are to "consider the establishment of a financial intelligence unit to serve as a national centre for the collection, analysis and dissemination of information regarding potential money-laundering." Palermo Convention, Article 7, paragraph 1(b) (Appendix X); and United Nations Convention Against Corruption, opened for signature at Merida, Mexico, December 9, 2003, Article 14, paragraph 1(b) [not yet in force] (see Appendix XI).

Receiving Transaction Reports

In designing an FIU or enhancing the effectiveness of an existing one, it is useful to consider its core functions as generating a continuous flow of information. Reporting entities and other FIUs provide information to the FIU, which, in turn, analyzes this information and passes the results of its analysis along to investigators and prosecutors, as well as other FIUs. In planning the FIU, it is important to ensure that there is an initial balance between the quantity of information to be provided to the FIU, on the one hand, and its capacity to store and analyze it, on the other hand. Similarly, there needs to be a balance between the number of cases to be sent to the police for further investigation or to prosecutors for prosecution, and the capacity of these bodies to deal effectively with those cases. This flow of information is essentially dynamic. As the number of reports increases, the FIU will need to adapt to ensure that it continues to be capable of handling the reports it receives. [42]

The basic definition of the reporting obligation has two main aspects: which persons and entities are to be obligated to report and what is to be reported. Other aspects needing considerations include the form and contents of reports, rules relating to the reporting organizations, and means of enhancing the flow and quality of reports (including sanctions).

Who Must Report?

Prudentially regulated financial institutions, and banks in particular, have traditionally been at the center of the system of reporting suspicious (and other) transactions. The sheer volume of transactions undertaken through them, compared with other institutions through which money can be transmitted, makes them the prime target for financial misuse. Reports of FIUs on the sources of the reports they receive confirm this point. In countries that have extended the reporting obligation beyond financial institutions, the largest proportion of reports continues to come from financial institutions and, in particular, from banks.

Reports of nonfinancial institutions are increasingly important, however. As financial institutions put in place more sophisticated systems to detect and report suspicious transactions, criminals may be tempted to use other institutions and professionals for laundering purposes. It is therefore

---

[42] Obviously, once the obligation to report certain transactions is established, reporting entities are obliged to report these transaction whether or not the FIU is in a position to analyze them. Similarly, the FIU must send cases for investigation or prosecution even if the receiving agencies are not sufficiently equipped to deal with them.

important that those institutions and professionals also detect and report suspicious transactions.[43]

The successive FATF recommendations mark the progressive widening of the range of institutions subject to the reporting obligation, starting with regulated financial institutions and then expanding beyond them. The 1990 Recommendations gave countries the option of having a permissive or mandatory system of reporting suspicious transactions that was directed at financial institutions. In addition, countries were asked to consider a wider system of reporting that would cover financial institutions and other financial intermediaries. The 1996 revisions extended the reach of the recommendations to all financial institutions and other nonregulated financial intermediaries, with particular attention paid to *bureaux de change*.[44]

The year 1999 marked the beginning of the international movement to extend the reporting obligation beyond financial institutions and intermediaries. In that year, in Moscow, a ministerial conference of the Group of Eight (G-8) countries on combating transnational organized crime stated that the ministers had "agreed to consider putting certain responsibilities, as appropriate, on those professionals, such as lawyers, accountants, company formation agents, auditors, and other financial intermediaries who can either block or facilitate the entry of organized crime money into the financial system."[45] The 2003 revisions to the Forty Recommendations of the FATF implement the G8's "Gatekeeper" initiative by extending basic AML/CFT prevention requirements, including the reporting requirements, with some qualifications, to a list of "designated non-financial businesses and professions" that includes casinos; real estate agents; dealers in precious metals and precious stones; lawyers, notaries, and other independent professionals and accountants in certain defined circumstances; and trust and company service providers.[46]

---

[43] This "displacement effect," whereby as more stringent preventive measures are put in place in the financial sector, money launderers seek to use other businesses or professions to achieve their goals, has been observed for a number of years by the FATF (see FATF, *Annual Report*, 2002–2003, page 6; and FATF, 2002, *Review of the FATF Forty Recommendations, Consultation Paper* [hereinafter referred to as the *Consultation Paper*], paragraph 273).

[44] FATF Recommendation 8 and 9 and Interpretative Note (1996).

[45] Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime (Moscow, October 19–20, 1999), Communiqué, paragraph 7.

[46] Even before the 2003 FATF Recommendations were issued, the European Union issued its 2001 revised Anti-Money Laundering Directive, which implemented the Gatekeeper initiative in EU member countries.

Financial institutions

Banks were the first institutions to be specifically subjected to the reporting obligations under the original 1990 Recommendations. Nonbank financial institutions were also included in principle, but no list of such institutions was provided in the recommendations. A working group of the FATF was established to set out a minimal list of nonbank financial institutions and other professions dealing with cash that could be made subject to the recommendations. In the 1996 Recommendations, "financial institutions" were subjected to the reporting and other recommendations. These included those that were subject to prudential supervisory regime, such as banks, insurers, and stock dealers, and those that were not, particularly *bureaux de change*. These are now included in the scope of "financial institutions" in the 2003 Recommendations.[47]

The 2003 Recommendations clarified the scope of the reporting obligation (and other obligations) by, among other things, providing a detailed list of what constitutes "financial institutions."[48] The list includes not only the institutions normally subject to prudential supervision, such as those accepting deposits, making loans, underwriting insurance, or managing portfolios, but also formal and informal money- and value-transfer services.

Bank and insurance and securities companies

At the start of the fight against money laundering, the focus of attention was on credit and financial institutions, such as banks and insurance and securities companies. It was recognized that when these institutions were used to launder proceeds from criminal activities, their soundness and stability could be seriously jeopardized and the public's confidence in the banking system as a whole could be lost.[49] At the same time, it was clear that keeping the financial system from being used for money laundering was a task that could not be carried out without the cooperation of credit and financial institutions and their supervisory authorities.

The Declaration of Principles adopted in December 1988 by the Basel Committee on Banking Supervision constituted a major step toward involving banks in the prevention of the use of the financial system for money-laundering purposes. Since public confidence in banks, and hence their stability, could be undermined by adverse publicity owing to their inadvertent association with criminals, the Declaration of Principles encouraged banks' managements to put in place effective procedures to ensure that all persons

---

[47] FATF Recommendations, Glossary (2003). See Appendix VII.

[48] *Id.*

[49] See, for example, the first consideration of the Council Directive 91/308/EEC of June 10, 1991 on prevention of the use of the financial system for the purpose of money laundering.

conducting business with their institutions were properly identified, that transactions that did not appear legitimate were discouraged, and that cooperation with law-enforcement agencies was achieved.[50]

Although, because of its ability to move funds rapidly, the banking system was considered especially vulnerable to money laundering, insurance companies have also been identified as major targets of money laundering, because of the variety of services and investment vehicles offered that can be used to conceal the source of money.[51]

Life insurance and, in particular, life insurance products with an investment feature are favored by money launderers. Money can also be laundered, however, by the use of other types of insurance. For example, illegally obtained funds may be used to purchase assets that are deliberately destroyed in order to enable the holder to receive "clean" claim money from an insurer. Most countries have established, in accordance with international standards, reporting duties for life insurance companies. Countries can also consider imposing similar AML/CFT requirements on certain other types of insurance contracts. Insurance intermediaries also play an important part in finding customers for insurance companies and undertaking transactions on their behalf. For this reason, in accordance with the FATF Recommendations, the same principles that apply to insurers should generally apply to insurance intermediaries.

As the sophistication of financial institutions has grown, new and creative ways to hide the source of illegally obtained profits have been devised. Among them, investment products sold by securities and investment firms will be particularly interesting for money launderers who wish to hide the origin of illegally gained proceeds or use them to make long-term investments. Different types of securities and investment companies will have different vulnerabilities to money laundering. For example, Internet-based brokerage accounts will be particularly vulnerable to use by money launderers, since they provide little opportunity for face-to-face contact with customers or for verifying the identity of those logging in.

In many countries, financial groups engage in banking, securities, and insurance businesses, and it has become particularly important for countries to have consistent AML/CFT requirements across sectors and to apply these requirements consistently.

---

[50] Basel Committee on Banking Supervision (BCBS), *Prevention of Criminal Use of the Banking System for the Purpose of Money-Laundering*, December 1988.

[51] International Association of Insurance Supervisors (IAIS), *Anti-Money Laundering Guidance Notes for Insurance Supervisors and Insurance Entities*, January 2002.

Nonfinancial businesses and professions

The 2003 FATF recommendations widen the reporting obligation beyond financial institutions to casinos; real estate agents; dealers in precious metals and precious stones; and lawyers, notaries, other independent professionals, and accountants. The inclusion of a wider range of businesses and professions in the scope of the reporting obligation may lead to FIUs receiving reports very different from those supplied by financial institutions. The analysis of such reports may require skills that are not commonly available in many FIUs. Moreover, in many countries, these sectors are not supervised as closely as traditional financial sector institutions (and banks in particular). As a result, greater efforts may be needed to achieve the required level of compliance with the reporting requirements, both in terms of quantity and quality of data supplied.

Casinos[52]

Casinos offer an attractive venue for laundering illegal proceeds, because gambling involves large volumes of cash and many casinos offer their clients a wide variety of financial services. Casinos are also attractive to organized criminal groups who, if they are successful in gaining control of casinos, can use them to disguise their criminal activities. Strict rules on ownership of casinos and close supervision of their activities help mitigate these risks.

Some methods that are often used to launder money may also be banned (and are banned in some jurisdictions), including the following:

- buying chips or tokens with cash, or conducting minimal or no betting and then requesting repayment of the balance by a check drawn on the casino's account or by a transfer to a bank account;
- using a chain of casinos in different countries and asking for an amount of credit to be made available in a jurisdiction other than the one in which the funds were originally placed, in the form of a check or through a bank transfer; and
- asking that a winner's check be made out to a third person or without a nominee.

The FATF's *Consultation Paper* mentions the importance of certain forms of noncasino gambling, including horse-race betting, card clubs, and lotteries, but in the end, the 2003 Recommendations did not include these forms of gambling. Internet casinos are included, but other forms of internet gambling are not.

---

[52] This section draws on the *Consultation Paper*, discussion of casinos (part 5.1).

Real estate agents and dealers in precious metals and precious stones

Real estate and high-value items, such as gold pieces and precious metals and stones, offer attractive opportunities for money launderers. The purchase of real estate is a known form of investing illicit proceeds and holding them. Precious metals and stones can be used in the same manner and also as a means of transporting illicit proceeds from one jurisdiction to another.

The 2003 FATF Recommendations list real estate agents, dealers in precious metals, and dealers in precious stones among the nonfinancial professionals subject to the reporting requirement. Dealers in precious metals and stones are only required to report suspicious transactions above the designated threshold of US$/EUR 15,000. The second EU directive on preventing the financial system from being used for money laundering includes a broader list of professions in this category, which it describes as "dealers in high-value goods, such as precious stones or metals, or works of art, auctioneers, wherever the payment is made in cash, and in an amount of EUR 15,000 or more."[53] This wider definition can include dealers in automobiles (including used cars), boats, and antiques—traders that so far had been left largely unregulated. Since these traders are not regulated or supervised, their inclusion in the scope of the reporting requirements raises the question of which agency will be responsible for their compliance with the AML/CFT requirements. (See Chapter 4 for a discussion of this point.) Regardless of the choice of supervising agency, ensuring adequate reporting on such trades may well require a determined outreach effort.

Lawyers, notaries, other independent professionals, and accountants

Together with trust and company service providers, lawyers, notaries, and accountants are seen as gatekeepers, because, owing to the nature of some of their activities, they may be in a position to detect the intended use of legal arrangements, such as trusts and corporate vehicles, to launder funds. Indeed, criminals may seek the services of legal professionals precisely to receive assistance in making illegal transactions more difficult to detect or to use the lawyer's client account as a means of introducing illegal funds into the banking system.[54]

The limited degree to which these professionals may be required to report illegal activity however, stems from the deeply ingrained view that legal professionals are bound by rules of confidentiality and of loyalty to clients that

---

[53] Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering, Article 2 [EU].

[54] R. E. Bell, 2002, "The Prosecution of Lawyers for Money Laundering Offenses," *Journal of Money Laundering Control*, Vol. 6, No. 2, p. 17–26.

are not easily reconciled with an obligation to report suspicious transactions. The scope of the reporting obligation and the rule against "tipping off" have both been cited as alien to the basic duties of lawyers. To date, the international effort to include legal professionals in the scope of the reporting obligation has had mixed results.

Before the 2003 FATF Recommendations were issued, the amended EU directive had already required EU member countries to extend the reach of the reporting obligation to certain activities of legal professionals—they had to submit reports when they participated in certain defined transactions by assisting their clients concerning them, or when they acted on behalf of their clients in financial or real estate transactions. In extending the reporting obligation to lawyers and notaries, the FATF also limited the scope of activities that could trigger the reporting obligation. Lawyers, notaries, other independent legal professionals, and accountants are required to provide suspicious transaction reports only when, on behalf of a client or for a client, they engage in a financial transaction related to the following activities: "buying and selling of real estate, managing of client money or other assets, management of bank, savings or securities accounts, organization of contributions for the creation, operation or management of companies, and creation, operation or management of legal persons or arrangements, and buying and selling of business entities."[55] As is stated in the *Consultation Paper*, "In essence..., independent legal professionals are brought into the fight against money laundering when they are involved in particularly vulnerable lines of business."[56]

A large number of bar associations and of international groups of lawyers have expressed their opposition to the extension of the reporting requirements to their profession; and in some countries, attempts to implement the initiative have proved difficult. In two countries, Monaco[57] and Canada,[58]

---

[55] FATF Recommendations 12 (d) and 16 (a) (2003).

[56] *Consultation Paper*, paragraph 278. The statement is made in regard to the EU directive, but is equally applicable to the Revised Recommendations as they were issued.

[57] In Monaco, a reference to "attorneys, except if they have acquired the information relating to transactions entailing movements of funds in ensuring the defense of their clients" in a decree listing professions subject to the reporting requirements of the anti-money-laundering law was struck down on the grounds that the text failed to enumerate the kinds of transactions involved and failed to specify the circumstances in which information could be regarded as having been acquired in ensuring the defense of a client and thus was not drafted in terms clear and precise enough to avoid arbitrariness. A similar reference to lawyers in the anti-money-laundering law itself, however, was not challenged, leaving the situation unclear (Tribunal Suprême de la Principauté de Monaco, décision du 6 mars 2001, *Journal de Monaco, Bulletin Officiel de la Principauté*, no 7486, March 16, 2001).

[58] In Canada, regulations issued in November 2001 that applied the suspicious transaction reporting obligation and the prohibition against "tipping off" of the Proceeds of Crime (Money

(continued)

attempts to extend the reporting obligation to attorneys were successfully challenged in the courts. Nevertheless, the reporting obligation for the legal profession exists in a number of countries, although the obligation is tailored to meet the special situation of lawyers. In the United Kingdom, the reporting obligation is subject to an exception for privileged information.[59] In Slovenia, the obligation is limited to certain acts performed by legal and other professionals on behalf of their clients.[60] In Belgium, the obligation is also limited to certain acts performed by lawyers on behalf of their clients (as set out in the revised EU directive), and the circumstances in which reports must be submitted are more limited than they are for the financial professions. Moreover, lawyers furnish their reports to the head of the bar association, who transmits it to the FIU if he finds that the legal conditions requiring the report are met.[61] In Australia, the reporting obligation of solicitors is limited to cash transactions above a prescribed minimum amount (AU$10,000) to which they are a party in the course of their practice.[62]

It should be noted that although the number of suspicious transaction reports produced by legal professionals may not be large when compared with the number provided by financial institutions, they may be of an entirely different nature and could require considerable expertise to analyze. Financial transactions involving complex legal arrangements, multiple trusts, and corporate vehicles are only some of the structures that would require scrutiny.

Laundering) Act to lawyers, notaries, accountants, real estate brokers, and other nonfinancial intermediaries were repealed in March 2003, after virtually all Canadian jurisdictions had granted a temporary exemption to lawyers pending final resolution of the broad legal and constitutional challenges commenced in the courts by the law societies. A test case for these challenges in the courts of British Columbia has now been adjourned by agreement of the parties (Federation of Law Societies of Canada, Money-Laundering Chronology of Events, July 2003, and Federation of Law Societies of Canada, petitioner, and Attorney General of Canada, respondent, Order of the Honorable, the Chief Justice of the Supreme Court of April 15, 2003, Supreme Court of British Columbia, Vancouver Registry, no. L013117).

[59]Proceeds of Crime Act 2002, Section 330 [United Kingdom] The United Kingdom's FIU has issued a "good practice" document as guidance for disclosures by the legal profession (National Criminal Intelligence Unit, *Part 7 Proceeds of Crime Act 2002, National Criminal Intelligence Service guidance in relation to disclosures by the legal profession*, October 2003).

[60] Law on the Prevention of Money Laundering, as amended to July 20, 2002, Articles 28 and 28a [Slovenia].

[61] Although financial institutions must report all transactions that they know are linked, or they suspect are linked, to money laundering or the financing of terrorism, legal professionals must make a report only when they "become aware of facts" that they know or suspect are linked to these crimes (Law of January 11, 1993 on Preventing Use of the Financial System for Purposes of Laundering Money, as amended, effective February 2, 2004, Articles 14*bis* [Belgium]. See also Jean Spreutels and Claire Scohier, "*La Prévention du blanchiment des capitaux, évolutions récentes*, *Rev. Dr. ULB*," 1997-1 (1998), pp. 165–87, available on the website of the Belgian FIU at *http://www.ctif-cfi.be/fr/index.htm.*

[62] Financial Transaction Reports Act 1988, as amended, Section 15A [Australia].

Thus, extension of the reporting obligation to these professions may well have staffing and cost implications for the FIU.

Trust and company service providers

Trust and company service providers are also brought under the new FATF reporting standard. They include persons not otherwise covered in the FATF Recommendations who provide to third parties services such as acting as a formation agent of legal persons, a director or secretary of a company, a partner of a partnership, or in a similar position in relation to other legal persons; providing a registered office, business address, or accommodation for a company or partnership; acting as a trustee to an express trust; and acting as a nominee shareholder for another person.[63]

Others

Some countries extended the reporting obligation beyond the international standards. For example, in South Africa, although only designated institutions must report transactions above a specified amount, any person who operates, is in charge of, manages, or is employed by a business must report certain defined suspicious transactions.[64] In Colombia, the reporting obligation and other related obligations are extended to entities involved in foreign trade.[65]

What Is to Be Reported?

The international standard on reporting transactions has evolved over time. In the late 1980s and early 1990s, there was considerable discussion as to whether reporting institutions should report all transactions above a certain amount, only those transactions that appeared to be related to criminal activity, or a combination of both.[66] The first FATF Recommendations, issued in 1990, stated that countries should ensure that financial institutions pay special attention to suspicious transactions; investigate their backgrounds; and keep the findings available for supervisors, auditors, and law-enforcement agencies; but there was no standard requiring them to report these transactions to a competent authority. In fact, countries were encouraged to consider the feasibility and utility of a different reporting system, based on the obligation to

---

[63] FATF Recommendation 12 (e) and Glossary (2003). See Appendix VII.

[64] Financial Intelligence Centre Act, 2001, Section 29 [South Africa].

[65] Circular 170 of October 10, 2002 of the Tax and Customs Administration Directorate (DIAN). The list includes public and private warehouses, customs intermediaries, ports, companies located in free trade zones, international cargo agents, curriers, and postal shipping intermediaries [Colombia].

[66] For a discussion of this issue, see Jean-François Thony, "Processing Financial Information in Money Laundering Matters: The Financial Intelligence Units," 3 *European Journal of Crime, Criminal Law and Criminal Justice* 257, pp. 258–62 (1996).

report transactions above a fixed amount to a central authority.[67] With the adoption of the 1996 revisions to the FATF Recommendations, suspicious transaction reporting was established as the international standard.[68]

In some countries, including the United States, the obligation of financial institutions is to report "suspicious activities" rather than "suspicious transactions."[69] The meaning of the former expression is somewhat broader than the latter, since it includes suspicious transactions and other circumstances that raise suspicions of criminal activities. The difference between the two expressions, however, may be narrowed in part by specifying that reporting entities must report transactions that were not executed if the circumstances that led to their not being undertaken are suspicious, a requirement that occurs in many countries.[70]

Suspicious Transaction Reports

There are two aspects to the definition of the obligation to report suspicious transactions. The first is the definition of what "suspicious" means. This establishes the "level of conviction" that needs to be present in order for the facts surrounding a particular transaction to amount to a reportable "suspicion." The second is the definition of the range of criminal activity, a suspicion of which may trigger the reporting obligation. FATF Recommendation 13 refers to funds that "are the proceeds of criminal activity."[71] Some national legislation uses a slightly different standard.

In defining the obligation to report suspicious transactions, the benchmark should be set in such a way that the smallest possible number of suspicious transactions go unreported, while the number of reports that turn out to not be suspicious is limited. At the same time, it is important to recognize that it is not the function of the reporting entities to investigate suspicious transactions beyond assembling the basic facts necessary to establish that a transaction is, indeed, suspicious. It is thus expected that a large proportion of reports will be found, upon analysis by the FIU, not to be linked to criminal activity.

---

[67] FATF Recommendation 24 (1990).

[68] The 1996 and 2003 Recommendations use the term "funds" rather than "transactions," but the FATF appears to equate the term with "transactions" (*Consultation Paper*, paragraph 142).

[69] 12 CFR part 21, Subpart B, Suspicious Activity Report [United States].

[70] In Monaco, for example, the reporting obligation extends to cases where an institution refuses to carry out a transaction which would have fallen under the reporting obligation if it had been carried out (Law No. 162 of July 7, 1993 on the participation of financial entities in combating money laundering, amended by Law No. 1253 of July 12, 2002, articles 5 and 32 [Monaco].

[71] For a discussion of this standard, see page 46.

What is a suspicion?

A suspicion is a conclusion to which a reporting institution arrives after consideration of all relevant factors. The definition of the suspicion needs to be expressed in the clearest terms possible. The requirement of clarity in the definition of a suspicious transaction is particularly important in countries where criminal sanctions are attached to failures to comply with the reporting requirement. It is also important in other jurisdictions, since complex and expensive systems have to be put in place to implement the reporting obligation.

In many countries, the law requires that "suspicious" transactions be reported but does not define "suspicious." The terms "suspicious" and "suspicion" have a fairly wide range of meanings and may include situations where a very low "evidentiary threshold" is involved. For example, in the context of the laws of the United Kingdom and of Scotland, it has been noted that the ordinary meaning of the word would include the idea of "imagining something without evidence or on slender evidence."[72] Similarly, in the United States, the term "suspicion" has been defined as "the imagination or apprehension of the existence of something wrong based only on slight or no evidence, without definitive proof."[73] In French, the equivalent term "*soupçon*" also has a number of meanings, some of which also imply very little evidence such as, for example "a simple conjecture, opinion, advice or hypothesis or intuition..."[74] Although these definitions do not have the force of law, they clearly show that the term "suspicious" and "suspicion" can have a variety of meanings.

The use of such a broad standard gives considerable discretion to the reporting entity in its decisions to report or not to report transactions. This discretion is consistent with the view that decisions on what transactions are suspicious should be made by staff of the financial institutions on the basis of their skills, experience, and knowledge of the customer, rather than on the basis of a rigid set of rules. Such a standard places a significant burden on the reporting entities, however, and also tends to increase the number of suspicious transaction reports received by the FIU. This places an additional burden on the FIU, which needs more staff and other resources (including access to

---

[72] Alastair N. Brown, "Money Laundering: A European and U.K. Perspective," [1997] 8 *J.I.B.L.* 307, at 309. The author takes the view that in the context of the reporting obligation, "the term 'suspicion' means a state of mind which considers that there is a real possibility that the person is a [criminal]."

[73] Bryan A. Garner, Ed. in Chief, *Black's Law Dictionary*, Seventh Edition, West Group, St. Paul, Minnesota, 1999, at 1460.

[74] "*Simple conjecture, avis, hypothèse ou intuition concernant quelque chose sans connotation défavorable,*" *Trésor de la Langue Française*, available on the Internet at *http://zeus.inalf.fr*.

information) to analyze the reports. Some countries, in view in particular of the penalties attached to failures to report, have acted to limit the discretion of reporting entities. Some have done so by adding specificity to the required "suspicion," while others have avoided the use of the "suspicious" criteria altogether.

Certain countries have tried to make the meaning of the word "suspicion" clearer by requiring, in the law itself, that the suspicion be grounded in some factual observation. For example, the Swiss money-laundering law refers to a "*soupçon fondé*" ("a founded suspicion" in the unofficial translation issued by the Swiss authorities)[75]—that is, a suspicion grounded in some factual basis, however slim. The Australian law also uses a more objective criterion and requires cash dealers to report transactions when they have "reasonable grounds to suspect that information" they have may be relevant to the investigation or prosecution of an offense.[76] These laws may have made the standard more objective, but it has been observed that they may also have made the "evidentiary threshold" higher.[77]

Another way of limiting, to some extent, the range of possible interpretations of the term "suspicion" consists in establishing a mechanism under which a body is charged with providing more specificity to the term. This has been done in Luxembourg, where the *Commission de Surveillance du Secteur Financier* (*CSSF*) has issued a circular that contains a set of indicators that is intended to specify the reporting obligation.[78] The indicators are similar to the 39 indicators of money laundering issued earlier by the Swiss Federal Banking Commission under a provision of the Anti-Money Laundering Law dealing with the detection of high-risk transactions.[79] In Lithuania, decisions of

---

[75] *Loi fédérale concernant la lutte contre le blanchiment d'argent dans le secteur financier du 10 octobre 1997* (Federal Act on the prevention of money laundering in the financial sector of October 10, 1997), Article 9, par. 1 [Switzerland].

[76] Financial Transaction Reports Act 1988 (as amended), Section 16 (1) (b) (ii) [Australia].

[77] In the European context, questions have been raised as to the extent to which such provisions are consistent with an appropriate division of labor between the financial institutions and the FIU. A recent report referred to the perceived requirement in legislation for suspicions to be "well-grounded" or "very well-grounded" and commented that "it is primarily for the competent authorities themselves [i.e., the FIUs] to establish whether the suspicion is such as to require further investigation by the police. The wording of some legislation might give the impression that employees of credit and financial institutions might have some form of investigative role. States should be careful in drafting or reviewing their legislation, that they do not, inadvertently, appear to create additional hurdles for credit and financial institutions to overcome before reporting" (Council of Europe, European Committee on Crime Problems, Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures, *A Review of the Anti-Money Laundering Systems in 22 Council of Europe Member States, 1998–2001*, par. 149).

[78] Circulaire IML 94/112 dated November 25, 1994, annex I [Luxembourg].

[79] *Ordonnance de la Commission fédérale des banques en matière de lutte contre le blanchiment d'argent du 18 décembre 2002* (Ordinance of the Swiss Federal Banking

(continued)

the government set out criteria clarifying what "suspect" transactions are.[80] In other countries, for example Canada,[81] the FIU has issued guidelines, which are not part of the law or regulations, and are not binding, to assist reporting entities in detecting suspicious transactions.

Other jurisdictions have avoided using the term "suspicion" and its variants in the law, and have attempted to base the reporting obligation on a more objective criterion. It may be noted in this respect that the EU directive on the prevention of money laundering requires countries to obligate concerned entities and persons to inform the competent authorities "of any fact which might be an indication of money laundering."[82] The Spanish law requires the reporting of "any fact or transaction with regard to which there is an indication or there is certainty that it is related to laundering...."[83]

Another approach that avoids the use of the term "suspicion" as the basis for the reporting obligation is found in the Netherlands, where the reporting obligation is based on the "unusual" nature of transactions. The Dutch law requires persons subject to the reporting obligation to report "unusual" transactions.[84] Under this approach, there is no requirement to link a transaction with a suspected criminal offense; it suffices that the transaction be "unusual." The ministers of justice and finance have joint responsibility for issuing "indicators," if necessary, for each category of transaction, for a period not exceeding six months, after consultation with the FIU. Once approved by the government, the indicators become permanent.[85] The current list of indicators contains generally applicable indicators, as well as indicators related to certain types of transactions, such as life insurance contracts, credit card transactions, and casino transactions.[86]

Commission Concerning the Prevention of Money Laundering dated December 18, 2002), Article 8, and annex [Switzerland].

[80] Decision of the government of May 15, 2003, supplementing government Decision of September 6, 2002 on the approval of the criteria under which a monetary operation is considered suspicious" *Official Gazette*, No. 49-2177, May 21, 2003 [Lithuania].

[81] See, for example, *Guideline 1, Backgrounder*, and, 2003; *Guideline 2, Suspicious Transactions*, both issued March 23, 2003; all guidelines are available on Fintrac's website at *http://www.fintrac.gc.ca*.

[82] Directive 2001/97/EC of the European Parliament and of the Council of December 4, 2001 amending Council Directive 91/308EEC on the prevention of the use of the financial system for the purpose of money laundering, Article 6, paragraph 1(a) [European Union] The criterion is unchanged from the 1991 Directive.

[83] Law 19/193 of December 28, 1993 concerning specific measures for preventing the laundering of capital, Article 3, par. 4 (a) [Spain].

[84] Disclosure of Unusual Transactions (Financial Services) Act of December 16, 1993, Article 9, par. 1 [Netherlands].

[85] *Id*., Article 8.

[86] *List of indicators applicable from January 28, 2002*, available from MOT [Netherlands].

In an "intermediate" approach, both the "unusual" and "suspicious" criteria are used in different steps in the identification of transactions to report. In Colombia, for example, any transaction that is inconsistent with the customer's profile or that falls within a category of objective alerts predetermined by the reporting institution is to be considered "unusual." The transaction is checked further by the reporting institution in order to determine whether it has an economic and legal explanation. If it does not, it is considered "suspicious" and is reported to the FIU.[87]

The 2003 FATF Recommendations leave it to each country to decide on the exact nature of the suspicion necessary to trigger the reporting obligation. Recommendation 13 refers to a financial institution that "suspects or has reasonable grounds to suspect" that funds are related to criminal activity.[88] While the manner in which the obligation is defined varies from country to country, the fact remains that financial institutions, and other reporting entities subject to the know-your-customer standard are in the best position to detect suspicious or unusual transactions.

What is criminal activity for purposes of the reporting obligation?

The basic intent of the reporting obligation, as stated in the 1996 FATF Recommendations, is to provide the FIU with information on transactions involving funds that could stem from criminal activity.[89] The expression "criminal activity" is repeated in the 2003 Recommendations. In practice, however, the range of criminal offenses that constitute "criminal activity"—and thus give rise to an obligation to report a transaction to which they are related—varies from country to country. Although many countries define the obligation by reference to money laundering, others take a different approach. For example, in Belgium, where the predicate offenses are defined very broadly by reference to all crimes,[90] the reporting obligation is limited to cases where the funds are suspected of originating in one of a limited number of crimes.[91]

---

[87] Circular 25 of 2003 of the Superintendency of Banks, Chapter 11, Sections 2.3.1.3 and 2.3.1.4 [Colombia].

[88] In its discussion of the reporting obligation, the *Consultation Paper* draws a sharp distinction between "suspecting" (described as a subjective criterion) and "having reasonable grounds to suspect" (an objective criterion) (paragraph 139). In practice, as the examples mentioned in the text show, the context in which the term "suspect" is used (including any qualifying words and the use of mandatory indicators of suspicion) muddles the distinction somewhat.

[89] FATF Recommendation 15 [1996].

[90] Criminal Code, article 505, paragraph [Belgium].

[91] *Loi du 11 janvier 1993 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme, I* [Belgium].

The 2003 Recommendations have attempted to provide further guidance in this respect. The new Recommendation 13 and its Interpretative Note define the standard for the reporting obligation by reference to the standard for the definition of predicate offenses in the criminalization of money laundering, which is set out in Recommendation 1. The standard for criminalization, in turn, refers to the 1988 Vienna Convention and the Palermo Convention. The Vienna Convention referred only to drug-related offenses as predicate offenses, but the more recent Palermo Convention sets out the general principle that predicate offenses should include "the widest range of predicate offenses" and "all serious crimes," which the convention defines as conduct constituting an offense punishable by imprisonment for a period of at least four years.[92]

Building on the Palermo Convention, FATF Recommendation 1 (2003) states that "countries should apply the crime of money laundering to all serious offenses, with a view to including the widest range of predicate offenses." It also specifies that, at a minimum, the law should include a range of offenses within each of the designated categories of offenses set out in the glossary. The reporting obligation is then defined in Recommendation 13 by reference to a suspicion that funds are "proceeds of criminal activity," which is defined in the Interpretative Notes as "a) all criminal acts that would constitute a predicate offense for money laundering in the jurisdiction; or b) at a minimum to those offenses that would constitute a predicate offense as required by Recommendation 1." The Interpretative Note adds that countries "are strongly encouraged to adopt alternative a. A similar obligation is contained in the International Convention for the Suppression of the Financing of Terrorism, which sets as a standard the reporting of "transactions suspected of stemming from a criminal activity."[93]

Reports of Transactions Related to Terrorism Financing

In addition to the reporting of transactions suspected of money laundering, countries must also ensure that concerned entities report transactions suspected of being related to terrorism. This new standard was established by the adoption of the FATF Special Recommendations on Terrorist Financing in October 2001.[94]

---

[92] Palermo Convention, Article 2 (b) and Article 6, paragraph 2 (a) and (b). The Convention also sets out a special rule for countries that rely on a list of offenses, which are to include as predicate offenses "a comprehensive range of offenses associated with organized criminal groups" (*Id*., paragraph 2(b)).

[93] International Convention for the Suppression of the Financing of Terrorism, Article 18 (b) (see Appendix IX).

[94] Special Recommendation IV (see Appendix VIII).

Most countries have implemented this standard by amending the law in which the reporting obligation is contained. In some countries, such an amendment may not be necessary. This would be the case when the reporting obligation was worded in broad enough terms—for example, in cases where it refers to transactions suspected of being related to any criminal activity and the financing of terrorism is a crime in that jurisdiction. By contrast to money-laundering transactions, terrorism financing transactions are illegal not because of the criminal origin of the funds, but in view of the criminal intent with which they are carried out. Training may be necessary to ensure that reporting entities detect such transactions, which often appear "normal," except for their illicit objective.

Reports of Transactions Above a Specified Amount

Before suspicious transaction reports became the international standard, countries with money-laundering prevention systems relied on the analysis of large transactions to detect criminal activity. Large transaction reports are still valued in some jurisdictions as an additional source of data that can yield intelligence and also as a means of reconstructing the "money trail" once suspicious activity is detected and criminal investigations are undertaken.[95]

A number of countries have implemented such a system. In the United States, financial institutions must report all cash transactions above $10,000 to a central location supervised by FinCEN (unless exempted).[96] Starting in January 2003, Canada implemented a system under which cash transactions above a specified amount (CAN$10,000) are to be reported.[97] Reports are made to the Canadian FIU. International wire transfers above the same amount must also be reported.[98] A similar obligation exists in Australia, where cash dealers must report cash transactions to which they are a party involving currency (coin or paper money) of the equivalent of AU$10,000 or more and all international wire transfers.[99] A transaction may be reportable as being both suspicious and above the threshold amount.

---

[95] FATF Recommendation 19 states that countries should consider "the feasibility and utility of a system where banks and other financial institutions and intermediaries would report all domestic and international currency transactions above a fixed amount, to a central agency with a computerized database, available to competent authorities for use in money laundering or terrorist financing cases, subject to strict safeguards to ensure proper use of the information."

[96] The reporting obligation is contained in a regulation, 31 CFR 103.22, issued under the authority of the Bank Secrecy Act (31 U.S.C. 5311 *et seq.*) [United States].

[97] Proceeds of Crime Money Laundering and Terrorist Financing Regulations, Section 12. (1) and others [Canada] This reporting obligation came into effect on January 31, 2003.

[98] *Id*. The obligation to report wire transfers was phased in during 2002 and 2003.

[99] Financial Transaction Reports Act 1988, Section 7 and AUSTRAC Guideline No. 2 [Australia].

Such systems produce vast numbers of reports and require sophisticated computer equipment, in the reporting entities as well as in the FIU, if they are to be administered effectively. In the United States, the currency transaction reporting system generated more than 12 million reports in U.S. fiscal year 2002.[100] The laws provide for exemptions to be granted for designated financial institutions, government agencies, and established businesses that handle large amounts of cash in the normal course of their work.

Reports of Cross-Border Transportation of Currency and Bearer Negotiable Instruments

A growing number of international instruments encourage countries to implement a system of reporting cross-border movements of currency. FATF Recommendation 19 states that "[c]ountries should consider implementing feasible measures to detect or monitor the physical cross-border transportation of currency and bearer negotiable instruments, subject to strict safeguards to ensure proper use of information and without impeding in any way the freedom of capital movements." The Palermo Convention contains a similar requirement for consideration.[101] The United Nations Convention Against Corruption also contains a similar provision, to which it adds that "such measures may include a requirement that individuals and businesses report the cross-border transfer of substantial quantities of cash and appropriate negotiable instruments."[102] In the Czech Republic, for example, the customs authorities are required to report to the FIU when they ascertain, in the performance of their duties, that valid banknotes, coins, checks, or traveler's checks in an amount exceeding CZK 350,000 (about US$13,000) have been transported.[103]

Data from Other FIUs

One of the most important functions of an FIU is the unfettered exchange of financial data and intelligence with other FIUs. The principles governing the exchange of information between FIUs are set out in the Egmont Group's *Principles for Information Exchange Between Financial Intelligence Units for Money Laundering Cases* and are discussed later in this chapter.[104] Legislation

---

[100] *Use of Currency Transaction Reports, Report to the Congress submitted by the Financial Crimes Enforcement Network on behalf of the U.S. Department of the Treasury*, October 2002, page 2.

[101] Palermo Convention, Article 7, par. 2 (Appendix X).

[102] United Nations Convention Against Corruption, Article 14, par. 2 (Appendix XI).

[103] Money Laundering Act, No. 61/1996 Coll., as amended by Act No. 15/1998 Coll., Article 5 [Czech Republic].

[104] Annexed to the Egmont Group's Statement of Purpose. See Appendix V.

governing the exchange of information between FIUs should allow such exchanges to take place without impediments.

An FIU may receive financial information from a foreign FIUs upon its request, or spontaneously, in the event that a foreign FIU receives financial information, or develops intelligence that it believes may be of interest to the FIU. In the latter case, the receiving FIU will need to analyze the information in the same manner as it analyzes similar information and determine whether the information leads to intelligence concerning illicit activity.

Rules Related to Reporting Entities

Confidentiality of customer information

The officers and staffs of financial institutions are generally subject to a duty not to disclose client-related information that they acquire as a result of their business. Such a duty is usually viewed as an implied condition of the contract between the financial institution and its customer. In some countries, in addition to this duty of discretion, laws establish an obligation of secrecy, the breach of which may lead to the imposition of criminal penalties.[105]

Other laws may reinforce the protection of customer information. This is the case for laws adopted in many countries with the objective of protecting the confidentiality of personal information contained in electronic databases. These laws often restrict the use financial institutions may make of their client information and the circumstances in which they may provide such information to third parties.[106] These various restrictions on the power of financial institutions to disclose customer information must be overcome in order to allow the anti-money-laundering reporting system to function. This is usually done through specific provisions in the laws establishing the reporting obligation. The duty to provide information should cover not only the provision of suspicious transaction reports and other reports but also the institution's duty to respond to further requests for information from the FIU, including requests for relevant documents.

The 2003 FATF Recommendations contain a general provision to the effect that "[c]ountries should ensure that financial institutions' secrecy laws

---

[105] In France, for example, the criminal sanctions for breach of the duty of secrecy apply to directors and employees of "credit institutions" (Code monétaire et financier, article L-511-33) [France].

[106] See the Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data, Strasbourg, January 28, 1981 (Council of Europe, ETS no. 108), and Explanatory Report on the Convention.

do not inhibit the implementation of the FATF Recommendations."[107] The extension of the reporting obligation to certain nonfinancial professions as part of the implementation of the G-8's Gatekeeper initiative has raised difficult issues with regard to the duty of confidentiality that is attached to the exercise of these professions. This is particularly the case for the legal professions, where, traditionally, the requirement of confidentiality has been very strong.

Rules against "tipping off"

To avoid suspect funds being transferred out of the reporting institution and to avoid prejudicing investigations by making suspects aware of them, it is important that reporting institutions not inform account holders and customers of the suspicious transaction reports they provide to the FIU.[108] Such a provision is found in many AML laws and is set out in FATF Recommendation 14.

Immunity of reporting entity and its staff for reports made in good faith

A corollary of the obligation to report suspicious transactions is that a person who makes such a report in good faith should be immune from liability for the legal consequences of having made the disclosure. The FATF Recommendations have made this a standard since 1990.

There are two aspects to this immunity. First, the law requiring the suspicious transaction reports should make it clear that those making the reports are exempt from legal requirements of professional secrecy and confidentiality. Second, persons making the required reports in good faith should also be protected against potential liability to the persons named in the reports, who, if they were to learn of the disclosure, might attempt to recover damages from the persons who made the reports.

Laws on the immunity of reporting entities vary in their scope. The Belgian law is particularly comprehensive in this regard. It states that "No civil, criminal, or disciplinary proceedings may be initiated and no professional sanction imposed upon the institutions or individuals referred to in [the AML law], their employees and representatives who in good faith have provided information pursuant to [the relevant provisions of the AML]."[109] In Liechtenstein, the law addresses the two aspects of the recommendation specifically, as follows: "Anyone who reports to the FIU [...] in accordance

---

[107] Recommendation 4. For a discussion of the conflict between the protection of private information and the reporting obligations of entities subject to the AML law, see Guy Stessens, 2000, *Money Laundering: A New Law Enforcement Model*, (Cambridge, England: Cambridge University Press), pp. 143–45.

[108] The FATF Recommendations have contained a standard to this effect since the original recommendations were issued in 1990.

[109] Law of January 11, 1993 on Preventing Use of the Financial System for Purposes of Laundering Money, Article 20 [Belgium].

with [the law] – and if it is found that such reporting was unjustified – is exempt from any liability, provided that he/she has acted neither intentionally nor with gross negligence. This action of reporting is not illegal within the meaning of the criminal law, provided that the person had no intention of communicating false information."[110] In South Africa, the law also covers the two aspects: "No action, whether criminal or civil, lies against [a reporting person or institution] complying in good faith with a provision of this Act [....]"[111] In the Netherlands, the immunity against liability for damages to third parties is narrower, since it is qualified by the terms "unless, considering all circumstances, it is plausible that no disclosure should have been made."[112]

Form and Contents of Reports to FIU

In some countries, the power to decide on the form and contents of reports is delegated to the FIU. This is the case, for example, in the Netherlands.[113] In Australia, schedules to the law contain the elements that must be reported for each type of reporting entity. Items may be deleted from the schedules or added to them by regulations issued by the government.[114]

In many countries, the reports must be in writing, but provision is also made for making oral reports (for example, by telephone) in the event of an emergency. A written confirmation is usually required after an oral report has been sent.[115] The FIU usually provides a uniform format for reports covering each particular type of institution.

In some countries, reports may be filed electronically. Electronic filing includes not only the automated production of batches of reports sent by electronic means, as many large financial institutions do for reports on high-value currency transactions, but also the ability of reporting persons and entities to file reports by filling out an on-screen form provided by the FIU. In a number of economically advanced countries, the vast majority of reports are filed electronically.

In many of the economically less advanced countries, however, the infrastructure necessary to support the wide use of information technology may not be available. In these countries, reports are routinely filed on paper forms;

---

[110] Due Diligence Act of May 22, 1996, Article 9 (3) [Liechtenstein].
[111] Financial Intelligence Centre Act, 2001, Section 38(1) [South Africa].
[112] Disclosure of Unusual Transactions (Financial Services) Act, Article 13 [Netherlands].
[113] *Id.*, Article 11 [Netherlands].
[114] Financial Transaction Reports Act 1988, as amended, and Schedules 1–4; legally, the Regulations are issued by the Governor General (Section 43 of the Act) [Australia].
[115] See, for example, Law of January 11, 1993 on Preventing Use of the Financial System for Purposes of Laundering Money, Article 12, paragraph 1 [Belgium].

and, if the FIU has the capability, the reports can then be indexed electronically or entered into a local secure database.

In most cases, the information required for suspicious transaction reports includes not only the particulars of the transaction or of the customer but also a statement of the reason or reasons why the transaction is considered suspicious or of the facts that made it suspicious.

Improving Flow and Quality of Reports

To obtain compliance with the AML/CFT reporting obligations, there needs to be in place a set of measures intended to foster improvements in the flow and quality of reports without resort to sanctions, such as awareness raising and training. These awareness-raising and training actions of the FIU or other supervisory agency will be particularly useful when the FIU is being established, when the building of trust between the staff of the reporting entities and the FIU is important. Similarly, these actions can be taken when new sectors become subject to the reporting requirements.

Remedies also have to be in place, however, to ensure that all concerned institutions understand the mandatory nature of the reporting obligation and to be exercised against deficient institutions once other actions have been tried without producing the desired results. The use of sanctions in appropriate cases also serves to make clear to the whole reporting community the determination of the FIU (or other supervising agency) to arrive at satisfactory reporting levels.

Outreach actions

Before sanctions are levied on delinquent entities, a number of other actions may be taken to enhance the quality and flow of reports. One possible approach is to assess the reporting practices of sectors so as to be able to direct training and other outreach activities to the sectors most in need of them. For this purpose, the FIU may analyze basic data on each reporting entity in a sector, the volume of transactions, the market share, the nature of the business, and other factors to arrive at a general estimate of the number of reports each entity could be expected to generate. Then the reporting practice of each sector is monitored; and if the numbers of reports "expected" and received do not match, different actions may be envisaged.

Training programs may be directed at the institutions in the sectors which show the greatest need for improvement. Training may also be directed at sectors that are being added to the list of reporting institutions. The immediate objective of the participation of the FIU staff in training of the targeted sectors would be to foster improved reporting, but it could also be seen as the start of the bilateral relationship between the FIU and the entities in the sector. The quality of reports received from each sector may also be

analyzed.[116] Findings may be reported back to the reporting entities in each sector on either an aggregated basis in sector-wide meetings or individually.

Another tool, used by some FIUs, is to request from reporting entities (based upon a legal requirement) that they report periodically to the FIU on their work on AML/CFT, including statistical data on reports sent to the FIU. The FIU can then check whether the data reported and the reports actually received match. If they do not, the FIU or the supervisory body should go back to the reporting entity and request an explanation for any discrepancy. This system promotes the use of efficient systems by reporting entities to monitor their reporting activities.

Administrative sanctions

After an outreach program has been in place for a certain length of time, the FIU[117] needs to consider the case of entities that fall below the level of reporting of the sector as a whole. In this regard, the difference between failures to report "cash" or other transactions above a set amount and failures to report suspicious transactions should be noted. For the former (or any other reporting obligation based on an objective criterion), there is a factual test to determine whether a transaction should have been reported; for suspicious transactions, a subjective judgment, based on all facts of the case, is involved. Hence the usefulness of internal guidelines on the detection of suspicious transactions.

Where there is a low level of suspicious transaction reports, the examination of a sampling of transactions may reveal to what extent transactions that should have been reported were not. Assuming a high level of unreported transactions is found, the FIU may try to determine whether the reporting entities have followed the applicable guidelines on the detection of suspicious transactions. In this context, individual decisions not to report certain transactions are less important than the pattern they reveal. The decisions not to report should be reviewed along with the analysis that was conducted to determine whether these decisions form part of a pattern of not reporting.

An array of administrative sanctions may be set out in the legislation to deal with non-compliant entities, and the application of the sanction varies according to the gravity of the offense. A typical set of graduated administrative sanctions would include warnings, reprimands, fines of different

---

[116] The Honduran FIU has developed a system to monitor electronically the quality of financial disclosures (i.e., STRs) reported to the FIU by reporting entities. This system has proven to be an effective method to ensure quality control of financial data submitted to and analyzed by the FIU.

[117] The authority to impose administrative sanctions may be given to the FIU or to another supervisory authority. In this section, only the FIU is mentioned to simplify the presentation.

amounts, and ultimately cancellation of the noncompliant entity's authorization to operate. Publication of these sanctions (where this is allowed or required) may contribute to making the reporting community aware that the reporting obligations are enforced.

The procedure to apply administrative sanctions varies from country to country. The FIU or other supervisory authority usually has the power to issue the first level of sanction, such as warnings. In some countries, the FIU is also empowered to levy other administrative sanctions. For example, in the Czech Republic, the FIU is in the ministry of finance, and the minister of finance has the authority to levy certain fines for noncompliance under the AML Act, but if the failures are such as to warrant repeal of a license, the minister must refer the matter to the authority empowered to decide on the repeal of a license.[118] In other countries, the FIU can only initiate the sanction process by referring cases to a supervisory authority or an administrative court. This is the case in Belgium, where the FIU lacks sanctioning power and must refer cases to the competent supervisory, regulatory, or disciplinary authorities for sanction. (The minister of finance is the designated authority with respect to entities not falling under the supervision or control of an agency.)[119]

Criminal sanctions

In some countries, breaches of their reporting obligations under the AML law on the part of individuals and corporations constitute violations of the criminal law. Although in both administrative and criminal proceedings, fines can be the penalty imposed upon conviction, there is a very significant difference between administrative and criminal proceedings. First, in the case of criminal sanctions, if the criminal law so provides, failure to report may lead to imprisonment in addition to fines or as an alternative to fines. In any case, criminal convictions leave a permanent mark on the record of an individual, and, under the "fit-and-proper" test in force in many countries, may result in the person being barred from managing a financial institution or becoming a member of the board of directors of such an entity. In addition, criminal proceedings often bring with them considerable negative publicity for the firm and the individual, which may have negative commercial consequences. It may also be noted that criminal convictions may be more difficult to obtain under the same set of facts, since the criteria for conviction (i.e., proof beyond a reasonable doubt) is higher than the one usually applied in administrative proceedings (i.e., preponderance of evidence).

---

[118] Act No. 61 Coll., Chapter 3, Section 12 (1), and 13 (1) [Czech Republic].

[119] Law of January 11, 1993 on Preventing Use of the Financial System for Purposes of Laundering Money, article 22 [Belgium].

For all these reasons, making breaches of reporting obligations and of similar obligations subject to criminal sanctions should be considered with care. Some countries have criminalized many types of conduct in breach of the reporting entities' AML/CFT obligations. This is the case, for example, in South Africa.[120] In other countries, attempts have been made to limit the conduct subject to criminal sanctions to cases where circumstances are such that the breach can be seen as the result of gross negligence. For example, in Monaco, a person who "in clear disregard of his professional duty of care as set out in the [AML law] and its implementing regulations" contravenes the provisions on reporting suspicious transactions (including transactions not carried out on grounds of AML/CFT suspicions) is liable to criminal prosecution leading to the imposition of fines.[121]

Analyzing Reports

The second element of the core functions of an FIU, as defined by the Egmont Group, is the analysis of reports received from reporting entities. The purpose of the analysis is to establish whether the data contained in the reports, substantiated as necessary by the FIU, provide a sufficient basis to warrant transmitting the file for further investigation or for prosecution (as the case may be). It should be noted, however, that in practice, the line that separates the analysis performed by the FIU from the investigations performed by the law-enforcement authorities may not be drawn in the same way in all countries and may also vary, depending on the type of FIU involved

The number of reports FIUs receive varies considerably from country to country. In some cases, the volume of reports may be too large for the FIU to be able to analyze all of them in a timely fashion. In such cases, the FIU may use internal criteria to prioritize reports and deal only with the most important ones. In most circumstances, suspicious transaction reports and communications from other FIUs receive higher priority than reports based on the amount of the transaction. Reports that are not immediately analyzed, however, may prove valuable later in the analysis of priority reports and provide useful data in performing operational or strategic analysis. Many FIUs store this "sleeping data" for later use and report using it after some months or years, when new reports are received and matched with this stored data.

The analytical process starts with the receipt of a report, continues with the collection of additional related information, goes through different forms of analysis, and ends with either a detailed file concerning a money-

---

[120] Financial Intelligence Center Act, 2001, Sections 46-71 [South Africa].

[121] Law No. 1253 of July 12, 2002 amending Law No. 162 of July 7, 1993 on the participation of financial entities in combating money laundering, article 32 [Monaco].

laundering (or financing of terrorism) case that is forwarded to the law-enforcement authorities or prosecutors or the reaching of a conclusion that no suspicious activity was found. After the analysis is performed, the primary report that triggered it may represent a small part of the file.

As soon as the data received exceed a certain volume, electronic means of storing it and analyzing it are required. Otherwise, retrieving the data and analyzing it become too time-consuming and the analysis may not be as thorough. The ability to quickly analyze data is vital for a system of countering the laundering of the proceeds of crime, and computerized databases and analytical tools are an important element in achieving this goal. Nevertheless, it is important to keep in mind that electronic databases and software can only facilitate the work of analysts, not replace it.

For purposes of presentation, it is useful to distinguish between different levels of intelligence produced in an FIU. Three levels are generally identified: tactical, operational and strategic.[122] Each has its uses, and none is intrinsically more valuable than the others. The three levels of analysis are complementary, and it is beneficial for an FIU to undertake all three.

Tactical Analysis

Tactical analysis is the process of collecting the data needed to build up a case establishing wrongdoing and the accompanying facts that clarify the reasons behind the commission of a criminal offense. Tactical analysis produces tactical information. Although tactical analysis may be performed on all incoming reports, it is likely that suspicious transaction reports will provide the most directly useful leads, and the description that follows is based on the analysis of such reports.

Tactical analysis includes the matching of data received from reporting institutions with data held by the FIU or accessible to it, including lists of names, addresses, phone numbers, and data in the other reports forwarded by the reporting institutions. Some reporting institutions may produce the simplest form of tactical information themselves, by adding to their reports related information on the reported client or transaction that they have in their databases.

Upon receipt of a suspicious transaction report, the analyst will look for additional information on the subject, the company, the transactions, or other elements involved in a particular case to provide the basis for further analysis. The main sources of such additional information are briefly described below.

---

[122] Some FIUs consider tactical and operational intelligence as one level.

The FIU's own data

The analyst will check the data in the report against information in the FIU's internal sources, such as data from earlier suspicious transaction reports, cash-transaction reports, and cross-border-transfer reports (if applicable). For this purpose, the newly received data are broken down into components that are checked against the sources previously mentioned. When a component is matched with existing data, this information is added to the compiled data on the case. After additional data are collected, one may start using the term "case," which may relate to many individual transactions.

Publicly available sources

The information will be checked against data in publicly available sources, such as company registers and company status or business reports and credit reports issued by private companies, audit companies, and accounting bodies. Even telephone registries are sometimes good sources of information.

Government-held databases

Checks will also be performed on data held in governmental databases. Such data would usually include tax records, company-formation records, police records, immigration and customs records, vehicle registries, and supervisory findings. It is vital that these data be available as quickly as possible, and on a real-time basis as much as possible. Ideally, an FIU would be able to access these databases directly through electronic means, based on a law, a regulation, or an agreement between the agencies concerned. Some of the data might, in fact, be part of an FIU's internal database.

Additional information from original reporting entities and other entities

If necessary, the analyst may go back to the primary information source—that is, the financial and nonfinancial institutions that provided the initial reports, if this is permitted, to request additional information from them (if necessary). It is also very useful if the FIU is authorized to seek information from other institutions subject to the AML/CFT reporting obligations that may have been involved in related transactions or business of the suspicious customer, even if they have not provided reports on them.

Other FIUs

After completing the initial checking of the new data against these national sources, and establishing grounds of suspicion for money laundering or related offenses, the FIU may, when international elements are involved, request additional information from foreign FIUs or other counterparts.

Operational Analysis

Operational analysis consists of using tactical information to formulate different hypotheses on the possible activities of the suspect to produce operational intelligence. Operational analysis supports the investigative process. It uses all sources of information available to the FIU to produce activity patterns, new targets, relationships among the subject and his or her accomplices, investigative leads, criminal profiles, and—where possible—indications of possible future behavior. One of the techniques of operational analysis used in some FIUs is financial profiling. This provides the analyst with methods for developing indicators of concealed income of an individual, a group of individuals, or an organization. It is an effective indirect method of gathering, organizing, and presenting evidence related to the financial status of subjects. The relevance of the profile is to show that the target cannot demonstrate a legitimate source for the difference between his or her outflow of cash and his income. The tracing of a person's assets may also provide leads linking the subject with predicate offenses.

Through operational analysis, the information received by the FIU is developed into operational intelligence, which can be transmitted to law-enforcement agencies or prosecutors for further action. In order to ensure that its tactical and operational analyses are relevant, the FIU should monitor the extent to which its work contributes to successful prosecutions.

Strategic Analysis

Strategic analysis is the process of developing knowledge ("strategic intelligence") to be used in shaping the work of the FIU in the future. The main characteristic of strategic intelligence is that it is not related to individual cases, but rather to new issues and trends. The scope of any strategic analysis may be narrow or wide, as required. It may consist of the identification of evolving criminal patterns in a particular group or the provision of broad insights into emerging patterns of criminality at the national level to support the development of a strategic plan for the FIU.

Strategic intelligence is that which is developed after all available information has been collected and analyzed. It requires a wider range of data than operational analysis, as well as experienced analysts. The data come from reports provided by the reporting entities, the FIU's own operational intelligence and tactical information, public sources, and law-enforcement and other government agencies. The analyst may conclude from the data that, for example, an unusual pattern or volume of transactions is emerging in a certain financial sector or in a certain region. Such findings may form the basis for further actions of the FIU or the law-enforcement agencies. At a broader level, strategic intelligence may suggest the need to impose reporting and other AML/CFT obligations on new entities. Depending on the circumstances,

strategic intelligence may be shared with other law-enforcement agencies, as well as with the government agencies charged with the development or coordination of anti-money-laundering policy.

Disseminating Reports

The third core function of an FIU is the dissemination of the information it has received and the sharing of the results of its analysis. The ability of an FIU to quickly share reliable financial intelligence and related information with domestic and foreign authorities is critical to the success of its mission. Since funds move quickly in and out of financial institutions and across national boundaries, FIUs must be able to provide, as rapidly as possible, financial information to competent authorities for purposes of criminal law-enforcement work. The ability of FIUs to share valid information quickly affects not only the effectiveness of a country's internal AML/CFT regime but also its ability to cooperate internationally.

There are three aspects to the dissemination function of FIUs. The first two are related to exchanges of information inside a country, and the third is related to international exchanges. The first concerns the duty of the FIU to transmit information to the competent authorities for further investigation or prosecution whenever its analysis reveals money laundering or other criminal activity. The second concerns the exchange of information between the FIU and domestic agencies other than the ones to which files are transmitted for further investigation or prosecution. The third is the international exchange of information, mainly, but not exclusively, from FIU to FIU.

Transmitting Reports for Investigation or Prosecution

When an FIU concludes its analysis of a suspicious transaction or series of transactions with a finding that they reveal criminal activity (as defined in the FIU law), it is the duty of the FIU to transmit the results of its analysis to the competent authorities for further investigation or prosecution.[123] The decision as to which authority will receive the information depends on the legal system of the country involved. In some systems, the information is transmitted to the police, so they may carry out the investigations that will result in a file ready to be transmitted to the prosecuting authorities for prosecution. In other systems, the file is transmitted directly to the prosecuting authorities, which will order

[123] Some FIUs, such as those in Norway, Denmark (both "police/judicial"-type FIUs), and Luxembourg (a prosecutorial-type FIU), have the power to prosecute their own cases. Technically, these FIUs do not "transmit" files for prosecution.

further investigations, if necessary, and, if the evidence is sufficient, will initiate the prosecution.

The law governing the FIU normally specifies the scope of the obligation to send a file for investigation or prosecution, which varies from country to country. In most systems, the scope is fairly narrow, in accordance with the "specialty principle,"[124] under which the information furnished to the FIU by financial and other institutions can be used only for a specifically defined purpose, such as combating money laundering.[125] In Slovenia, for example, the law adopted in 2001 limited the duty to transmit documentation to the competent authorities to cases where the FIU considered, "on the basis of data, information and documentation obtained under the Law" that there existed reasons for suspicion of money laundering.[126] An amendment to the law widened the duty to report to the competent authorities to include cases of corruption and criminal association, as well as all serious crimes subject to a prison sentence of five years or more.[127] In Belgium, the scope of the obligation is narrower: the suspicion has to come from the examination of a suspicious transaction report, and the crimes on which reports may be made to prosecutors are limited to money laundering and terrorism financing.[128] In law-enforcement-type FIUs, the specialty principle may not operate in the same way. For example, in South Africa, an autonomous police-type FIU, the FIU provides the information to an investigating authority, the tax authorities and the intelligence service at the request of such authority, or at the initiative of the FIU if the FIU "reasonably believes such information is required to investigate suspected unlawful activity."[129]

Once the competent law-enforcement authority has received the information from the FIU, the use it may make of it is determined by the law governing the actions of that agency or by general laws of criminal procedure. Often when the prosecutor's office receives information that can lead to

---

[124] For a discussion of the specialty principle, see Guy Stessens, 2000, *Money Laundering: A New Law Enforcement Model* (Cambridge, England: Cambridge University Press), pp. 193–99.

[125] The original European Money Laundering Directive of 1991 contained a provision to this effect; it was deleted in the 2001 amendment (Council Directive 91/308/EEC on the prevention of the use of the financial system for the purpose of money laundering, Article 6, third paragraph [EU].

[126] Law on the Prevention of Money Laundering, entered into force on October 25, 2001, Article 22, paragraph (1) [Slovenia].

[127] Law on the Prevention of Money Laundering, amendment entered into force on July 20, 2002, Article 22, paragraph (3) [Slovenia].

[128] The law requires that a file be transmitted to the prosecutor's office "as soon as the examination of [a suspicious transaction] report reveals a serious indication of money laundering or financing of terrorism." Law of January 11, 1993 on Preventing Use of the Financial System for Purposes of Laundering Money, Article 16 [Belgium].

[129] Financial Intelligence Act, 2001, Section 40(1)(a) [South Africa].

criminal charges against an individual or corporate entity, the prosecutor's office is free to use the information as it sees fit and to determine, on the basis of all relevant factors, what criminal charges will be made.[130]

Sharing Information with Other Domestic Agencies

In addition to transmitting files for investigation or prosecution, FIUs may also be in a position to assist other agencies in the country to accomplish their mission by providing them with useful financial information. Among the main potential recipients of FIU intelligence are financial sector regulators and supervisors. The ability of the FIU to provide this assistance depends on the laws that govern the use the FIU can make of the information it obtains. Box 9 sets out the agencies with which an FIU may share information.

Box 9. Sharing Information with Other Domestic Agencies

FIUs provide information to domestic agencies, and receive information from them, as follows:

- Banks, money remitters, and other financial institutions provide suspicious transaction reports; they may provide other reports, and receive feedback from, the FIU.
- Financial regulators may report to the FIU financial information, including suspicious transactions found in the course of their supervision of financial institutions, and may receive financial intelligence and information on breaches of anti-money-laundering laws on the part of entities subject to their jurisdiction from the FIU.
- Police and prosecutors provide law-enforcement information to the FIU and receive financial intelligence (in police FIUs, the FIU function and the law-enforcement function are integrated in a single agency) from the FIU.
- Other government agencies (e.g., company registrars and motor-vehicle-registration offices) provide raw data to the FIU.
- Tax authorities, anti-corruption agencies, customs and excise agencies, and intelligence agencies may, if legislation allows, receive financial intelligence from the FIU and provide information to the FIU.

[130] If some of the information involved was received from a foreign FIU, its use may be restricted by the agreement governing the exchange of information between the two FIUs.

In most systems, the law determines the agencies with which the FIU may share information and the uses the receiving agency or agencies may make of the information. The law governing the FIU may state that the FIU will provide financial information, for the purpose of prosecution, to the prosecutor's office and, in addition, will exchange information with specified financial regulators and supervisors. For example, in South Africa, the law lists the country's law-enforcement, tax, and intelligence agencies, as well as the financial supervisory bodies, as recipients of FIU information.[131] Once another agency has received information from the FIU, the law governing the agency will normally specify what uses the agency may make of the information. In particular, these laws (for example, the laws governing the conduct of financial regulators) will normally contain strict confidentiality requirements similar to those applying to the FIU and its staff. As a result, the receiving agency will be able to share the received information only to the extent permitted by law.

In contrast to transmittal of files to prosecutors or investigative agencies, which concern criminal matters, transmittals to financial supervisors or regulators and other government agencies may involve statistics, administrative matters, or civil cases. For example, a financial regulator or supervisor investigating a subject for misconduct that does not constitute a crime but for which an administrative sanction or civil penalty may apply, may need financial intelligence held by the FIU to support its case.

In determining the agencies that will be authorized to receive financial information from the FIU, legislators must weigh the privacy rights of individuals against the needs of domestic agencies for timely financial information.[132] Legislators must ensure that their national FIU is authorized to share information with the relevant institutions or agencies engaged in the fight against money laundering and terrorist financing. At the same time, they will impose safeguards to protect the sensitive financial information that an FIU acquires from being disclosed to unauthorized persons.[133]

As, over time, financial institutions report more and more financial disclosures to FIUs, and the consumers of financial intelligence expand their requests for information from FIUs, FIUs have to equip themselves to meet the increased demand for their services. Since the resources of the FIU may not increase at the same rate as the demand for its services, FIUs may need to find effective ways to share information with appropriate domestic authorities.

---

[131] Financial Intelligence Centre Act (2001), Section 40(1)(a), (d) [South Africa].

[132] Paul Allan Schott, 2003, *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism,* pp. VII-13–14.

[133] Safeguards typically include a duty imposed on FIU personnel not to disclose financial information outside of their normal duties.

In many countries, the FIU exchanges information with other local agencies on the basis of the legislation and regulations authorizing such exchanges. In some countries, FIUs have used memoranda of understanding or similar documents to make more detailed arrangements for exchanging information authorized by law with other agencies with which they exchange information on a regular basis. These memoranda of understanding set out the terms under which the FIU will entertain requests, the conditions for using FIU information, and any other conditions upon which the parties agree. These written arrangements are an excellent way to ensure that the parties understand the rules for exchanging and using financial intelligence, even though they are unenforceable at law. Box 10 outlines the steps involved in requesting financial information from a FIU.

Box 10. Requesting information from an FIU

Requesting financial information from an FIU involves the following steps:

Step 1. A domestic agency (i.e., a financial supervisor or law-enforcement agency) or a foreign FIU makes a request for financial information to support a case involving money laundering, terrorist financing, or related crimes.

Step 2. The requested FIU determines whether the request satisfies legal, policy, and operational requirements. If so, the FIU searches its databases and files for information responsive to the request.

Step 3. If necessary and appropriate, the FIU seeks information from other government agencies and financial institutions to respond to the request.

Step 4. The FIU analyzes the information and prepares a report to share with the requesting agency or FIU and determines the conditions under which the requesting agency or FIU may use and disseminate the information contained in the report.

International Information Sharing[134]

Comprehensive and effective AML/CFT regimes must allow for FIU-to-FIU information exchange that support international cooperation.[135] At the

[134] For other discussions of this topic, see Guy Stessens, 2000, *Money Laundering: A New Law Enforcement Model* (Cambridge, England: Cambridge University Press), Part IV; and Paul Allan Schott, 2003, *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism*, Chapter VIII.

[135] FATF Recommendation 40 (2003) states, in relevant part, that "[c]ountries should ensure that their competent authorities provide the widest possible range of international cooperation to their foreign counterparts....Where the ability to obtain information sought by a foreign competent

(continued)

international level, FIUs share financial intelligence with other FIUs to support the analysis of STRs and intelligence gathering. With FIU-to-FIU information sharing, FIUs, domestic law-enforcement agencies and other domestic "consumers" of financial intelligence are able to seek and obtain information promptly from foreign governments to deter, detect, and prosecute money laundering, terrorist financing, and related crimes. The international FIU-to-FIU network facilitates the rapid exchange of financial intelligence across borders—a process that usually occurs faster through FIUs than through other government information-sharing channels.[136] It should be noted that although information exchanged between FIUs facilitates the development of financial intelligence, it cannot be used as evidence in criminal proceeding without the express consent of the providing FIU. Countries usually provide evidence to be used in criminal cases through mutual-judicial-assistance procedures, which tend to be time consuming. However, FIU-to-FIU exchanges of information should not be used as a substitute for them.

The Egmont Group has stressed the importance of the unfettered sharing of information between FIUs. Its *Principles for Information Exchange Between Financial Intelligence Units for Money Laundering Cases* are discussed later on, at the end of the subsection on "International Information Sharing."[137] Legislation governing the exchange of information between FIUs should allow such exchanges to take place without impediments.

Most international exchanges of financial intelligence are organized in a "symmetrical" way: each agency communicates with its counterparts of the same type abroad. In addition, some FIUs, including the ones in Austria, the Cayman Islands, Denmark, Slovenia, and Venezuela, have the authority to exchange financial intelligence with foreign law-enforcement agencies. Some FIUs, such as Slovenia's,[138] are authorized to share financial intelligence with international organizations, which would include Interpol,[139] Europol,[140] or the European Union's Anti-Fraud Office (OLAF).[141]

---

authority is not within the mandate of its counterpart, countries are also encouraged to permit a prompt and constructive exchange of information with non-counterparts...."

[136] See *Information Paper on Financial Intelligence Units and the Egmont Group*, p. 1, available at *http://www.egmontgroup.org*.

[137] The text is annexed to the Egmont Group's Statement of Purpose. See Appendix V.

[138] Law on the Prevention of Money Laundering, as amended to July 2002, Article 21 [Slovenia].

[139] International Criminal Police Organization (ICPO-Interpol).

[140] European Office of Police (Europol).

[141] European Anti-fraud Office (OLAF).

Legal basis for exchanges of information between FIUs

An FIU's ability to share information with its counterparts and other agencies in foreign governments is determined by law or statute. Many countries authorize their FIU to exchange information with other FIUs to combat money laundering and related crimes. Following the terrorist attacks of September 11, 2001, more and more countries have authorized their FIUs to share information related to not only money laundering but also terrorist financing. For member countries of the European Union, the Decision of October 17, 2000 sets out detailed rules concerning the exchange of information between members' FIUs.[142]

Most countries provide their FIU with authority to exchange information with other FIUs of any type. Given the importance of information sharing among FIUs, and the work of the Egmont Group in this respect, the trend is toward enhancing FIUs' ability to cooperate with their counterparts that abide by international FIU information-exchange principles. Indeed, a large number of FIUs members of the Egmont Group have undertaken to exchange information with other FIUs in accordance with the Egmont Group's model memorandum of understanding—that is, free exchange of information for purposes of analysis at the FIU level and no dissemination or further use of the information for any purpose without the previous consent of the supplying FIU and protection of the confidentiality of the information.

Some FIUs are authorized by law to exchange information with other FIUs without the need for an agreement between them. In other countries, as a matter of law or policy, the FIU exchanges information with other FIUs with which it has entered into a Memorandum of Understanding (MOU). MOUs set out the terms and conditions under which they share financial intelligence and other financial information with other FIUs. A typical MOU identifies the parties, the type of information eligible for information sharing, the limits on the use of any shared information, and restrictions on redissemination of shared information. The Egmont Group developed a model MOU for FIU-to-FIU information sharing.[143]

MOUs are designed to support information exchange. While an MOU is unenforceable in a court of law, it carries with it a moral obligation to live up to the terms of the arrangement. If a party disagrees on the interpretation or application of the MOU by the other party, the parties typically will attempt to resolve the problem among themselves. If, after discussion, they are

---

[142] Council Decision of October 17, 2000 concerning arrangements for cooperation between financial intelligence units of the member states in respect of exchanging information.

[143] Some FIUs prefer to enter into exchanges of letters rather than MOUs. An exchange of letters can contain the same substantive provisions as an MOU.

unsuccessful, they may choose to mediate the issue with the help of a third party,[144] amend the terms of the MOU, or terminate the MOU. Since an FIU's reputation is paramount to its ability to participate effectively in the FIU network, an FIU that is known to breach the terms of information sharing will have difficulty finding FIUs willing to share their sensitive financial information with it.

Historically, a few countries have required that there be a formal agreement with another country before the respective FIUs could share financial intelligence. Countries that require a formal agreement to be authorized by the ministry of foreign affairs or other senior government official before their FIU can exchange information with other FIUs place their FIU at a distinct disadvantage in terms of its effectiveness as a partner in the international fight against money laundering and terrorist financing, because most FIUs do not require formal agreements to share information. Countries with such a requirement may not be in a position to offer other countries "the widest possible range of international cooperation to their foreign counterparts," as called for by FATF Recommendation 40.

Exchange of information

Most requests for financial intelligence via the FIU network are made in writing. The requesting FIU sends a request to another FIU, either by letter or by filling out a request form. Requests are transmitted either on paper or electronically. Some FIUs send requests to each other via secure networks shared by them, such as the Egmont Secure Web or, for European Union FIUs, FIU-NET (see Box 11). In urgent cases, FIUs will request information orally. If the receiving FIU accepts such a request, it will normally ask the requesting FIU to follow up with a request in writing.

FIUs have developed request forms to meet a specific need to standardize international requests. Sometimes a requesting FIU fails to supply sufficient information about the underlying case, the type of information sought, the intended use of the information, or the potential users of the information. When this happens, the receiving FIU needs to ask the requesting FIU to supply the missing information. This can result in delays in processing the request. To avoid these delays, the Egmont Group developed a Request for Research form for FIU-to-FIU requests for information on money-laundering cases. Egmont encourages its members to use the form to standardize FIU-to-FIU exchange of information requests.

---

[144] Egmont FIUs are able to resort to the Egmont Committee for assistance in mediating information-sharing problems between them.

Box 11. FIU.NET

The FIU.NET is a computer network through which participating financial intelligence units exchange information in a quick and safe manner. As of May 2004, 16 FIUs from member states of the European Union share financial intelligence via FIU.NET.

The origin of FIU.NET can be found in the invitation issued in October 2001 by the Joint ECOFIN/JHA Council (i.e., the European ministers of finance, justice, and home affairs) to the member states to set up a system for the exchange of financial intelligence information by automated means. Subsequent to this invitation, the European Commission awarded a grant to the ministry of justice of the Netherlands to advance FIU.NET and undertake the development of the required, highly sophisticated electronic connections among the participating FIUs.

In the current implementation of the FIU.NET, there are two basic kinds of information flows, which occur when

- an FIU asks for information by means of a request; or
- an FIU provides an answer to an earlier request.

Guided by the display (screen), the financial analyst of the requesting FIU fills out the frames of the information-exchange scenarios to ask another FIU (the providing FIU) whether a certain subject is known. The requesting FIU sends the request via the network. If the providing FIU knows the subject, and is willing to share the information, it can transmit information in any electronic format to the FIU.NET database of the requesting FIU. Exchanging information thus becomes a quick and relatively simple process.

FIU.NET runs over a private network and is highly secure, protected by firewalls as well as sophisticated encryption and authentication technologies. At each FIU, the hardware comprises servers, firewalls, a Virtual Private Network facility, and one or more client Windows PCs.

The participating FIUs are those of Belgium, the Czech Republic, Estonia, France, Germany, Hungary, Italy, Latvia, Lithuania, Luxembourg, Poland, Slovakia, Slovenia, Spain, the Netherlands, and the United Kingdom.

Special arrangements for terrorist financing cases

In recent years, terrorist attacks have had an important impact on the ways in which FIUs exchange information. In the immediate aftermath of the September 11, 2001 terrorist attacks, the Egmont Group FIUs acknowledged that it was important to agree upon a framework for rapidly and effectively exchanging information related to terrorist financing. Although the Egmont Group FIUs were keen to support the investigation of the terrorists of

September 11, 2001, some FIUs had experienced multiple requests with insufficient details supplied from different agencies within the same government. To minimize the burden on all FIUs, the Egmont Group agreed that any domestic requestor seeking information from the FIU network should seek the assistance of their domestic FIU rather than deal directly with a foreign FIU. In that way, the FIUs would serve as a gateway for requests going to other FIUs, and, given their knowledge of the requirements for information exchange, could accelerate the process.

Egmont Group principles of information exchange in money-laundering cases

The Egmont Group has made the improvement of information exchange between FIUs its priority. In June 2001, it adopted the set of *Principles for Information Exchange Between Financial Intelligence Units for Money Laundering Cases*, and, to underline the importance it attached to them, it appended these principles to its Statement of Purpose as an annex.[145]

The *Principles of Information Exchange* serve as the international standard for information exchange between FIUs. In addition, to address the practical issues that impede the efficiency of mutual assistance among FIUs, the Egmont Group issued a paper on *Best Practices for the Implementation of Exchange of Information between Financial Intelligence Units*.[146]

The principles encourage international cooperation between FIUs in money-laundering cases on the basis of trust and flexibility. They stress that FIUs should be able to provide information to one another at an FIU's request or spontaneously. Information exchanged by FIUs may be used only for the specific purpose for which the information was requested or provided, and may not be transferred to another authority (including for use as evidence in a court case) without the prior consent of the disclosing FIU. In addition, the confidentiality of the information provided should be protected by strict controls and safeguards, and should be considered, at a minimum, as being protected by the same confidentiality provisions as apply to similar information obtained by the receiving FIU from domestic sources.

---

[145] See Appendix V.
[146] Available on the Egmont Group website at *http://www.egmontgroup.org*.

4

OTHER FIU FUNCTIONS

Although all Egmont Group member FIUs have the three core functions of receiving suspicious transaction and other reports, analyzing them, and disseminating the resulting financial intelligence, some FIUs are also entrusted with other functions. Five of these other functions are discussed below: monitoring compliance with AML/CFT requirements, blocking transactions, training of reporting-entity staff on reporting and other AML/CFT obligations, conducting research, and enhancing public awareness of AML/CFT issues.

Some FIUs carry out additional functions. Of particular interest is the gathering and storage of financial intelligence. Although, over the years, many FIUs have accumulated considerable financial information and intelligence in the course of receiving and analyzing suspicious and other transactions, some FIUs have become national, centralized "storehouses" of financial information and intelligence, and have developed programs under which law-enforcement agencies may access this information. FinCEN in the United States provides an example.

Other FIUs, whether formally or informally, have become important advisers to their governmental authorities on many aspects of money laundering and the means of combating it. Such FIUs may provide strategic analyses that will be used in the defining of government priorities in combating financial crime. They may also be particularly well suited to provide drafts of amendments to legislation in support of evolving criminal policy.

It may also be noted that in some countries, the list of FIU functions contained in a law or other document contains additional activities or responsibilities of the FIU that have been discussed elsewhere in this handbook. For example, the issuance of an annual report is sometimes listed as an FIU function.

Monitoring Compliance with AML/CFT Requirements

An AML/CFT preventive system requiring businesses and professionals to identify their customers, keep records, set up internal controls, and report suspicious transactions needs monitoring if it is to be effectively implemented. The mere existence of sanctions is not sufficient to ensure compliance. If no attention is paid to supervision, there is a risk that sectors that resist the requirements will not comply with them or will comply less thoroughly than they should. Regular and thorough supervision enhances compliance. In

addition, a properly functioning supervisory system will have a similar function as feedback: it will contribute to the quality of the information provided to the FIU.

FATF Recommendation 23 sets as a standard that countries ensure that financial institutions are subject to adequate regulations and supervision. The primary goal of the supervisory function is to ensure that institutions are effectively implementing AML/CFT requirements and have put in place adequate measures to control the risk of their being involved in or used for money laundering or the financing of terrorism; it is not to detect instances of money laundering or the financing of terrorism.[147]

AML/CFT Supervision Arrangements

Some countries have given the supervisory function regarding AML/CFT compliance on the part of regulated institutions to the existing supervising or regulating institutions dealing with these institutions. These supervisors and regulators have extensive knowledge of the concerned sectors, can integrate the ML/FT risk in their general risk analysis, and generally have the necessary experience of the supervisory function. These agencies also often have the necessary resources. Such an arrangement is also consistent with the fact that international standards on prudential supervision include AML/CFT supervision.[148]

In countries with a single financial supervisory agency, this supervisor will be the only party involved in ensuring compliance with AML/CFT requirements. For example, in the United Kingdom, one of the statutory objectives of the Financial Services Authority under the Financial Services and Markets Act 2000 is reducing the extent to which regulated firms may be used in connection with financial crime, including money laundering.[149]

In other countries, however, several supervisors can be involved in AML/CFT monitoring: the central bank for banks and other credit institutions; the insurance supervisor for the insurance industry; and the securities supervisors for stock exchanges, brokers, and dealers. In the Czech Republic, AML/CFT supervision of the regulated financial institutions is the responsibility of the Czech National Bank, the Securities Commission, and the

---

[147] Normally, supervisors who discover facts indicating money laundering in the course of their supervision are under an obligation to notify the FIU and may also initiate related sanctions.

[148] See the subsection of Chapter 2 on "Core Principles of Financial Sector Supervision." Explicit legal authority may be needed for the regulator or supervisor to undertake AML/CFT supervision if the AML/CFT requirements are not included in the general law governing the supervised institutions.

[149] Financial Services and Markets Act 2000, § 6(1) [United Kingdom].

Credit Unions Supervisor; and the FIU is the supervisor for gambling houses, casinos, betting shops, auction halls, real estate agencies, entities offering financial leasing or other types of financing, foreign exchange bureaus, and facilitators of cash or wire transfers.[150]

For reporting entities that do not have a supervisory authority, such as money-remittance services or dealers in high-value goods, there is a need to assign AML/CFT supervision responsibility to a designated agency or agencies. It is possible to designate the FIU for this purpose, as has been done in the Czech Republic. It is also possible to appoint a supervisor whose field of experience is related to the nature of the activities of a nonregulated group or that is particularly well placed to monitor a certain activity. For example, some countries have chosen to have dealers in high-value goods supervised by an investigative agency, such as the Economic Control Agency in the Netherlands, or by the customs administration, as is the case in France and in the United Kingdom. In Poland, the customs authorities oversee the compliance with the reporting obligation related to cross-border transportation of cash and bearer instruments.[151] Such "matching" of industries and supervisors is not always possible, however, and supervision may have to be entrusted to agencies with little relationship to the industry. In the Netherlands, for example, the Dutch central bank monitors the AML/CFT compliance of casinos.[152]

FIU as AML/CFT Supervisor

In some countries, the FIU is responsible for monitoring compliance with the reporting obligation and the other preventive obligations of all institutions covered by the law, whether they are prudentially supervised or not. This is the case, for example, in Australia, Canada, and Spain. An advantage of such an arrangement is that the AML/CFT expertise is concentrated in one supervisory agency, which may improve its efficiency. It should be noted, however, that supervision is a resource-intensive task that requires considerable knowledge of the supervised institutions. If the FIU is to discharge its responsibilities in this regard, it should be granted adequate resources for the purpose, so that this

---

[150] Section 8(3) of Act No. 61 of February 15, 1996, on Selected Measures against Legitimization of Proceeds from Criminal Activities [Czech Republic].

[151] Act no. 61 Coll. of February 15, 1996 on Selected Measures against Legitimization of Proceeds from Criminal Activities and on the Amendment of Related Legislation, as amended to 2000, Section 5, paragraph 8 [Poland].

[152] Disclosure of Unusual Transactions Act, Article 17 (b) and article 8a, paragraphs 1g and 2g of the Execution regulation. The Dutch central bank has long been responsible for the supervision of *bureaux de change*. Since casinos need a license from the central bank to act as a *bureaux de change*, it was decided that the central bank would inspect compliance with AML/CFT requirements in general for casinos.

task can be accomplished without constraining the FIU's ability to carry out its core functions.

In countries where the FIU is responsible for ensuring compliance with the AML/CFT obligations, arrangements are needed to ensure that the FIU and the other supervisors can work together to further compliance.[153] Given the knowledge of the sectors that they derive from their oversight responsibilities, the supervisory agencies can play a significant role in helping to ensure compliance with AML/CFT obligations among the entities placed under their authority.[154]

When a country decides to give monitoring responsibility to the FIU, whether it is for all reporting institutions and professions or some of them, the law must provide the FIU with adequate powers to allow it to perform this function. In particular, the FIU needs the power to not only request information related to all suspicious transaction reports but also to enter the premises of the supervised institutions, to inspect documents and make copies of them, and to share information with other supervisors, including suspected cases of non-compliance with sector standards, both domestic and foreign. In short, all the powers that the traditional supervisors have for inspecting AML/CFT should also be provided to the FIU.

The FIU also needs a clear legal mandate if it is to supervise compliance with AML/CFT obligations. More generally, since the establishment of an FIU with responsibility for supervision of AML/CFT requirements may affect the manner in which existing prudential supervisors and regulators carry out their supervisory tasks under accepted international standards, it is important that careful consideration be given to defining the respective responsibilities of each involved agency and ensuring that the law clearly reflects the intended arrangements.

Information Exchange and Cooperation

No matter what arrangements are made with respect to the primary responsibility for AML/CFT supervision, given the multiplicity of agencies involved, arrangements for cooperation among the concerned agencies are necessary to prevent conflicts and ensure coordination of activities. In particular, when an agency other than the FIU is charged with inspecting institutions in a sector for compliance with the AML/CFT requirements, the supervisory agency needs specific information from the FIU, such as the

---

[153] FATF Recommendation 31 contains a general standard regarding cooperation among policymakers, the FIUs, law-enforcement agencies, and supervisors to combat money laundering and terrorism financing.

[154] FATF Recommendation 29.

frequency, completeness, and quality of reports received from each supervised institution; the typologies most frequently reported; the cities or areas of major concern; and the institutions that seem to warrant closer scrutiny. It is not sufficient for supervisors to review the suspicious transaction reports that have been submitted to the FIU when performing onsite inspections; they will need to cross-check this information with the data received by the FIU. Cross-checking will give insight into the controls of the financial institutions and allow supervisors to perform statistical analysis and, thus, compare the performance of financial institutions.

Since the data received by the FIU are covered by strict secrecy rules, the law needs to lift the secrecy rules to make it possible for the FIU to provide such data to the other supervisors. For instance, in the Czech Republic, the law stipulates that the FIU has the obligation to maintain secrecy; however, this secrecy requirement is not to be imposed on, inter alia, persons performing bank supervision.[155]

In cases where several authorities are involved, it is important that all parties, including the FIU, cooperate to ensure that supervision is equally enforced among the various sectors. This can be done informally by means of regular meetings to exchange experiences. A more formal arrangement based on a law may, however, provide the legal basis for the exchange of information between the concerned agencies. For example, Monaco has created a committee that is in charge of coordinating between the different supervisory agencies involved.[156] Such cooperation mechanisms can help ensure that there is a level playing field among reporting institutions and reduce "regulatory arbitrage."

Blocking Transactions and Freezing Accounts

Even in the best of circumstances, an FIU may not be able to determine instantly whether the transaction referred to in a particular report is related to criminal activity or not and, in the affirmative case, transmit the file to the proper authorities for investigation or prosecution. In some cases, a delay in the start of the criminal proceedings may result in the reported transaction

---

[155] Act No. 61 of February 15, 1996, on Selected Measures against Legitimization of Proceeds from Criminal Activities, Sections 7(2) and 7(4)(a) [Czech Republic].

[156] Sovereign Order 15.530 of September 27, 2002 creating a committee to coordinate the different administrative departments whose remit includes the supervision of financial activities. The committee's task is to organize exchanges of information between the authorities responsible for supervising banking, investment, and insurance activities and the management and administration of foreign legal entities, and to address all issues of common concern relating to coordination of the supervision of the above-mentioned activities [Monaco].

being completed and the funds being lost for law-enforcement purposes. In order to give FIUs time to determine whether a transaction is related to criminal activity or not, some jurisdictions give the FIU the power to block the reported transaction for a limited time. During this period, the FIU can analyze the transaction, and if, after analysis, the conclusion is reached that the transaction is indeed related to criminal activity, the FIU can transmit the file to the proper law-enforcement authorities that have the power to freeze the transaction and the related bank accounts for a longer period.[157]

The power of the FIU in this regard is usually limited to the blocking of a particular suspicious transaction. In a few cases, the FIU has the broader power to freeze an entire bank account or even to seize assets. It should be noted that the power of the FIU to block transactions is unusual in that, in most legal systems, such action can only be taken by either a court or by order of a court.

There is no international anti-money-laundering norm or standard that requires an FIU to have the power to block transactions. A number of international treaties, including the Strasbourg Convention, the International Convention for the Suppression of the Financing of Terrorism, and the Palermo Convention, require that states that are parties take domestic measures for the freezing of suspicious transactions.[158] Similarly, the 2003 FATF Recommendations contain a general statement to the effect that countries should adopt measures to enable their authorities to confiscate criminal property, including allowing them to carry out provisional measures, such as freezing and seizing, to prevent any dealing, transfer, or disposal of such property."[159] Under these instruments, however, the power to freeze may be conferred on authorities other than the FIU; and in many countries, the power is granted to the courts.

In most countries where the FIU has powers of this type, the power is limited to blocking individual transactions reported to it for a maximum period of time set out in the law. A few FIUs have wider powers, including the power

---

[157] There may be instances where, in the presence of a transaction related to criminal activity, the best course of action is not to block the transaction, in order to allow a related investigation to follow its course undisturbed. This is noted in Luxembourg, Cellule de Renseignement Financier (CRF), *Rapport d'activité pour 2001 et 2002*, page 7. In Italy, the FIU may suspend a transaction at the request of investigative authorities, "provided that this will not be detrimental to the course of the investigation and to the current operations of the intermediaries." (Decree Law 143 of May 3, 1991, Article 3, paragraph 6 [Italy]).

[158] See [Strasbourg] Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime, Article 3; United Nations Convention against Transnational Organized Crime, Article 12; and International Convention for the Suppression of the Financing of Terrorism, Article 8.

[159] FATF Recommendation 3 (2003).

to block transactions at the request of a foreign FIU. For example, the Barbados FIU may freeze a bank account for a maximum of five days upon a request of a local law-enforcement authority or a foreign FIU related to an offense over which the FIU has jurisdiction, subject to an appeal procedure on the part of the owner of the account.[160] In Thailand, the "Transaction Committee" of five persons chaired by the head of the FIU has the power to freeze transactions and also seize assets. In an emergency, the head of the FIU can act alone and then report to the Transaction Committee.[161]

Most laws that give blocking power to an FIU give it the authority to block a transactions on its own initiative, usually upon receipt of a suspicious transaction report. In some systems, this authority is more limited. In Italy, for example, the FIU may suspend a transaction only if it is requested to do it by another authority (e.g., by the Bureau of Antimafia Investigation or the Finance Police).[162] In Bulgaria, the director of the FIU initiates the process, but it is formally the minister of finance who issues the blocking order.[163]

The length of the period during which the FIU may block a transaction is a key element in the legislation. The blocking authority is intended to give the FIU time to review the case and determine whether the facts warrant transmitting it to the competent authorities for investigation and prosecution, and to allow these authorities to take measures, within their own powers, to safeguard the assets in question. The length of time required for these steps to be taken may vary from country to country. As Table 1 shows, the periods tend to cluster around a span ranging between 24 and 72 hours—that is 2–3 days. A period longer than three days may be warranted by the local constraints, but a much longer period could cause prejudice to the relationship between the reporting institution and its customer, and could raise questions related to fundamental rights of the account owner. A long period would also increase the risk of the account owner being tipped off.

There are variations on the general trend. For example, in the Czech Republic, a financial institution making a suspicious transaction report may not carry out the reported transaction during a 24-hour period following receipt of the report by the FIU if this would "thwart or complicate the securing of the proceeds." During that time, the FIU may block the transaction for an additional period, which cannot bring the total blockage period to more than

---

[160] Financial Intelligence Unit Act, 2000, Section 4 (2)(c) [Barbados].

[161] Anti-Money Laundering Act, Articles 35, 36 and 48 [Thailand]. The members of the Transaction Committee are selected from the 25 members of the Anti-Money Laundering Board, most of whom are high-ranking civil servants.

[162] Decree Law 143 of May 3, 1991, Article 3.6 [Italy].

[163] Law on Measures Against Money Laundering of 1998, as amended through April 4, 2003, Article 12, paragraph 1 [Bulgaria].

72 hours from the receipt of the report by the FIU, if analyzing the transaction takes longer than the initial 24 hours. In the event that the reporting entity is notified of the start of criminal proceedings, it must wait three days before executing the transaction.[164] In Thailand, the blocking period varies, depending on the factual elements available to the FIU. The delay is a maximum of three days if there is only probable cause that the transaction is linked to money laundering, while it can be as long as 10 days if there is evidence that a transaction is involved or may be involved in the commission of a money-laundering offense.[165]

Table 1. FIU Power to Block Transactions and Freeze Accounts in Selected Countries

Country	Block Transactions	Maximum Time	Freeze Accounts	Maximum Time
Barbados	✓	72 hours	✓	5 days
Belgium	✓	Two working days		
Bulgaria	✓	72 hours		
Croatia	✓	2 hours		
Czech Republic	✓	72 hours		
France	✓	12 hours		
Italy	✓	48 hours		
Luxembourg	✓	Unlimited		
Poland	✓	48 hours		
Slovenia	✓	72 hours		
South Africa	✓	5 days		
Thailand	✓	3–10 days	✓	90 days

The reporting entity should be entitled to know rapidly whether it can execute the requested transaction, and close coordination between the reporting entity and the FIU is needed to ensure that this happens. Laws sometimes contain detailed provisions in this regard. For example, in Belgium, the law requires the entity reporting a suspicious transaction to indicate the time it intends to carry it out. The FIU must "provide immediate acknowledgment" to the reporting entity. If the matter is "serious and urgent," the FIU may notify the entity of its opposition to execution of the transaction before the time mentioned by the reporting entity. This action blocks the transaction for two

[164] Money Laundering Act No 61/1996 Coll. as amended by Act No. 15/1998 Coll., Article 6.2 [Czech Republic].

[165] Anti-Money Laundering Act of B.E. 2542, Articles 35 and 36 [Thailand].

working days from the time of notification of the entity. If the FIU wishes to have this period extended, it must seek authorization from the Crown Prosecutor. In the absence of such a notification, the reporting entity is free to execute the transaction.[166] In other countries, whether to grant an extension may be decided by a court or an investigating judge.[167] In Austria, the reporting entity has the right to demand of the FIU that the latter decide whether there are objections to the immediate execution of a transaction. If no answer is given by the end of the next working day, the entity is free to execute the operation.[168]

What is the next step when a transaction has been blocked? In some systems, the FIU may request a judge to order the blocking or seizure of funds, accounts, or other assets related to the suspicious transaction.[169] Other systems allow the FIUs to request a prosecutor to take the necessary measures.[170] In Estonia, the FIU may refer the case to the courts only to obtain the seizure of the property that is the object of the money laundering.[171]

Training for Staff of Reporting Institutions in Reporting and Other Requirements

Training the staff of reporting entities is an important element of the strategy to enhance the flow and quality of reports. Indeed, under FATF Recommendation 15, financial institutions are responsible for implementing programs against money laundering and terrorist financing that include ongoing staff training. In many countries, it is a function of the FIU to participate in such training.

Training not only provides the staffs of the reporting entities with the information they need to understand the requirements, but it can also contribute to the establishment of a climate of trust between the staffs of the FIU and the reporting entities. This is especially important in the first few years of the FIU's existence, since there may be considerable initial reticence to overcome before satisfactory levels of reporting can be achieved. Training programs may also flag issues in the implementation of the legislation on reporting that can be addressed at a later stage. Finally, training can give staff

---

[166] Law of January 11, 1993 on Preventing Use of the Financial System for Purposes of Laundering Money, Article 12 [Belgium].

[167] See, for instance, Code Monétaire et financier, article 562-5 [France].

[168] Federal Banking Law of 1993, Article 41.1 [Austria].

[169] See for example, Law 90-614 of 12 July 1990, Article 6 paragraph 4 [France].

[170] Law of January 11, 1993, Article 12.3 [Belgium], and Financial Intelligence Sector Act, 2001, Section 34 (1)(b) [South Africa].

[171] Money Laundering Prevention Act of 25 November 1998, Article 18.3 [Estonia].

of reporting entities a sense of purpose and of the importance of the work they perform, which can be a factor in the FIU's obtaining improved reporting.

Training on recognizing suspicious transactions can be done by the FIU staff, external (private) consultants, compliance officers of the reporting entities, or a combination of these. For example, training specialists could be brought in to design the courses and prepare the materials (a task for which there may not be any qualified staff in the FIU), but some of the training sessions could be taught by FIU staff who have the necessary expertise. In many countries, private companies are available to carry out this type of assignment and to provide compliance training more generally. In small countries with no such established private expertise, however, the FIU may be the only source of expertise available locally, and cost considerations may limit its opportunities to seek private expertise from outside the country.

The courses can be tailored to each type of reporting entity, and training programs can be conducted in partnership with their respective professional associations and supervisors. For example, the national association of bankers could organize training seminars for banks, or join the FIU in organizing them or vice versa. National regulators and supervisors with a stake in AML/CFT may also participate in the training programs.

The types of training needed may also vary over time. At the beginning of its operations, an FIU will usually concentrate its training on the basic reporting requirements and general awareness raising. Confidence building is also an important product of such early training. At a later stage, the FIU staff can offer more specialized training that is tailored to specific sectors or even to specific reporting institutions (for the larger ones). Decisions as to which sector or institution will be offered training can be based on their relative sizes and market shares, as well as on recorded discrepancies between expected and actual volumes of reports. Such targeted training programs can focus on specific indicators of suspicious transactions in the selected sector and can be presented with related case studies.

Whatever approach is chosen, FIU staff can offer their unique experience in reviewing reports and following evolving typologies in each key sector as an important contribution to the training of staff in reporting entities. Participation of FIU staff is also desirable if one of the objective of the training program is building trust between the FIUs' staff and the staff of the reporting institutions.

Conducting Research

FIUs conduct research for many reasons and, in particular, as a tool for shaping the FIU's own policy and developing national AML/CFT policy (if the FIU participates in this). In some cases, the legislation specifies that research is

a function of the FIU; in other cases, the FIU carries out the research on the basis of the inherent need for such a function to reach its stated objectives.

Some research projects may make use of the results of strategic analysis of transactions. Depending on the nature of the research project, however, other types of information may be used, including statistical data, case typologies, and developments in the context of AML/CFT. Although research is not the main task of an FIU, the ability to conduct research in the areas of its activities enhances the FIU's ability to carry out its core functions and also provides its management and others with a greater and more objective understanding of the FIU's work.

Enhancing Public Awareness of AML/CFT Issues

In many countries, the establishment of an FIU is received without enthusiasm. The public feels threatened by the potential misuse of their financial data, and reporting institutions worry about the reaction of their customers if they assist the FIU in its work. Trust is not there at the beginning. These problems can be particularly acute for a law-enforcement FIU, since entities that cooperate with the FIU may appear involved in police work and investigations. For administrative-type FIUs, counterpart law-enforcement agencies may not have supported the establishment of the FIU and may be reluctant to work with it once it is established.

Whatever the country or the system, the public needs to be convinced of the value of an FIU as an institution, the importance of its role, and the benefits and protection of the financial system that it offers. No FIU can function well without the trust of the public and the staffs of the reporting institutions.

Trust can be achieved over time through a variety of means. The most important is in the day-to-day, case-by-case cooperation with reporting institutions, where professionalism of the FIU staff can foster a climate of trust. It is important that staff are well trained so that they know how to discuss issues through the appropriate channels and keep in mind the issue of data protection at all times.

Another way to enhance trust and AML/CFT awareness in the public is working with the media. Many FIUs issue information brochures for the public, arrange for staff members to give interviews and publish articles on AML/CFT in magazines and professional publications, and make additional

information available to journalists.[172] One way to engage the media is to publicize success stories (while protecting confidential data and the safety of FIU staff). In some parts of the world, FIU's prefers to keep low profiles, for the sake of security of their staffs. In such circumstances, the FIUs can work with other government agencies and other stakeholders to raise public awareness in an indirect manner.

[172] The MOT, the Netherlands' FIU, issues a newsletter with money-laundering cases and typologies every three months; the OMLP, the Slovenian FIU, prepares articles for professional publications of various sectors (banking, securities, insurance, etc.); its staff are interviewed by daily newspapers; and it also offers statistical data about its work to a broader spectrum of the media at an annual press conference; other FIUs also engage in similar practices.

5

ENHANCING THE EFFECTIVENESS OF FIUS

Once an FIU is established and has been functioning for a while, it becomes necessary to assess its effectiveness as well as that of the country's entire AML/CFT system. Such assessments should be conducted periodically to ensure that the FIU and the system as a whole are continuously striving to improve their effectiveness. This is consistent with good public sector management policy and is now also an FATF standard.[173]

Over time, an effective AML/CFT system's objective would be to significantly reduce occurrences of money laundering and the financing of terrorism. This would be the result of the preventive and repressive components of the system working in the most effective manner (and assuming a certain degree of stability in the external environment, such as basic criminality patterns and the amount of cooperation received from other countries). Before a definite downward trend can be set in motion, however, fluctuations will be observed in the statistics. The number of suspicious transactions reported, the number of cases prosecuted, and other data will vary from year to year, as know-your-customer obligations are placed on financial and other entities, reporting obligations are fine-tuned, prosecuting authorities acquire expertise in financial crime, and, it must be added, criminals adjust their methods to take into account the new environment.

To attain the maximum degree of effectiveness, all agencies involved—from the reporting entities to the judiciary authorities—need to increase their own effectiveness and to cooperate with each other to form a well-functioning whole. It follows that each component of the system needs to be assessed in terms of its efforts to achieve what is expected of it, even if it is only one part of the total system.

Analyzing the effectiveness of an FIU is not an easy task, given the linkages between its operations and those of the other elements in the

[173] FATF Recommendation No. 32 (2003) reads as follows: "Countries should ensure that their competent authorities can review the effectiveness of their systems to combat money laundering and terrorist financing systems by maintaining comprehensive statistics on matters relevant to the effectiveness and efficiency of such systems. This should include statistics on the STRs [suspicious transaction reports] received and disseminated; on money laundering and terrorist financing investigations, prosecutions and convictions; on property frozen, seized and confiscated; and on mutual legal assistance or other international requests for cooperation."

AML/CFT system. For example, deficiencies of FIU intelligence might not be attributable to the FIU itself, but to a weakness in other parts of the system. Similarly, the FIU's output depends, in large part, on the quality of information it receives from reporting institutions, and the FIU can influence such quality only to a limited extent, through training, feedback, and guidance to reporting institutions.[174] Also, any bottlenecks at later stages of the process, such as a lack of expertise on financial operations on the part of law-enforcement agencies or the judiciary, may limit the impact of the FIU's work. An additional source of difficulty in many countries is the lack of a coherent statistical framework covering the different parts of the system.

The international development of criteria and methods to assess the effectiveness of FIUs is at an early stage. So far, the FATF has established as a standard the principle of periodic reviews of the effectiveness of the AML/CFT system, including the FIU, based on a coherent set of statistics maintained by the concerned authorities. The actual reviews of the effectiveness of the FIUs are to be performed by the FIUs themselves or their governing authorities, using such methods as they believe are appropriate.

Collecting Relevant Data

The first step in assessing the effectiveness of an FIU is the collection of data related to the inputs it receives and the FIU's outputs. Generally, to paraphrase Recommendation 32, competent authorities should maintain comprehensive statistics on matters relevant to the effectiveness and efficiency of the AML/CFT system, including statistics on the suspicious transaction reports (STRs) received and disseminated; on money-laundering and terrorist-financing investigations, prosecutions, and convictions; on property frozen, seized, and confiscated; and on mutual legal assistance or other international requests for cooperation.

A more detailed, but not exhaustive, list limited to the operations of the FIU would be as follows:[175]

- STRs received—total and breakdown by
    - type of entity making the report (financial institution, designated nonfinancial businesses and professions);

---

[174] An FIU with supervisory powers over AML/CFT matters would, of course, have greater power (and responsibility) to improve the quality of the information it receives from reporting entities.

[175] The list is illustrative only. It includes elements that are set out in the assessment methodology associated with Recommendation 32 and others.

  - STRs analyzed, disseminated, and sent for investigation or prosecution;
  - content, region of origin, amount of currency, possible crimes involved, complexity, etc.;
  - STRs actually analyzed, used, disseminated, stored, or discarded; and
  - STRs resulting in prosecution or convictions for money laundering, financing terrorism, or an underlying predicate offense.
- Assessments of the quality of STRs.
- Reports filed on (i) domestic or foreign currency transactions above a certain threshold; (ii) cross-border transportation of currency and bearer negotiable instruments; or (iii) international wire transfers (if applicable).
- Types and frequency of additional information requested.
- Amount of information available for competent authorities in each FIU disclosure in terms of the number of
  - STRs and cash-transaction reports (CTRs) used and linked to the information reported;
  - reporting institutions involved;
  - persons or possible suspects identified; and
  - types of databases queried.
- Time taken to disclose relevant information to competent authorities after it is received from reporting institutions.
- Requests for assistance made or received by the FIU, including whether the request was granted or refused.
- Time taken to respond to each request for assistance made to the FIU.
- Spontaneous referrals made by the FIU to foreign authorities.
- Frequency and scope of guidance issued to reporting institutions (general and individual guidance) (if applicable).
- Response times of reporting institutions to requests for additional information.
- Frequency and scope of strategic analysis provided to other competent authorities and policymakers.
- Feedback received from law-enforcement agencies, the judiciary, or other authorities.

These data need to be appropriately correlated. For example, a large number of STRs received should not be taken as an indication of FIU "success" without observing whether the reports come from a wide variety of sectors or only one (i.e., banking) and whether the reports contain useful information. Similarly, a low number of cases forwarded by the FIU for further investigation or prosecution does not necessarily indicate that the FIU is ineffective if each case already encompasses the analysis of many STRs or if the value added by the FIU often leads to successful prosecutions.

Identifying Opportunities for Improvement

The analysis of the data collected on each function of the FIU may lead to questions concerning the adequacy of the resources devoted to that particular function. A further analysis of that function may reveal opportunities for improving it. A valuable input in this analysis would be feedback from law-enforcement agencies and other entities that receive the FIU's information.

For example, the analysis of STRs may appear in need of improvement. If the reports do not usually contain sufficient relevant information, there may be scope for requiring more such information from the reporting entities and other sources. If the data received appear adequate, improvements may be sought in the analysis function. This function requires strong analytical resources to get the most out of the qualitative data received. Enhancing effectiveness of the FIU in this case might require (among other actions) the following:

- training analysts in the intricacies of the various reporting industries;
- providing analysts with better access to additional sources of information;
- adding to the pool of experts through personnel arrangements with specialized authorities such as financial-supervisory or law-enforcement agencies (by, for example, establishing a secondment program with these agencies);
- increasing the automation of the reporting system so that the information can automatically feed the FIU's databases, thereby facilitating the gathering of various reports that are relevant to a single case; and
- training the reporting institutions staff on what constitutes a good-quality STR, and what information is useful to the FIU (and what is not).

For each function of the FIU, a number of questions may be raised. Among these are the following:

- *Legal framework.* Does the FIU have the necessary powers to perform each of its functions?
- *Capacity.* Is it operationally and technically capable of performing each function according to its purposes?
- *Quality of information disseminated.* Are the reports from reporting institutions and the FIU's access to other information adequate to enable the FIU to fulfill its functions? What is the value added by the FIU to the information it receives? Is there a mismatch between what is expected of it and what it delivers? A frequent cause of tension is that police and prosecutorial authorities expect information from the FIU that it cannot deliver and make little use of the other valuable information that is available to the FIU.

- *Timeliness*. Is the information at all stages of the FIU process flowing at the required speed? Are there any bottlenecks within the FIU?
- *Cost-effectiveness.* Is the FIU striving to produce what it must produce in a manner proportionate to its resources devoted to it?

Much more work remains to be done to develop internationally acceptable standards and methods of assessing the effectiveness of FIUs. Gathering experience with the collection and analysis of statistics on FIU performance is a preliminary step toward achievement of this important goal.

6

INTERNATIONAL ASSESSMENTS OF FIUS

Assessments of AML/CFT frameworks have been carried out since the first round of mutual evaluations of FATF members began in 1992, and FIUs have been included in these assessments from the beginning. A review by the FATF of the first two rounds of mutual evaluations of its members stated that the suspicious transaction reporting system and its associated FIUs were "the driving force in many anti-money laundering regimes" and that the FIU was "central to the anti-money-laundering efforts of almost all members."[176] Assessments of AML/CFT regimes, including FIUs, are now being conducted globally on the basis of a recognized set of standards and procedures.

Standards Regarding FIUs

Before the adoption of the 2003 FATF Recommendations, the standard on AML/CFT did not mention FIUs specifically. In certain contexts in the 1996 Recommendations, FIUs were included in the expression "competent authorities." Nevertheless, as the quotations in the preceding paragraph show, FIUs were considered a key element of the AML/CFT framework. Thus, although no formal standard related specifically to FIUs existed until 2003, AML/CFT assessments took FIUs as a central element in the framework to combat money laundering and the financing of terrorism.

With the endorsement of the *Methodology for Assessing Compliance with Anti-Money Laundering and Combating the Financing of Terrorism Standards* by most institutions with assessing responsibilities in 2002, the assessments were carried out under a methodology that included specific mention of FIUs, although this was not yet formally part of the international standard.[177]

---

[176] FATF, *Review of FATF Anti-Money Laundering Systems and Mutual Evaluation Procedures, 1992–99*, February 16, 2001, paragraphs 67 and 105. Similar statements are contained in the *Review of the Anti-Money Laundering Systems in 22 Council of Europe Member States, 1998–2001*, Strasbourg, March 21, 2002, paragraph 249. ("The FIU is central to the anti-money laundering efforts of most PC-R-EV [now MONEYVAL] members. Indeed, some of the more proactive FIUs, as well as being the disclosure-receiving agencies, are very much the focal point of national anti-money laundering strategies.")

[177] The methodology endorsed in 2002 and used in the assessments so far integrates the "assessable" FATF Anti-Money Laundering Recommendations and Special Recommendations on

(continued)

Originally, the FATF Recommendations concerned only the members of the FATF. Over the years, however, the recommendations have been increasingly recognized as the world standard for anti-money laundering and combating the financing of terrorism. The 1996 Recommendations were adopted by a number of FATF-style regional bodies (FSRBs) and endorsed by the Executive Boards of the IMF and the World Bank for use in the work of these institutions.

In July 2002, the Executive Boards of the IMF and the World Bank conditionally endorsed the FATF Recommendations as the anti-money-laundering and combating the financing of terrorism standard for the operational work of the two institutions. They also endorsed a 12-month pilot program of AML/CFT assessments based on this standard and using the related methodology. Reports on the Observance of Standards and Codes (ROSCs) are prepared on the basis of this standard.

The IMF and World Bank Executive Boards also emphasized that all assessment procedures should be compatible with the uniform, voluntary, and cooperative nature of the ROSC exercise; the assessments would be conducted in accordance with a comprehensive and integrated methodology; and assessments would be followed up with appropriate technical assistance at the request of countries assessed in order to build their institutional capacity and develop their financial sectors.

In March 2004, the Executive Boards of the IMF and the World Bank unconditionally endorsed the 2003 FATF Recommendations as the new standard for use in their work, together with a revised methodology to assess the new standard. As a result, AML/CFT is now a permanent component of the two institutions' work. FSRBs are expected to consider the 2003 Recommendations and Methodology in the course of 2004.

Assessing Compliance with FIU-Related Standards

Under the IMF and World Bank's 12-month pilot program, some 53 assessments were commenced, including some carried out by the IMF and World Bank and others by the FATF and the FSRBs. Under the then-current methodology, assessments were made with regard to 27 of the FATF 40 Recommendations and seven of the Eight Special Recommendations on Terrorist Financing.[178] In decreasing order of compliance, each

---

Terrorist Financing, as well as the basic principles issued by the Egmont Group regarding FIUs and those issued by the international groups of financial supervisors regarding money laundering.

[178] Some recommendations were not assessed, either because by their nature they were not assessable or because they had not fully come into force. It may also be noted that the assessments

(continued)

recommendation was rated as "compliant," "largely compliant," "materially noncompliant," or "noncompliant."

The data collected in the course of the 41 assessments for which detailed reports were available were analyzed and summarized in a joint IMF-World Bank paper of March 2004.[179] The rating of the cluster of FATF Recommendations of greatest interest to FIUs was generally high. Taken together, compliance with Recommendations 16 (legal protection for bona fide reports), 17 (prohibition against tipping off), and 18 (compliance with instructions) was very high, with 88 percent, 86 percent, and 76 percent, of jurisdictions, respectively, rated "compliant."[180]

Implementation of the Special Recommendations on Terrorist Financing has lagged behind those related to money laundering. For example, 68 percent of the jurisdictions were assessed as either "compliant" or "largely compliant" with Recommendation 15 on the reporting of suspicious transactions, while 22 percent were rated "materially noncompliant." and 10 percent were rated "noncompliant." In contrast, only 59 percent of the jurisdictions were rated "compliant" or "largely compliant" with Special Recommendation VII on reporting transactions suspected of being related to terrorist financing, while 13 percent were rated "materially noncompliant" and 28 percent were rated "noncompliant."

Other findings relating to FIUs concerned the independence of the FIU, its staffing, clarifying its role vis-à-vis supervisors, strengthening its organizational structure, providing it with wider access to official databases, improving the training and skills of FIU staff, and developing management-reporting systems to monitor the effectiveness of the FIU.

Concurrently with the carrying out of those IMF assessments, the Fund, the World Bank, and other institutions provided considerable technical assistance to countries wishing to strengthen their AML/CFT frameworks. The technical assistance provided by the IMF and the World Bank in this area increased sharply during the two-year period extending from January 2002 through December 2003. During that time, the two organizations delivered 117 technical assistance projects, including 85 projects directly to individual countries and 32 regional projects reaching more than 130 countries.[181] The

---

reviewed under the pilot program, which were based on the 1996 FATF Recommendations, did not cover the collection of statistics discussed in the preceding chapter, since there was no FATF recommendation on this point until the adoption of the 2003 Recommendations.

[179] International Monetary Fund and World Bank, 2004, *Twelve-Month Pilot Program of Anti-Money- Laundering and Combating the Financing of Terrorism (AML/CFT) Assessments,* March 10 (Washington), Annex II.

[180] *Id*., Annex II, Table 6.

[181] *Id.,* paragraph 18.

increase in technical assistance activity was spurred, in large part, by the assessments, which provide national authorities with a diagnostic tool to identify their countries' technical assistance needs. More than one-quarter of the technical assistance projects consisted of providing different forms of advice on the establishment and strengthening of FIUs.

7

CONCLUSIONS

FIUs are an essential component of the international fight against money laundering, the financing of terrorism, and related crime. Their ability to transform data into financial intelligence is a key element in the fight against money laundering and the financing of terrorism. The place of FIUs is now well established in the arsenal of measures to combat these serious crimes. Yet FIUs face a number of challenges.

Two general challenges appear as constants in the design of FIUs and the improvement of existing ones. The first is that there is no set formula to make an FIU work. Each FIU must be tailored to the specific situation of the country in which it is located. Factors such as the structure and relative importance of financial crime in the country, the government's objectives in combating this form of criminality, the resources available for the task, and the legal and administrative systems of the country all have to be taken into consideration in designing an FIU or proposing measures to improve the performance of an existing one. As this handbook has demonstrated, on many issues of FIU design, many solutions are possible and none is inherently better than the others.

Establishment of an FIU that can carry out the three core functions of receiving suspicious transaction and other reports, analyzing them, and disseminating financial intelligence has recently become the subject of an international standard and is encouraged in a number of recent international conventions dealing with financial crime. Nevertheless, the standard is expressed in very broad terms, and authorities in each country must have a clear vision of their own policy objectives and of the local and regional context when they design an FIU that will meet the standard. And beyond complying with the standard, each country needs to ensure that its FIU makes the contribution that it can to the successful functioning of the AML/CFT system as a whole.

The second challenge is, paradoxically, change. In the many countries that have established FIUs over the past ten years or so, change has been evident, with their FIU having had to establish themselves as credible organizations capable of dealing with financial institutions and other reporting entities, other government agencies, and international counterparts, changing traditional relationships between economic agents and law-enforcement organizations in the process.

Change will continue to be a feature of the work of FIUs in the future. Although the adoption of the new FATF Recommendations in 2003 may signal a temporary stabilization of the standards applicable to FIUs themselves, other aspects of the fight against money laundering will continue to evolve. Not the least of these is the behavior of criminals. Criminal behavior is like a stream of water, following gravity and constantly prodding the banks for weak points through which it can spread further. As defenses are set up in the supervised financial sector, criminals may move their funds deeper underground or through other, less regulated sectors of the economy. Similarly, as some countries take decisive steps to strengthen their legal and administrative systems to deal with financial crime, criminals may move some of their operations to countries that have not yet done so. There is a need to be constantly on the lookout to counter changes in patterns of criminal behavior.

Against this general background, FIUs currently face more specific challenges. The most important ones are the integration of the financing of terrorism in their work, the broadening of the suspicious transaction reporting obligation beyond the regulated financial sector, and the quest for improved international cooperation.

For countries fortunate enough not to have had to deal with terrorism in the past, the addition of combating the financing of terrorism to the scope of the FIU's functions presents special challenges. Terrorism is, in many ways, different from money laundering. Terrorism is traditionally not considered a profit-motivated crime; and although significant sums of money may be involved in the commission of terrorist acts, the objective of depriving criminals of the profits of their illegal activity, which is at the heart of an anti-money- laundering strategy, does not apply directly to terrorism. Also, in many countries, the agencies involved in combating terrorism are not the same ones dealing with money laundering, thus requiring FIUs to develop new relationships with the former. (In countries that have already faced terrorism, the basic elements needed to combat it may be in place, and the addition of combating the financing of terrorism to the FIU's functions may be more easily integrated.)

The second specific challenge faced by FIUs is the broadening of the reporting obligation (and other preventive obligations) to entities beyond the prudentially regulated financial institutions. The extension of the reporting obligation to casinos; dealers in high-value goods; and, more recently, the accounting and legal professions has had a number of implications for FIUs. Some of these professions, such as casinos may be highly regulated in some countries but not in others. Some may not be regulated beyond the basic requirements of incorporation, as may be true of car dealers. Considerable outreach resources are likely to be needed to bring such professions up to an acceptable level of compliance with the reporting requirements. The nature of the reports provided by accounting and legal professionals are bound to be

very different from those provided by financial institutions. Complex company structures and trust arrangements require specialized expertise to unravel. Resources have to be allocated to this type of work, and difficult decisions may need to be made as to the balance of resources to be devoted to these new types of reports as compared with the more traditional types.

The third specific challenge is the need to improve the ability of FIUs to engage in international cooperation. The dynamic growth in FIUs worldwide over the last fifteen years has been accompanied by a strong growth in international cooperation between FIUs. The ability of the more than 80 FIUs to network and share financial intelligence based on agreed principles of information exchange has served as a formidable mechanism for fighting financial crime worldwide. Despite the achievements to date in this area, significant challenges lie ahead. In particular, removing legal obstacles that remain in the way of information sharing and developing and improving systems to ensure the confidentiality of exchanged information remain crucial challenges.

APPENDIXES

Appendix

I

Statement of Purpose of the Egmont Group of Financial Intelligence Units

The Hague, 13 June 2001

Recognising the international nature of money laundering;

Realising that in order to counter money laundering an increasing number of governments around the world have both imposed disclosure obligations on financial institutions and designated financial intelligence units, or "FIUs," to receive, analyse, and disseminate to competent authorities such disclosures of financial information;

Identifying terrorism financing as a distinct and growing problem that like money laundering crosses national borders and operates within the international financial system;

Finding that FIUs acting in their capacity to receive, analyse and disseminate sensitive financial disclosures increasingly have become valuable tools in the global fight against terrorism financing by supporting the work of traditional national government agencies;

Convinced that co-operation between and among FIUs across national borders both increases the effectiveness of individual FIUs and contributes to the success of the global fight against money laundering and terrorism financing;

Mindful of both the sensitive nature of disclosures of financial information and the value of the FIUs established to protect their confidentiality, analyse them, and refer them, as appropriate, to the competent authorities for investigation, prosecution, or trial;

Understanding that effective international co-operation between and among FIUs must be based on a foundation of mutual trust;

Acknowledging the important role of international organisations and the various traditional national government agencies – such as Finance and Justice ministries, the police, and financial institution supervisory agencies – as allies in the fight against money laundering and terrorism financing;

Having periodically convened plenary gatherings – known as Egmont Group Meetings[1] *– to discuss issues common to FIUs and to foster such international*

[1] Named after the Egmont-Arenberg palace in Brussels where the first such meeting was held on 9 June 1995.

co-operation among established FIUs, to assist and advise FIUs under development, and to co-operate with representatives of other government agencies and international organisations interested in the international fight against money laundering and terrorism financing;

Having also agreed upon a definition of "Financial Intelligence Unit," completed a survey on the possibilities and modalities of information exchange, prepared a model Memorandum of Understanding for the exchange of information, created a secure Internet Web-site to facilitate information exchanges, and embarked upon several specific initiatives to develop the expertise and skills of the FIUs' staffs and to contribute to the successful investigation of matters within the FIUs' jurisdiction;

Aware that obstacles continue to limit information exchange and effective co-operation between some FIUs, and that those obstacles may include legal restrictions and/or the very nature of the FIUs themselves (– as administrative, judicial, or police); and

Convinced that there exists both significant potential for broad-based international co-operation among the FIUs and a critical need to enhance such co-operation,

The FIUs participating in the Egmont Group hereby affirm their commitment to to encourage the development of FIUs and co-operation among and between them in the interest of combating money laundering and in assisting with the global fight against terrorism financing.

To that end, we affirm our accession to the definition of a Financial Intelligence Unit adopted at the plenary meeting of the Egmont Group in Rome in November 1996, as amended at the Egmont Plenary Meeting in Guernsey in June 2004:

> "A central, national agency responsible for receiving, (and as permitted, requesting), analysing and disseminating to the competent authorities, disclosures of financial information:
>
> (i) concerning suspected proceeds of crime and potential financing of terrorism, or
>
> (ii) required by national legislation or regulation,
>
> in order to combat money laundering and terrorism financing."

We also adopt the findings of the legal working group concerning the identification of those agencies that meet the FIU definition at the present time.

Henceforth, we agree that Egmont Group plenary meetings shall be convened by and for FIUs and other invited persons or agencies who are in a position to contribute to the goals of the Egmont Group. Egmont Group Participants shall include FIUs and other agencies representing governments that do not

presently have FIUs. All other invited persons, agencies or international organisations shall be considered "Observers."

We believe it is crucial to develop a network of information exchange on the basis of the *"Principles of Information Exchange Between Financial Intelligence Units"* as set forth in the Annex and incorporated herein by this reference.

We recognise the right of every FIU to subject co-operation to additional conditions as required by its national legislation.

We further agree to pursue as a priority, through the appropriate working groups and otherwise:

- Determination of appropriate consequences that attend to an Egmont Group Participant's status with respect to the definition of FIU adopted in Rome;
- Development of FIUs in governments around the world;
- Further stimulation of information exchange on the basis of reciprocity or mutual agreement;
- Access to the Egmont Secure Web-site for all FIUs;
- Continued development of training opportunities, regional/operational workshops, and personnel exchanges;
- Consideration of a formal structure to maintain continuity in the administration of the Egmont Group, as well as consideration of a regular frequency and location for plenary meetings;
- Articulation of more formal procedures by which decisions as to particular agencies' status vis-à-vis the FIU definition are to be taken;
- Designation of additional working groups, as necessary;
- Development of appropriate modalities for the exchange of information;
- Creation of Egmont Group sanctioned materials for use in presentations and communication to public audiences and the press about Egmont Group matters.

As originally approved in Madrid on 24 June 1997, amended at The Hague on 13 June 2001, in Sydney on 23 July 2003 and in Guernsey on 23 June 2004.

Appendix

II

Procedure for Being Recognized as an Egmont Group Financial Intelligence Unit (FIU)

The Statement of Purpose adopted at the Madrid Plenary meeting of the Egmont Group called for a formal articulation of the process by which a financial intelligence unit (FIU) is recognised as meeting the Egmont FIU definition in order to become an Egmont Group member.

The Outreach Working Group (OWG) has the task of spreading the Egmont idea worldwide. The role of OWG members with respect to non-Egmont member jurisdictions is to act as a support / monitor FIU towards any candidate unit with a view to obtaining all the necessary contact details, legislation and information concerning the prospective FIU and its operational status. The OWG members will provide as much assistance as possible to the candidates.

Any Egmont member who has information on potential candidates passes this on to the Chairman of the OWG, who organises a first screening of the unit by a member of the OWG.

This entails collecting at a minimum the following information:

- contact address and name;
- money laundering legislation in force;
- operational status of a FIU (off-site);
- willingness to join the Egmont Group;
- the possibility of exchanging information with other FIUs;
- operational status of a FIU (on-site).

In principle the assessment includes an on site visit. If the OWG member acting as supporting FIU is not able to do so, another Egmont member may fulfil this requirement.

Once the OWG has obtained all necessary information and is satisfied that the prospective candidate may meet the Egmont criteria, the OWG Chair makes a written recommendation to the Legal Working Group (LWG) Chair, with copy to the Egmont Permanent Administrative Support (PAS). The LWG then proceeds to an in-depth assessment in view of a final decision on the recommendation of the candidate to the Heads of FIU.

This procedure starts with the decision of the LWG Chair to continue with a follow up of the findings and recommendations of the OWG. The LWG Chairman then instructs the PAS to send the candidate FIU the following

documents with a request to return the completed questionnaire together with any relevant supporting documentation to the PAS before a set deadline:

- Egmont questionnaire
- Information Paper
- Statement of Purpose
- Principles of Information Exchange between FIUs
- Interpretative Note on the Egmont Group Definition
- Model Memorandum of Understanding (MOU)

Following the timely receipt of all requested documentation the candidate's submission is examined by the LWG at its next meeting, the meeting immediately preceding the Plenary excluded.

The LWG makes the final assessment so as to ensure that the candidate FIU does indeed fulfil the Egmont admission criteria, *i.e.* that the unit:

- meets the Egmont FIU definition[1];
- has reached full operational status;
- is legally capable and willing to cooperate on the basis of the Egmont "Principles of Information Exchange";
- has a sponsoring Egmont FIU.

The LWG Chairman may decide to invite the candidate to present its application in a personal interview. As a rule the LWG assessment takes place in the presence of the monitoring OWG member FIU.

The assessment also infers the designation of a sponsoring FIU by the LWG. Beside providing guidance to the candidate in the admission procedure and speaking on behalf of the candidate at working group meetings, the sponsor is expected to be able to confirm the operational status of the candidate unit as an FIU out of first hand experience, including an on-site visit. Where appropriate, the monitoring OWG member FIU may act as a sponsor. The LWG can take the following decisions:

- defer the discussion to its next meeting, pending additional clarification or documentation from the candidate;
- emit a negative opinion when it considers one or more Egmont criteria not being met completely or partially;
- recommend the candidate unit to be recognised and accepted as an Egmont FIU, to be endorsed by the Heads of FIU at the next Plenary.

---

[1] "*A central, national agency responsible for receiving (and, as permitted, requesting), analysing and disseminating to the competent authorities, disclosures of financial information*
(i) concerning suspected proceeds of crime, or
(ii) required by national legislation or regulation, in order to counter money laundering."

The PAS informs the candidate in writing of the outcome of the LWG assessment and ensures the Egmont FIUs are kept posted through the minutes of the meeting and the Egmont Secure Web.

FIUs are officially recognised as an Egmont Group member by endorsement of the LWG recommendation by the Heads of FIU at their annual Plenary meeting.

Appendix

III

The Egmont Group: Financial Intelligence Units of the World

OPERATIONAL UNITS (Meeting the Egmont Definition)

Status as of 23 June 2004

1. Albania: Drejtoria e Bashkerendimit te Luftes Kunder Pastrimit te Parave (DBLKPP) Directory of Co-ordinating the Fight Against Money Laundering
2. Andorra: Unitat de Prevenció del Blanqueig (UPB) Money Laundering Prevention Unit
3. Anguilla: Money Laundering Reporting Authority (MLRA)
4. Antigua and Barbuda: Office of National Drug and Money Laundering Control Policy (ONDCP)
5. Argentina: Unidad de Información Financiera (UIF)
6. Aruba: Meldpunt Ongebruikelijke Transacties - Ministerie van Financiën (MOT-Aruba) Unusual Transactions Reporting Office
7. Australia: Australian Transaction Report & Analysis Centre (AUSTRAC)
8. Austria: Bundeskriminalamt (A-FIU)
9. Bahamas: Financial Intelligence Unit (FIU)
10. Bahrain: Anti-Money Laundering Unit (AMLU)
11. Barbados: Financial Intelligence Unit (FIU)
12. Belgium: Cellule de Traitement des Informations Financières / Cel voor Financiële Informatieverwerking (CTIF-CFI) Financial Information Processing Unit
13. Belize: Financial Intelligence Unit (FIU)
14. Bermuda: Bermuda Police Service / Financial Investigation Unit (BPSFIU)
15. Bolivia: Unidad de Investigaciones Financieras (UIF – Bolivia)
16. Brazil: Conselho de Controle de Atividades Financeira (COAF) Council for Financial Activities Control
17. British Virgin Islands: Government of BVI/Financial Services Department

18. Bulgaria: Financial Intelligence Agency (FIA)
19. Canada: Financial Transactions and Reports Analysis Centre of Canada/Centre d'analyse des opérations et déclarations financières du Canada (FINTRAC/CANAFE)
20. Cayman Islands: Financial Reporting Authority (CAYFIN)
21. Chile: Departamento de Control de Trafico Ilícito de Estupefacientes Consejo de Defensa del Estado (CDE) Department for Prevention of Illicit Narcotics Trafficking Council for the Defence of the State
22. Colombia: Unidad de Informacion y Analisis Financiero (UIAF)
23. Cook Islands: Cook Islands Financial Intelligence Unit (CIFIU)
24. Costa Rica: Centro de Inteligencia Conjunto Antidrogas/Unidad de Analisis Financiero (CICAD/UAF)
25. Croatia: Financijska Policija / Ured za Sprjecavanje Pranja Novca Financial Police / Anti Money Laundering Department (AMLD)
26. Cyprus: MO.K.A.Σ.—Unit for Combating Money Laundering
27. Czech Republic: Financní analytický útvar (FAU – CR) Financial Analytical Unit
28. Denmark: SØK / Hvidvasksekretariatet Stadsadvokaten for Særlig Økonomisk Kriminalitet / Hvidvasksekretariatet (HVIDVASK) National sPublic Prosecutor for Serious Economic Crime / Money Laundering Secretaria
29. Dominica: Financial Intelligence Unit (FIU)
30. Dominican Republic: Unidad de Inteligencia Financiera (UIF)
31. Egypt: Egyptian Money Laundering Combating Unit (EMLCU)
32. El Salvador: Unidad de Investigacion Financiera (UIF)
33. Estonia: Rahapesu Andmeburoo/Money Laundering Information Bureau
34. Finland: Keskusrikospoliisi / Rahanpesun selvittelykeskus (RAP) National Bureau of Investigation / Money Laundering Clearing House
35. France: Traitement du renseignement et action contre les circuits financiers clandestins (TRACFIN) Processing of information and action against clandestine financial networks
36. Georgia: Saqartvelos Finansuri Monitoringis Samsaxuri Financial Monitoring Service of Georgia (FMS)

37. Germany: Zentralstelle für Verdachtsanzeigen – Financial Intelligence Unit
38. Gibraltar: Gibraltar Co-ordinating Centre for Criminal Intelligence and Drugs/Gibraltar Financial Intelligence Unit (GCID GFIU)
39. Greece: Φορηας Αρθρου 7 N.2331/95 -- "Committee of Article 7 of Law 2331/1995" (C.F.C.I.)
40. Grenada: Financial Intelligence Unit (FIU)
41. Guatemala: Intendencia de Verificación Especial (IVE) Special Verification Intendency
42. Guernsey: Financial Intelligence Service (FIS)
43. Hong Kong: Joint Financial Intelligence Unit (JFIU)
44. Hungary: Pénzmosás Elleni Alosztály (ORFK)
45. Iceland: Ríkisssaksóknari (RLS) Unit of Investigation and Prosecution of Economic and Environmental Crime in Iceland
46. Indonesia: Pusat Pelaporan dan Analisis Transaksi Keuangan Indonesian Financial Transaction Reports and Analysis Centre (PPATK/INTRAC)
47. Ireland: An Garda Síochána / Bureau of Fraud Investigation (MLIU)
48. Isle of Man: Financial Crime Unit (FCU – IOM)
49. Israel: Israel Money Laundering Prohibition Authority (IMPA)
50. Italy: Ufficio Italiano dei Cambi / Servizio Antiriciclaggio – (UIC/SAR) Italian Foreign Exchange Office / Anti-Money Laundering Service
51. Japan: Japan Financial Intelligence Office (JAFIO)
52. Jersey: Joint Police & Customs Financial Investigation Unit- Jersey (FCU – Jersey)
53. Korea: (Republic of) Korea Financial Intelligence Unit (KoFIU)
54. Latvia: Kontroles dienests, Noziedîgi iegûto lîdzeklu legalizâcijas novçrsanas dienests (KD) Control Service - Office for Prevention of Laundering of Proceeds Derived from Criminal Activity
55. Lebanon: Special Investigation Commission (SIC) Fighting Money Laundering
56. Liechtenstein: Einheit für Finanzinformationen (EFFI)
57. Lithuania: Mokesèiu policijos departamentas prie Lietuvos Respublikos Vidaus reikalu ministerijos. (MDP prie VRM) Money Laundering

Prevention Division of the Tax Police Department at the Ministry of Internal Affairs

58. Luxembourg: Cellule de Renseignement Financier (FIU-LUX)
59. Macedonia: Ministerstvo za Finansii-Direkcija za Sprecuvanje na Perenje Pari Money Laundering Prevention Directorate (MLPD)
60. Malaysia: Unit Perisikan Kewangan, Bank Negara Malaysia (UPW)
61. Malta: Financial Intelligence Analysis Unit (FIAU)
62. Marshall Islands: Domestic Financial Intelligence Unit (DFIU)
63. Mauritius: Financial Intelligence Unit (FIU)
64. Mexico: Dirección General Adjunta de Investigación de Operaciones Unidad de Inteligencia Financiera (DGAIO / UIF) Attached Directorate General for Investigation of Transactions/Financial Intelligence Unit
65. Monaco: Service d'Information et de Contrôle sur les Circuits Financiers (SICCFIN) Service for Information and Monitoring of Financial Networks
66. Netherlands: Meldpunt Ongebruikelijke Transacties - Ministerie van Justitie (MOT) Unusual Transactions Reporting Office
67. Netherlands Antilles: Meldpunt Ongebruikelijke Transacties – Nederlandse Antillen (MOT-Nederlandse Antillen) Unusual Transactions Reporting Centre- Netherlands Antilles
68. New Zealand: NZ Police Financial Intelligence Unit
69. Norway: ØKOKRIM / Hvitvaskingsenheten The National Authority for Investigation and Prosecution of Economic and Environmental Crime – The Money Laundering Unit
70. Panama: Unidad de Análisis Financiero (UAF - Panama)
71. Paraguay: Unidad de Análisis Financiero (UAF - Paraguay)
72. Poland: Generalny Inspektor Informacji Finansowej (GIIF) General Inspector of Financial Information
73. Portugal: Unidade de Informação Financeira (UIF)
74. Romania: Oficiul Nacional de Prevenire si Combatere a Spalarii Banilor (ONPCSB) National Office for the Prevention and Control of Money Laundering
75. Russia: Komitet Rossijskoi Federacii po Finansovomu Monitoringu Financial Monitoring Committee of the Russian Federation (FMC)

76. Serbia: Uprava Za Spreèavanje Pranja Novca. Administration for the Prevention of Money Laundering

77. Singapore: Suspicious Transaction Reporting Office (STRO)

78. Slovakia: Spravodajská jednotka finacnej polície Úradu boja proti organizovanej kriminalite (SJFP UBPOK) Financial Intelligence Unit of the Bureau of Organised Crime

79. Slovenia: Urad RS za Preprecevanje Pranja Denarja Ministrstvo za Finance Office for Money Laundering Prevention (OMLP)

80. South Africa: Financial Intelligence Centre (FIC)

81. Spain: Servicio Ejecutivo de la Comisión de Prevención de Blanqueo de Capitales e Infracciones Monetarias (SEPBLAC) Executive Service of the Commission for the Prevention of Money Laundering and Financial Crime

82. St. Kitts and Nevis: Financial Intelligence Unit (FIU)

83. St. Vincent & the Grenadines: Financial Intelligence Unit (FIU)

84. Sweden: Finanspolisen Rikspolisstyrelsen (NFIS) National Criminal Intelligence Service, Financial Unit

85. Switzerland: Meldestelle für Geldwäscherei, Bureau de communication en matière de blanchiment d'argent, Ufficio di comunicazione in materia di riciclaggio di denaro Money Laundering Reporting Office – Switzerland (MROS)

86. Taiwan: Money Laundering Prevention Center (MLPC)

87. Thailand: Anti-Money Laundering Office (AMLO)

88. Turkey: Mali Suçlari Arastirma Kurulu (MASAK) Financial Crimes Investigation Board

89. Ukraine: Держфінмоніторинг, Державний департамент фінансового моніторингу State Department for Financial Monitoring (SDFM)

90. United Arab Emirates: Anti-Money Laundering and Suspicious Cases Unit (AMLSCU)

91. United Kingdom: National Criminal Intelligence Service / Financial Intelligence Division (NCIS / FID)

92. United States: Financial Crimes Enforcement Network (FinCEN)

93. Vanuatu: Financial Intelligence Unit (FIU)

94. Venezuela: Unidad de Inteligencia Financiera (UNIF)

Appendix

IV

Interpretive Note Concerning the Egmont Definition of a Financial Intelligence Unit

History of The Egmont Group

In June 1995, government agencies and international organizations gathered at the Egmont-Arenberg Palace in Brussels to discuss money laundering and ways to confront this global problem. Out of this first meeting was born the Egmont Group ("Egmont"), an informal body of government disclosure receiving agencies that share a common goal – to provide a forum to enhance mutual cooperation and to share information that has utility in detecting and combating money laundering and, more recently, terrorism financing. Over time, working groups have developed to carry out the tasks of Egmont. Today, Egmont has four working groups: Legal, Training and Communication, Outreach and Operational.

Early on, the participants in Egmont recognized the need for developing effective and practical means of cooperating, especially concerning information exchange and the sharing of expertise. To meet those challenges, the Legal Working Group examined obstacles related to information exchange among government agencies that specifically combat money laundering through the processing of financial information. To identify financial disclosure receiving agencies around the world and to better understand how such government agencies function, jurisdictions completed questionnaires and submitted them for review by the Legal Working Group. On the basis of the answers provided from the questionnaires, the Legal Working Group devised a functional definition of government agencies, called Financial Intelligence Units ("FIUs") that combat money laundering.

Although initially the focus of the Egmont FIU was essentially on money laundering, FIUs are also playing an important role in the international effort to combat the financing of terrorism. The financial disclosures that FIUs currently receive, analyze and disseminate have proven to be invaluable sources of information for those national agencies that investigate terrorism financing. In order to meet international mandatory standards countries have or are in the process of amending their domestic legislation to bring terrorism financing within the remit of their FIU as an autonomous offence, beside as a predicate offense for money laundering, thus expanding the scope of the FIU's overall functions.

Egmont Definition

Based upon the work of the Legal Working Group, Egmont approved the following definition of an FIU in 1996, consequently amended in 2004 to reflect the FIU's role in combating terrorism financing:

A central, national agency responsible for receiving, (and as permitted, requesting), analysing and disseminating to the competent authorities, disclosures of financial information:

(i) concerning suspected proceeds of crime and potential financing of terrorism, or
(ii) required by national legislation or regulation,

in order to combat money laundering and terrorism financing.

The definition of an FIU can best be understood through a brief explanation of each of its component parts.

1. A central, national agency. Egmont's focus on international co-operation requires that only one government agency per territory or self-autonomous jurisdiction, recognized by international boundaries, serve as the contact point for international exchanges. It must operate in a jurisdiction that is governed by the laws of that territory. To be clear, use of the phrase "central, national agency" carries with it no political designation or recognition of any kind.

An anti-money laundering/terrorism financing government agency operating in a jurisdiction that in political terms constitutes a dependency of another nation, may be considered an FIU as long as it is the only government agency that carries out these efforts in that internationally recognized boundary. Recognition that such government agency meets the Egmont definition of an FIU does not necessarily equate to sovereignty.

In federal systems, the phrase "central, national agency" implies that only one government agency may be considered an FIU under Egmont. Even though federal systems have multiple subdivisions, only one centralized agency serves as contact point for information exchange for Egmont.

2. Responsible for. This word denotes that the legal framework, which establishes the FIU, authorizes, at a minimum, the functions outlined in the Egmont definition.

3. Receiving, (and as permitted, requesting) analysing and disseminating. This phrase designates the three principal activities of all Egmont FIUs, and the functions that make them unique.

- **Receiving.** FIUs serve as the central reception point for receiving financial disclosures. This takes into account FIUs that have more than one office and FIUs that receive disclosures from different domestic agencies. This concept also distinguishes FIUs from law enforcement agencies with a general (overall) law enforcement mission.

- **(And as Permitted, Requesting).** Some but not all FIUs have the ability to query specific financial information from certain financial institutions and other nonfinancial entities beyond the financial disclosures that FIUs normally receive from reporting entities. For this reason, the language is in parentheses and is limited in scope.

- **Analysing.** Analysis involves an initial evaluation of the utility or relevance of disclosures received from reporting entities at the pre-investigation stage. Analysis of information reported to FIUs may occur at different stages and take different forms. Some FIUs analyse every financial disclosure when it arrives at the FIU. For other FIUs, such a system is impossible due to the sheer volume of financial disclosures that they receive. Those FIUs make the financial disclosures immediately available to appropriate investigative authorities and the FIUs analyse financial disclosures in response to requests for information or on their own accord but not in response to each and every financial disclosure reported to it. In an increasing manner, many FIUs have incorporated analytical software that assists in determining money laundering trends and patterns for use by law enforcement, to provide feedback to the reporting institutions and in some cases for purposes of proactive targeting. In all cases, some de minimis level of analysis must occur in order to categorise a given piece of information and determine which agency, or group of agencies, should be entitled to receive it.

- **Disseminating.** FIUs at a minimum must be able to share information from financial disclosures and the results of their analysis regarding money laundering and related crimes, as determined by domestic legislation, and terrorism financing, firstly with domestic competent authorities and, secondly, with other FIUs. A critical element in assessing dissemination capability involves assessing the extent to which a candidate FIU's law permits the cooperation with other FIUs through the exchange of information.

4. Disclosures of financial information. These are the materials that FIUs use and share with each other to detect and combat money laundering and terrorism financing. In this regard, FIUs may share publicly available and as well as sensitive information (whether financial disclosures or law enforcement information) with competent authorities under terms that protect the information against misuse.

5. Concerning suspected proceeds of crime and potential financing of terrorism. The first type of disclosure of financial information concerns the reporting of suspicious or unusual transactions or activities regarding funds that are suspected of having originated from criminal activity or of being intended to support terrorist activity.

[Disclosures otherwise] required by national legislation, or regulation. This requirement encompasses all other mandated types of reporting requirements required by law, whether involving currency, checks, wires or other transactions.

6. In order to combat money laundering and terrorism financing. This phrase reemphasizes the common purpose of every FIU.

Appendix

V

Egmont Group: Principles for Information Exchange Between Financial Intelligence Units for Money-Laundering Cases

The Hague, 13 June 2001

Annex To The Egmont Group "Statement Of Purpose"

A. Introduction

1. The Egmont Group works to foster the development of Financial Intelligence Units ("FIUs")[1] and information exchange.

2. The Egmont Group agreed in its Statement of Purpose, adopted in Madrid on 24 June 1997, to pursue among its priorities the stimulation of information exchange and to overcome the obstacles preventing cross-border information sharing.

3. Information-sharing arrangements should have the aim of fostering the widest possible co-operation between FIUs.

4. The following principles for information exchange among FIUs are meant to outline generally-shared concepts, while allowing countries necessary flexibility.

B. General Framework

5. International co-operation between FIUs in cases involving money laundering should be encouraged and based upon a foundation of mutual trust.

6. FIUs should take steps to seek information that may be used by other, identified, domestic law enforcement or financial supervisory agencies engaged in enforcement and related regulatory activities related to money laundering.

7. FIUs should work to encourage that national legal standards and privacy laws are not conceived so as to inhibit the exchange of information, in accordance with these principles, between or among FIUs.

[1] See definition in the Egmont Group "Statement of Purpose."

8. Information-sharing arrangements must recognize and allow room for case-by-case solutions to specific problems.

C. Conditions for the Exchange of Information

9. FIUs should be able to exchange information freely with other FIUs on the basis of reciprocity or mutual agreement and consistent with procedures understood by the requested and requesting party. Such exchange, either upon request or spontaneously, should produce any available information that may be relevant to an analysis or investigation of financial transactions and other relevant information related to money laundering and the persons or companies involved.

10. An FIU requesting information should disclose, to the FIU that will process the request, at a minimum the reason for the request, the purpose for which the information will be used and enough information to enable the receiving FIU to determine whether the request complies with its domestic law.

D. Permitted Uses of Information

11. Information exchanged between FIUs may be used only for the specific purpose for which the information was sought or provided.

12. The requesting FIU may not transfer information shared by a disclosing FIU to a third party, nor make use of the information in an administrative, investigative, prosecutorial, or judicial purpose without the prior consent of the FIU that disclosed the information.

E. Confidentiality – Protection of Privacy

13. All information exchanged by FIUs must be subjected to strict controls and safeguards to ensure that the information is used only in an authorized manner, consistent with national provisions on privacy and data protection. At a minimum, exchanged information must be treated as protected by the same confidentiality provisions as apply to similar information from domestic sources obtained by the receiving FIU.

Appendix

VI

Egmont Group: Best Practices for the Improvement of Exchange of Information Between Financial Intelligence Units

Introduction

1. According to the **Statement of Purpose** of the Egmont Group, the Financial Intelligence Units (FIUs) participating in the Egmont Group resolve to encourage co-operation among and between them in the interest of combating money laundering and terrorism financing.

The members showed an awareness of the need to maximise information exchange and effective co-operation among FIUs and expressed their conviction that there exists both significant potential for broad-based international co-operation among the FIUs and a critical need to enhance such co-operation.

The Egmont Members agreed to pursue as a priority the further enhancement of information exchange on the basis of reciprocity or mutual agreement and the development of appropriate modalities to that end.

2. Consequently, a document on **"Principles of Information Exchange Between Financial Intelligence Units "** was agreed on and incorporated into the Statement of Purpose.

These principles reflect the intention of the Egmont Group to make their pursuit of the enhancement of information exchange a priority and to overcome the obstacles preventing cross-border information sharing. FIUs are therefore invited to do everything possible to ensure that national legal standards and privacy laws are not conceived so as to inhibit the exchange of information between or among FIUs. The principles relate to the conditions for the exchange of information, the permitted uses of information, as well as the confidentiality issue.

3. In some countries there might be restrictions that limit the free exchange of information with other FIUs or the access to information relevant to a requesting FIU. This document firstly describes practices that maximize cooperation between FIUs and can be used as inspiration for government authorities and officials when considering money laundering legislation.

Furthermore to address the practical issues that have been identified as impeding the efficiency of mutual assistance, this document aims to provide guidelines in terms of best practices for the exchange of information between FIUs. When dealing with international requests for information, FIUs should

endeavour to take these best practices into account to the greatest possible extent.

A. LEGAL

1. The Egmont principle of free exchange of information at FIU-level should be possible on the basis of reciprocity, including spontaneous exchange.

2. The exchange of information between FIUs should not be affected by their status, be it of an administrative, law enforcement, judicial or other nature.

3. Differences in the definition of the offences governing the competence of FIUs should not be an obstacle to free exchange of information at FIU-level. To this end, the FIU's competence should extend to all predicate offences for money laundering as well as terrorism financing.

4. The exchange of information between FIUs should take place as informally and as rapidly as possible and with no excessive formal prerequisites, while guaranteeing protection of privacy and confidentiality of the shared data.

5. Should an FIU still need MOUs to exchange information, these should be negotiated and signed by the FIU without undue delay. To that end the FIU should have the authority to sign MOUs independently.

6. It should be possible for communication between FIUs to take place directly, without intermediary body.

7. Requests from a counterpart FIU should be dealt with in the same way as a domestic disclosure so that the receiving FIU can exchange all information available to the FIU under its own authority.

To this end FIUs should have speedy access to complementary information. FIUs should in particular have access to:

- all relevant tools and registers existing in their respective jurisdiction, including law enforcement information;
- information held by financial institutions and other reporting entities;
- information on beneficial ownership and control of legal persons, such as corporate entities, trusts and IBCs.

8. The providing FIU's prior consent to disseminate the information for further law enforcement or judicial purposes should be granted promptly and to the largest extent possible.

The providing FIU should not refuse its consent to such dissemination unless this would fall beyond the scope of application of its AML/CFT provisions, could lead to impairment of a criminal investigation, would be clearly disproportionate to the legitimate interests of a natural or legal person or the

State of the providing FIU, or would otherwise not be in accordance with fundamental principles of its national law. Any such refusal to grant consent shall be appropriately explained.

B. PRACTICAL

1) REQUEST

The following practices should be observed by the FIU intending to submit a request for information:

1. All FIUs should submit requests for information in compliance with the Principles for Information Exchange that have been set out by the Egmont Group. Where applicable the provisions of information sharing arrangements between FIUs should also be observed.

2. Requests for information should be submitted as soon as the precise assistance required is identified.

3. When an FIU has information that might be useful to another FIU, it should consider supplying it spontaneously as soon as the relevance of sharing this information is identified.

4. The exchange of information between Egmont FIUs should take place in a secure way. To this end the Egmont FIUs should use the Egmont Secure Web (ESW) where appropriate.

5. If necessary the requesting FIU should indicate the time by which it needs to receive an answer. Where a request is marked "urgent" or a deadline is indicated, the reasons for the urgency or deadline should be explained. All FIUs should refrain from arbitrary use of this terminology. When the requested information is only partially urgent, the request for information should use the 'urgent' mark only for the relevant sections. The requesting FIU should indicate if it desires an acknowledgment of receipt of the request. The requesting FIU may not require an acknowledgment (orally or in writing) unless the request is marked "urgent" by that FIU or, in its view, an acknowledgment is necessary in the light of the circumstances of the case. An urgent request should include the contact information for the individual responsible for sending the request.

6. Where appropriate, especially in the case of urgent requests, and in order to speed up proceedings, the requesting FIU may ask for prior consent for further use of the information to be granted directly together with the reply itself.

7. The Egmont Group has developed a request for information form. The use of this form should be encouraged, when exchanging information.

8. Requests should contain sufficient background information to enable the requested FIU to conduct proper analysis/investigation.

Requests shall be accompanied by a brief statement of the relevant facts known to the requesting FIU. Particular attention should be paid to:

- the information identifying the persons or companies involved (at least name and date of birth for individuals and name and registered office for companies);
- the reported suspicious or unusual transactions or activities, including the involved accounts;
- the *modus operandi* or circumstances in which the transactions or activities took place;
- whether the request for information is based on one or more disclosures or whether it has another base, such as a request from a national police authority, a list of suspected terrorists… ;
- the link with the country of the requested FIU.

9. Requests for information that are not related to a specific country and that are being sent to several FIUs at the same time should be justified as much as possible, providing an overview of the underlying facts. Also the request should be targeted as precisely as possible. The FIU should therefore refrain from using group mailings unnecessarily and should consider carrying out preliminary research into the transactions in order to identify a possible target cluster of FIUs that are more likely to have the relevant information at their disposal.

2) PROCESSING THE REQUEST

1. Except if indicated otherwise, all incoming requests for information originating from a counterpart FIU should be answered, also in case of a negative reply.

2. The request should be dealt with as soon as possible upon receipt.

3. FIUs should assign unique case reference numbers on both outgoing and incoming case requests to facilitate tracking of a particular case request or response.

4. Where a request is acknowledged, the requested FIU concerned should provide the requesting unit with the name and contact details, including telephone and fax numbers, of the contact person and the case or reference number assigned to the case by the responding FIU.

5. FIUs should give priority to urgent requests. If the receiving FIU has concerns about the classification of a request as urgent, it should contact the requesting FIU immediately in order to resolve the issue. Moreover each request, whether or not marked as “urgent”, should be processed in the same timely manner as domestic requests for information.

6.a As a general principle, the requested FIU should strive to reply to a request for information, including an interim response, within 1 week from receipt in the following circumstances:

- if it can provide a positive/negative answer to a request regarding information it has direct access to;
- if it is unable to provide an answer due to legal impediments.

6.b Whenever the requested FIU needs to have external databases searched or query third parties (such as financial institutions), an answer should be provided within 1 month after receipt of the request. The requested FIU may consider contacting the requesting unit within 1 week from receipt to state that it has no information directly available and that external sources are being consulted or that it is experiencing particular difficulties in answering the request. The latter may be done orally.

6.c If the results of the enquiries are still not all available after 1 month, the requested FIU should provide the information it already has in its possession or at least give an indication of when it will be in a position to provide a complete answer. This may be done orally.

7. FIUs should consider establishing mechanisms in order to monitor request-related information, enabling them to detect new information they receive regarding transactions, STRs, etc. that are involved in previously received requests. Such a monitoring system would enable FIUs to inform former requestors of new and relevant material related to their prior request.

3) REPLY

1. Where the requested FIU desires feedback on how the information it provided was used, it should request this explicitly. When the requesting FIU is not able to obtain this information, it should reply stating the reasons why the requested feedback cannot be provided.

2. If appropriate, especially in case of urgent requests, and in order to speed up proceedings, prior consent for further use of the information can be granted with the reply itself.

3. The exchange of information between FIUs should take place in a secure way. To this end the Egmont FIUs should use the Egmont Secure Web (ESW) where appropriate.

4) CONFIDENTIALITY

1. All FIUs should use the greatest caution when dealing with supplied information in order to prevent any unauthorized use resulting in a breach of confidentiality.

Appendix

VII

FATF 40 Recommendations (2003)

Note: Only those recommendations directly related to FIUs have been included. Recommendations marked with an asterisk should be read in conjunction with their Interpretative Notes.

[...]

Reporting of suspicious transactions and compliance

13.* If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, directly by law or regulation, to report promptly its suspicions to the financial intelligence unit (FIU).

14.* Financial institutions, their directors, officers and employees should be:

a) Protected by legal provisions from criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the FIU, even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.

b) Prohibited by law from disclosing the fact that a suspicious transaction report (STR) or related information is being reported to the FIU.

15.* Financial institutions should develop programmes against money laundering and terrorist financing. These programmes should include:

a) The development of internal policies, procedures and controls, including appropriate compliance management arrangements, and adequate screening procedures to ensure high standards when hiring employees.

b) An ongoing employee training programme.

c) An audit function to test the system.

16.* The requirements set out in Recommendations 13 to 15, and 21 apply to all designated nonfinancial businesses and professions, subject to the following qualifications:

a) Lawyers, notaries, other independent legal professionals and accountants should be required to report suspicious transactions when, on behalf of or for a client, they engage in a financial transaction in relation to the activities described in Recommendation 12(d). Countries

are strongly encouraged to extend the reporting requirement to the rest of the professional activities of accountants, including auditing.

b) Dealers in precious metals and dealers in precious stones should be required to report suspicious transactions when they engage in any cash transaction with a customer equal to or above the applicable designated threshold.

c) Trust and company service providers should be required to report suspicious transactions for a client when, on behalf of or for a client, they engage in a transaction in relation to the activities referred to Recommendation 12(e).

Lawyers, notaries, other independent legal professionals, and accountants acting as independent legal professionals, are not required to report their suspicions if the relevant information was obtained in circumstances where they are subject to professional secrecy or legal professional privilege.

Other measures to deter money laundering and terrorist financing

17. Countries should ensure that effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, are available to deal with natural or legal persons covered by these Recommendations that fail to comply with anti-money laundering or terrorist financing requirements.

18. Countries should not approve the establishment or accept the continued operation of shell banks. Financial institutions should refuse to enter into, or continue, a correspondent banking relationship with shell banks. Financial institutions should also guard against establishing relations with respondent foreign financial institutions that permit their accounts to be used by shell banks.

19.* Countries should consider:

a) Implementing feasible measures to detect or monitor the physical cross-border transportation of currency and bearer negotiable instruments, subject to strict safeguards to ensure proper use of information and without impeding in any way the freedom of capital movements.

b) The feasibility and utility of a system where banks and other financial institutions and intermediaries would report all domestic and international currency transactions above a fixed amount, to a national central agency with a computerised data base, available to competent authorities for use in money laundering or terrorist financing cases, subject to strict safeguards to ensure proper use of the information.

20. Countries should consider applying the FATF Recommendations to businesses and professions, other than designated non-financial businesses and professions, that pose a money laundering or terrorist financing risk. Countries

should further encourage the development of modern and secure techniques of money management that are less vulnerable to money laundering.

Measures to be taken with respect to countries that do not or insufficiently comply with the FATF Recommendations

21. Financial institutions should give special attention to business relationships and transactions with persons, including companies and financial institutions, from countries which do not or insufficiently apply the FATF Recommendations. Whenever these transactions have no apparent economic or visible lawful purpose, their background and purpose should, as far as possible, be examined, the findings established in writing, and be available to help competent authorities. Where such a country continues not to apply or insufficiently applies the FATF Recommendations, countries should be able to apply appropriate countermeasures.

22. Financial institutions should ensure that the principles applicable to financial institutions, which are mentioned above are also applied to branches and majority owned subsidiaries located abroad, especially in countries which do not or insufficiently apply the FATF Recommendations, to the extent that local applicable laws and regulations permit. When local applicable laws and regulations prohibit this implementation, competent authorities in the country of the parent institution should be informed by the financial institutions that they cannot apply the FATF Recommendations.

[...]

Competent authorities, their powers and resources

26.* Countries should establish a FIU that serves as a national centre for the receiving (and, as permitted, requesting), analysis and dissemination of STR and other information regarding potential money laundering or terrorist financing. The FIU should have access, directly or indirectly, on a timely basis to the financial, administrative and law enforcement information that it requires to properly undertake its functions, including the analysis of STR.

27.* Countries should ensure that designated law enforcement authorities have responsibility for money laundering and terrorist financing investigations. Countries are encouraged to support and develop, as far as possible, special investigative techniques suitable for the investigation of money laundering, such as controlled delivery, undercover operations and other relevant techniques. Countries are also encouraged to use other effective mechanisms such as the use of permanent or temporary groups specialised in asset investigation, and co-operative investigations with appropriate competent authorities in other countries.

28. When conducting investigations of money laundering and underlying predicate offences, competent authorities should be able to obtain documents

and information for use in those investigations, and in prosecutions and related actions. This should include powers to use compulsory measures for the production of records held by financial institutions and other persons, for the search of persons and premises, and for the seizure and obtaining of evidence.

29. Supervisors should have adequate powers to monitor and ensure compliance by financial institutions with requirements to combat money laundering and terrorist financing, including the authority to conduct inspections. They should be authorised to compel production of any information from financial institutions that is relevant to monitoring such compliance, and to impose adequate administrative sanctions for failure to comply with such requirements.

30. Countries should provide their competent authorities involved in combating money laundering and terrorist financing with adequate financial, human and technical resources. Countries should have in place processes to ensure that the staff of those authorities are of high integrity.

31. Countries should ensure that policy makers, the FIU, law enforcement and supervisors have effective mechanisms in place which enable them to co-operate, and where appropriate coordinate domestically with each other concerning the development and implementation of policies and activities to combat money laundering and terrorist financing.

32. Countries should ensure that their competent authorities can review the effectiveness of their systems to combat money laundering and terrorist financing systems by maintaining comprehensive statistics on matters relevant to the effectiveness and efficiency of such systems. This should include statistics on the STR received and disseminated; on money laundering and terrorist financing investigations, prosecutions and convictions; on property frozen, seized and confiscated; and on mutual legal assistance or other international requests for co-operation.

[...]

Other forms of co-operation

40.* Countries should ensure that their competent authorities provide the widest possible range of international co-operation to their foreign counterparts. There should be clear and effective gateways to facilitate the prompt and constructive exchange directly between counterparts, either spontaneously or upon request, of information relating to both money laundering and the underlying predicate offences. Exchanges should be permitted without unduly restrictive conditions. In particular:

a) Competent authorities should not refuse a request for assistance on the sole ground that the request is also considered to involve fiscal matters.

b) Countries should not invoke laws that require financial institutions to maintain secrecy or confidentiality as a ground for refusing to provide co-operation.

c) Competent authorities should be able to conduct inquiries; and where possible, investigations; on behalf of foreign counterparts.

Where the ability to obtain information sought by a foreign competent authority is not within the mandate of its counterpart, countries are also encouraged to permit a prompt and constructive exchange of information with non-counterparts. Co-operation with foreign authorities other than counterparts could occur directly or indirectly. When uncertain about the appropriate avenue to follow, competent authorities should first contact their foreign counterparts for assistance.

Countries should establish controls and safeguards to ensure that information exchanged by competent authorities is used only in an authorised manner, consistent with their obligations concerning privacy and data protection.

Glossary

"**Core Principles**" refers to the Core Principles for Effective Banking Supervision issued by the Basel Committee on Banking Supervision, the Objectives and Principles for Securities Regulation issued by the International Organization of Securities Commissions, and the Insurance Supervisory Principles issued by the International Association of Insurance Supervisors.

"**Designated categories of offences**" means:

- participation in an organised criminal group and racketeering;
- terrorism, including terrorist financing;
- trafficking in human beings and migrant smuggling;
- sexual exploitation, including sexual exploitation of children;
- illicit trafficking in narcotic drugs and psychotropic substances;
- illicit arms trafficking;
- illicit trafficking in stolen and other goods;
- corruption and bribery;
- fraud;
- counterfeiting currency;
- counterfeiting and piracy of products;
- environmental crime;
- murder, grievous bodily injury;
- kidnapping, illegal restraint and hostage-taking;
- robbery or theft;
- smuggling;
- extortion;
- forgery;
- piracy; and

- insider trading and market manipulation.

When deciding on the range of offences to be covered as predicate offences under each of the categories listed above, each country may decide, in accordance with its domestic law, how it will define those offences and the nature of any particular elements of those offences that make them serious offences.

"**Designated non-financial businesses and professions**" means:

a) Casinos (which also includes internet casinos).
b) Real estate agents.
c) Dealers in precious metals.
d) Dealers in precious stones.
e) Lawyers, notaries, other independent legal professionals and accountants – this refers to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to 'internal' professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to measures that would combat money laundering.
f) Trust and Company Service Providers refers to all persons or businesses that are not covered elsewhere under these Recommendations, and which as a business, provide any of the following services to third parties:

    - acting as a formation agent of legal persons;
    - acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
    - providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
    - acting as (or arranging for another person to act as) a trustee of an express trust;
    - acting as (or arranging for another person to act as) a nominee shareholder for another person.

"**Designated threshold**" refers to the amount set out in the Interpretative Notes.

"Financial institutions" means any person or entity who conducts as a business one or more of the following activities or operations for or on behalf of a customer:

1. Acceptance of deposits and other repayable funds from the public.[1]
2. Lending.[2]
3. Financial leasing.[3]
4. The transfer of money or value.[4]
5. Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money).
6. Financial guarantees and commitments.
7. Trading in:
   (a) money market instruments (cheques, bills, CDs, derivatives etc.);
   (b) foreign exchange;
   (c) exchange, interest rate and index instruments;
   (d) transferable securities;
   (e) commodity futures trading.
8. Participation in securities issues and the provision of financial services related to such issues.
9. Individual and collective portfolio management.
10. Safekeeping and administration of cash or liquid securities on behalf of other persons.
11. Otherwise investing, administering or managing funds or money on behalf of other persons.
12. Underwriting and placement of life insurance and other investment related insurance.[5]
13. Money and currency changing.

When a financial activity is carried out by a person or entity on an occasional or very limited basis (having regard to quantitative and absolute criteria) such that there is little risk of money laundering activity occurring, a country may

---

[1] This also captures private banking.

[2] This includes inter alia: consumer credit; mortgage credit; factoring, with or without recourse; and finance of commercial transactions (including forfaiting).

[3] This does not extend to financial leasing arrangements in relation to consumer products.

[4] This applies to financial activity in both the formal or informal sector e.g. alternative remittance activity. See the Interpretative Note to Special Recommendation VI. It does not apply to any natural or legal person that provides financial institutions solely with message or other support systems for transmitting funds. See the Interpretative Note to Special Recommendation VII.

[5] This applies both to insurance undertakings and to insurance intermediaries (agents and brokers).

decide that the application of anti-money laundering measures is not necessary, either fully or partially.

In strictly limited and justified circumstances, and based on a proven low risk of money laundering, a country may decide not to apply some or all of the Forty Recommendations to some of the financial activities stated above.

"**FIU**" means financial intelligence unit.

Interpretative Notes

Recommendation 13

1. The reference to criminal activity in Recommendation 13 refers to: a) all criminal acts that would constitute a predicate offence for money laundering in the jurisdiction; or b) at a minimum to those offences that would constitute a predicate offence as required by Recommendation 1. Countries are strongly encouraged to adopt alternative (a). All suspicious transactions, including attempted transactions, should be reported regardless of the amount of the transaction.

2. In implementing Recommendation 13, suspicious transactions should be reported by financial institutions regardless of whether they are also thought to involve tax matters. Countries should take into account that, in order to deter financial institutions from reporting a suspicious transaction, money launderers may seek to state *inter alia* that their transactions relate to tax matters.

Recommendation 14 (tipping off)

Where lawyers, notaries, other independent legal professionals and accountants acting as independent legal professionals seek to dissuade a client from engaging in illegal activity, this does not amount to tipping off.

Recommendation 15

The type and extent of measures to be taken for each of the requirements set out in the Recommendation should be appropriate having regard to the risk of money laundering and terrorist financing and the size of the business.

For financial institutions, compliance management arrangements should include the appointment of a compliance officer at the management level.

Recommendation 16

1. It is for each jurisdiction to determine the matters that would fall under legal professional privilege or professional secrecy. This would normally cover information lawyers, notaries or other independent legal professionals receive from or obtain through one of their clients: (a) in the course of ascertaining the legal position of their client, or (b) in performing their task of defending or representing that client in, or concerning judicial, administrative, arbitration or

mediation proceedings. Where accountants are subject to the same obligations of secrecy or privilege, then they are also not required to report suspicious transactions.

2. Countries may allow lawyers, notaries, other independent legal professionals and accountants to send their STR to their appropriate self-regulatory organisations, provided that there are appropriate forms of co-operation between these organisations and the FIU.

[...]

Recommendation 19

1. To facilitate detection and monitoring of cash transactions, without impeding in any way the freedom of capital movements, countries could consider the feasibility of subjecting all crossborder transfers, above a given threshold, to verification, administrative monitoring, declaration or record keeping requirements.

2. If a country discovers an unusual international shipment of currency, monetary instruments, precious metals, or gems, etc., it should consider notifying, as appropriate, the Customs Service or other competent authorities of the countries from which the shipment originated and/or to which it is destined, and should co-operate with a view toward establishing the source, destination, and purpose of such shipment and toward the taking of appropriate action.

[...]

Recommendation 26

Where a country has created an FIU, it should consider applying for membership in the Egmont Group. Countries should have regard to the Egmont Group Statement of Purpose, and its Principles for Information Exchange Between Financial Intelligence Units for Money Laundering Cases. These documents set out important guidance concerning the role and functions of FIUs, and the mechanisms for exchanging information between FIU[s].

Recommendation 27

Countries should consider taking measures, including legislative ones, at the national level, to allow their competent authorities investigating money laundering cases to postpone or waive the arrest of suspected persons and/or the seizure of the money for the purpose of identifying persons involved in such activities or for evidence gathering. Without such measures the use of procedures such as controlled deliveries and undercover operations are precluded.

[...]

Recommendation 40

1. For the purposes of this Recommendation:

- "Counterparts" refers to authorities that exercise similar responsibilities and functions.
- "Competent authority" refers to all administrative and law enforcement authorities concerned with combating money laundering and terrorist financing, including the FIU and supervisors.

2. Depending on the type of competent authority involved and the nature and purpose of the cooperation, different channels can be appropriate for the exchange of information. Examples of mechanisms or channels that are used to exchange information include: bilateral or multilateral agreements or arrangements, memoranda of understanding, exchanges on the basis of reciprocity, or through appropriate international or regional organisations. However, this Recommendation is not intended to cover co-operation in relation to mutual legal assistance or extradition.

3. The reference to indirect exchange of information with foreign authorities other than counterparts covers the situation where the requested information passes from the foreign authority through one or more domestic or foreign authorities before being received by the requesting authority. The competent authority that requests the information should always make it clear for what purpose and on whose behalf the request is made.

4. FIUs should be able to make inquiries on behalf of foreign counterparts where this could be relevant to an analysis of financial transactions. At a minimum, inquiries should include:

- Searching its own databases, which would include information related to suspicious transaction reports.
- Searching other databases to which it may have direct or indirect access, including law enforcement databases, public databases, administrative databases and commercially available databases.

Where permitted to do so, FIUs should also contact other competent authorities and financial institutions in order to obtain relevant information.

Appendix

VIII

FATF Special Recommendations on Terrorist Financing

[...]

IV. Reporting suspicious transactions related to terrorism

If financial institutions, or other businesses or entities subject to anti-money laundering obligations, suspect or have reasonable grounds to suspect that funds are linked or related to, or are to be used for terrorism, terrorist acts or by terrorist organisations, they should be required to report promptly their suspicions to the competent authorities.

V. International co-operation

Each country should afford another country, on the basis of a treaty, arrangement or other mechanism for mutual legal assistance or information exchange, the greatest possible measure of assistance in connection with criminal, civil enforcement, and administrative investigations, inquiries and proceedings relating to the financing of terrorism, terrorist acts and terrorist organisations.

Countries should also take all possible measures to ensure that they do not provide safe havens for individuals charged with the financing of terrorism, terrorist acts or terrorist organisations, and should have procedures in place to extradite, where possible, such individuals.

Appendix

IX

International Convention for the Suppression of the Financing of Terrorism

[...]

Article 18

1. States Parties shall cooperate in the prevention of the offences set forth in article 2 by taking all practicable measures, *inter alia*, by adapting their domestic legislation, if necessary, to prevent and counter preparations in their respective territories for the commission of those offences within or outside their territories, including:

(a) Measures to prohibit in their territories illegal activities of persons and organizations that knowingly encourage, instigate, organize or engage in the commission of offences set forth in article 2;

(b) Measures requiring financial institutions and other professions involved in financial transactions to utilize the most efficient measures available for the identification of their usual or occasional customers, as well as customers in whose interest accounts are opened, and to pay special attention to unusual or suspicious transactions and report transactions suspected of stemming from a criminal activity. For this purpose, States Parties shall consider:

(i) Adopting regulations prohibiting the opening of accounts the holders or beneficiaries of which are unidentified or unidentifiable, and measures to ensure that such institutions verify the identity of the real owners of such transactions;

(ii) With respect to the identification of legal entities, requiring financial institutions, when necessary, to take measures to verify the legal existence and the structure of the customer by obtaining, either from a public register or from the customer or both, proof of incorporation, including information concerning the customer's name, legal form, address, directors and provisions regulating the power to bind the entity;

(iii) Adopting regulations imposing on financial institutions the obligation to report promptly to the competent authorities all complex, unusual large transactions and unusual patterns of transactions, which have no apparent economic or obviously lawful purpose, without fear of assuming criminal or civil liability for breach of any restriction on disclosure of information if they report their suspicions in good faith;

(iv) Requiring financial institutions to maintain, for at least five years, all necessary records on transactions, both domestic or international.

2. States Parties shall further cooperate in the prevention of offences set forth in article 2 by considering:

(a) Measures for the supervision, including, for example, the licensing, of all money-transmission agencies;

(b) Feasible measures to detect or monitor the physical cross-border transportation of cash and bearer negotiable instruments, subject to strict safeguards to ensure proper use of information and without impeding in any way the freedom of capital movements.

3. States Parties shall further cooperate in the prevention of the offences set forth in article 2 by exchanging accurate and verified information in accordance with their domestic law and coordinating administrative and other measures taken, as appropriate, to prevent the commission of offences set forth in article 2, in particular by:

(a) Establishing and maintaining channels of communication between their competent agencies and services to facilitate the secure and rapid exchange of information concerning all aspects of offences set forth in article 2;

(b) Cooperating with one another in conducting inquiries, with respect to the offences set forth in article 2, concerning:

(i) The identity, whereabouts and activities of persons in respect of whom reasonable suspicion exists that they are involved in such offences;

(ii) The movement of funds relating to the commission of such offences.

4. States Parties may exchange information through the International Criminal Police Organization (Interpol).

Appendix

X

United Nations Convention Against Transnational Organized Crime

[...]

Article 7

Measures to combat money-laundering

1. Each State Party:

(a) Shall institute a comprehensive domestic regulatory and supervisory regime for banks and non-bank financial institutions and, where appropriate, other bodies particularly susceptible to money-laundering, within its competence, in order to deter and detect all forms of money-laundering, which regime shall emphasize requirements for customer identification, record-keeping and the reporting of suspicious transactions;

(b) Shall, without prejudice to articles 18 and 27 of this Convention, ensure that administrative, regulatory, law enforcement and other authorities dedicated to combating money-laundering (including, where appropriate under domestic law, judicial authorities) have the ability to cooperate and exchange information at the national and international levels within the conditions prescribed by its domestic law and, to that end, shall consider the establishment of a financial intelligence unit to serve as a national centre for the collection, analysis and dissemination of information regarding potential money-laundering.

2. States Parties shall consider implementing feasible measures to detect and monitor the movement of cash and appropriate negotiable instruments across their borders, subject to safeguards to ensure proper use of information and without impeding in any way the movement of legitimate capital. Such measures may include a requirement that individuals and businesses report the cross-border transfer of substantial quantities of cash and appropriate negotiable instruments.

3. In establishing a domestic regulatory and supervisory regime under the terms of this article, and without prejudice to any other article of this Convention, States Parties are called upon to use as a guideline the relevant initiatives of regional, interregional and multilateral organizations against money-laundering.

4. States Parties shall endeavour to develop and promote global, regional, subregional and bilateral cooperation among judicial, law enforcement and financial regulatory authorities in order to combat money-laundering.

Appendix

XI

United Nations Convention Against Corruption

[...]

Article 14

Measures to prevent money-laundering

1. Each State Party shall:

(a) Institute a comprehensive domestic regulatory and supervisory regime for banks and non-bank financial institutions, including natural or legal persons that provide formal or informal services for the transmission of money or value and, where appropriate, other bodies particularly susceptible to money-laundering, within its competence, in order to deter and detect all forms of money-laundering, which regime shall emphasize requirements for customer and, where appropriate, beneficial owner identification, record-keeping and the reporting of suspicious transactions;

(b) Without prejudice to article 46 of this Convention, ensure that administrative, regulatory, law enforcement and other authorities dedicated to combating money-laundering (including, where appropriate under domestic law, judicial authorities) have the ability to cooperate and exchange information at the national and international levels within the conditions prescribed by its domestic law and, to that end, shall consider the establishment of a financial intelligence unit to serve as a national centre for the collection, analysis and dissemination of information regarding potential money-laundering.

2. States Parties shall consider implementing feasible measures to detect and monitor the movement of cash and appropriate negotiable instruments across their borders, subject to safeguards to ensure proper use of information and without impeding in any way the movement of legitimate capital. Such measures may include a requirement that individuals and businesses report the cross-border transfer of substantial quantities of cash and appropriate negotiable instruments.

3. States Parties shall consider implementing appropriate and feasible measures to require financial institutions, including money remitters:

(a) To include on forms for the electronic transfer of funds and related messages accurate and meaningful information on the originator;

(b) To maintain such information throughout the payment chain; and

(c) To apply enhanced scrutiny to transfers of funds that do not contain complete information on the originator.

4. In establishing a domestic regulatory and supervisory regime under the terms of this article, and without prejudice to any other article of this Convention, States Parties are called upon to use as a guideline the relevant initiatives of regional, interregional and multilateral organizations against money-laundering.

5. States Parties shall endeavour to develop and promote global, regional, subregional and bilateral cooperation among judicial, law enforcement and financial regulatory authorities in order to combat money-laundering.

BIBLIOGRAPHY

Basel Committee on Banking Supervision, 1997, *Basel Core Principles for Effective Banking Supervision*.

Bell, R.E., 2002, "The Prosecution of Lawyers for Money Laundering," *Journal of Money Laundering Control*, Vol. 6, No. 1, pp. 17–26.

Brown, Alastair, 1997, "Money Laundering: A European and U.K. Perspective," *J.I.B.L*, Vol. 8, p. 307.

Council of Europe, European Committee on Crime Problems, Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures, *A Review of the Anti-Money Laundering Systems in 22 Council of Europe Member States, 1998–2001*.

de Koker, Louis, 2002, "Money Laundering Control: The South African Model," *Journal of Money Laundering Control*, pp. 166–81.

Financial Action Task Force (FATF), 2001, *Review of FATF Anti-Money Laundering Systems and Mutual Evaluation Procedures, 1992–1999*.

———, 2002, *Review of the FATF Forty Recommendations, Consultation Paper, May 30.*

FinCEN*, 2002, Use of Currency Transaction Reports, Report to the Congress submitted by the Financial Crimes Enforcement Network on behalf of the U.S. Department of the Treasury.*

Gilmore, William C., 1999, *Dirty Money: The Evolution of Money-Laundering Counter-Measures*, 2nd ed. (Strasbourg: Council of Europe Press).

International Association of Insurance Supervisors (IAIS), 2003, *Insurance Core Principles and Methodology*, ICP 28.

International Organization of Securities Commissions (IOSCO), 2002, *Objectives and Principles of Securities Regulation*.

Schott, Paul Allan, 2003, *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* (Washington: World Bank and International Monetary Fund).

Sienczylo-Chlabicz, Joanna, and Wojciech Filipkowski, 2001, "The Polish Financial Intelligence Unit: A New Institution in the Polish Legal System," *Journal of Money Laundering Control*, Vol. 5, No. 2, pp. 150–57.

Spreutels, Jean, and Claire Scohier, 1998, "*La Prévention du blanchiment des capitaux, évolutions récentes*," *Rev. Dr. ULB*, 1997-1, pp. 165–87, available on the website of the Belgian FIU at *http://www.ctif-cfi.be/fr/index.htm*.

Stessens, Guy, 2000, *Money Laundering, A New International Law Enforcement Model* (Cambridge, England: Cambridge University Press).

Thony, Jean-François, 1996, "Processing Financial Information in Money Laundering Matters, The Financial Intelligence Units," *European Journal of Crime, Criminal Law and Criminal Justice* (Brussels), p. 257.

van Duyne, Petrus C., Marcel Pheijffer, Hans G. Kuijl, Arthur Th.H. van Dijk, and Gerard J.C.M. Bakker, 2003, *Financial Investigation of Crime: A Tool of the Integral Law Enforcement Approach* (Nijmegen: Wolf Legal Publishers).

Verhelst, Boudewijn, *The Financial Intelligence Units in the International Context*, Egmont Group.