

**EGMONT GROUP OF FINANCIAL INTELLIGENCE UNITS
OPERATIONAL GUIDANCE FOR FIU ACTIVITIES AND
THE EXCHANGE OF INFORMATION**

**Approved by the Egmont Group Heads of Financial Intelligence Units July
2013, revised February 2017**

Table of Contents

A. Introduction	3
B. General framework.....	4
C. Egmont operational guidance.....	4
GUIDANCE FOR INTERNATIONAL CO-OPERATION AND INFORMATION EXCHANGE.....	4
Channels for information exchange.....	4
Memoranda of Understanding between FIUs	5
Guidance for FIUs making requests	5
Guidance for FIUs receiving requests	7
Networking and multilateral co-operation	8
Reciprocity	8
Diagonal co-operation.....	9
GUIDANCE FOR OTHER FIU ACTIVITIES.....	9
Enhancing Information Exchange on Terrorism Financing Issues.....	9
Receipt function	10
Analysis function	11
Types of analysis	11
Collection, evaluation, verification and collation of information and analysis	13
Power to obtain information from reporting entities	14
Power to access information from other sources	16
Table of Amendments.....	19
Annex A: Sample query form	26
Annex B: Sample Spontaneous Disclosure cover letter	29
Annex C: Promoting the role of FIUs in national counter - terrorism apparatus	30

EGMONT GROUP OF FINANCIAL INTELLIGENCE UNITS OPERATIONAL GUIDANCE FOR FIU ACTIVITIES AND THE EXCHANGE OF INFORMATION

Keeping in mind the diversity of the Egmont Group membership, this document has been created to provide guidance to Financial Intelligence Units (FIUs) in relation to international co-operation, information exchange and other FIU activities. It provides a framework to which the Egmont Group membership, as a whole, can aspire. FIUs are strongly encouraged to implement these guidelines to the greatest extent possible.

A. Introduction

- 1) The Egmont Group of Financial Intelligence Units Charter and the Principles for Information Exchange between Financial Intelligence Units are obligatory documents and their elements are subject to the Support and Compliance Process. The Operational Guidance for FIU Activities and the Exchange of Information can assist FIUs to become more effective and efficient; however, its elements are not subject to the Support and Compliance Process.
- 2) Member FIUs have identified a need to maximize/optimize information exchange and effective/efficient co-operation among and between FIUs.
- 3) As such, FIUs are encouraged to ensure that national legal standards do not inhibit the exchange of information between or among FIUs. In this essence, the Egmont Group membership affirms accession to the standards set out in the Financial Action Task Force (FATF) Recommendations and associating Interpretative Notes on *Financial Intelligence Units (Recommendation 29)* and *Other Forms of International Co-operation (Recommendation 40)*. Members are responsible to familiarize themselves with these requirements as they have not been reiterated in this document. Where the language of FATF Recommendations 29 and 40 have been reiterated in this document, it is footnoted.

B. General framework

- 4) This document is expected to evolve and strengthen over time as the Egmont Group identifies better practices and applications that assist Egmont members.
- 5) As such, additional operational guidance may result from studies and projects created by Egmont Working Groups. Although not required, member FIUs should endeavour to use these results to inform their practices when engaging in international co-operation and information exchange.

C. Egmont operational guidance

GUIDANCE FOR INTERNATIONAL CO-OPERATION AND INFORMATION EXCHANGE

- 6) Irrespective of differences in the definition of the predicate offences, FIUs should strive for the free exchange of information between FIUs.
- 7) FIUs are encouraged to discover alternative means to co-operate when confronted with obstacles.
- 8) The Egmont Group encourages the broadest information exchange and does not limit this to Egmont Group members exclusively. However, it is within the rights of every FIU to decide only to exchange information with Egmont Group members.

Channels for information exchange

- 9) FIUs are encouraged to have procedures in place to ensure that the connection to Egmont Secure Web (ESW) is adequately maintained and that it is accessed on a regular and consistent basis to ensure the timely receipt of requests for information. Ideally, FIUs should check the ESW daily, especially to ensure urgent requests are suitably addressed. The same recommendations apply for FIUs using other secure channels to exchange information.

Memoranda of Understanding between FIUs

- 10) Whenever possible, exchanges of information should take place without the need for a Memorandum of Understanding (MOU).
- 11) In cases where FIUs are required by domestic legislation to enter into MOUs in order to exchange information, consider:
 - not imposing undue impediments or limitations on the exchange of information; and
 - making all efforts to enter into such MOUs before co-operation is requested by foreign counterpart FIUs.
- 12) FIUs that do not require an MOU to share information should make their best efforts to co-operate by establishing MOUs with those FIUs that do require MOUs to share information.
- 13) FIUs that receive requests to enter into MOUs should consider prioritizing requests that come from FIUs that require MOUs by law.
- 14) Ideally, the FIU making the requesting should send a letter of interest, the text of the proposed MOU, and the relevant domestic legislation to their foreign counterpart FIU. The FIU receiving the request should endeavour to respond within a reasonable period of time, indicating proposed revisions to the draft MOU and enclosing relevant domestic provisions. Once an agreed MOU has been reached, the parties should arrange the means for signing the memorandum.
- 15) The Egmont Group provides a model MOU which FIUs are free to use in negotiations.

Guidance for FIUs making requests

- 16) FIUs should endeavour to co-operate with foreign counterpart FIUs as soon as the assistance required is identified.
- 17) If necessary, the FIU making the request can identify a deadline or an urgent request, including justification. This will allow the FIU receiving the request to accurately prioritize the request. Where a request is only deemed partially urgent, the relevant urgent sections should be clearly

identified. FIUs should refrain from arbitrary use of this terminology. Requests designated as urgent should remain the exception rather than the rule.

18) Where appropriate, especially in the case of urgent requests, and 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. In such cases, the FIU making the request is required to give all details necessary for the FIU receiving the request to determine whether prior consent can be granted (for example, purpose of the request, institution, to whom the information will be disclosed and for what reason).

19) FIUs requesting information are encouraged to disclose all information needed so the FIU receiving the request can properly process the request. This information ideally includes:

- the reason for the request;
- a description of the suspicious activities under analysis is and the grounds for suspicion;
- details of the persons or companies involved (name and date of birth for individuals; name and registered office for companies) as well as the transactions and the accounts used.
- the information requested and the purpose for which it will be used, including, if foreseen, further dissemination;
- whether the request for information is based on reports or information received or is on behalf of another authority. If the request is on behalf of another domestic agency, that agency should be clearly identified along with the expected use of the information;
- whether the FIU receiving the request is authorized to disclose the request, in full or in part, to third parties, if such disclosure is required to obtain the requested information;
- signature from authorizing official;
- range of period to be analyzed; and
- any need for urgency.

20) FIUs are encouraged to use the Egmont Request for FIU Information form and cover letter. Templates can be found in [Annex A](#) and [B](#).

Guidance for FIUs receiving requests

- 21) All incoming requests for information should be answered as soon as possible, whether positive or negative. Ideally, acknowledgement of receipt should include a case reference number, the case number of the FIU making the request, and contact details of the analyst responsible for responding to the FIU making the request. The turnaround time of each request may differ, depending on the nature of the request. While acknowledging the need for flexibility, the following turnaround times are provided as a guide:
- Responses: As deemed appropriate and timely, consistent with the urgency of the request, or within one month if possible. Additional time is reasonable if there is need to query external databases or third parties. Ideally, negative responses are provided as soon as possible.
 - Feedback: As deemed appropriate and upon request¹.
- 22) FIUs should consider prioritizing urgent requests, and liaise with the FIU making the request if there are any concerns about the classification of the request. Ideally, foreign counterpart FIU requests for information should be processed in the same timely manner as domestic request for information.
- 23) Where the FIU receiving the request needs to query external databases or third parties, they should consider informing the FIU making the request that such information is not directly available and that external sources are being consulted. If a long wait time is anticipated, the FIU receiving the request should consider providing the requesting FIU with the information readily available and identifying when they expect to be able to more fully reply.
- 24) Further, when FIUs need to approach third parties (for example, designated non- financial businesses and professions) to obtain requested information, the FIU receiving the request is encouraged to discuss this with the FIU making the request, to ensure that approaching third parties would not adversely affect their actions or inquiries/investigations.
- 25) FIUs should consider establishing mechanisms to monitor request -related information, enabling them to detect new information they receive that is related to previously received requests (information regarding transactions, Suspicious Transactions Report (STRs), other disclosures etc.). This would enable FIUs to inform former requestors of new and relevant material related to their prior request.

¹ FATF Recommendation 40, Interpretive Note paragraph 8.

26) The FIU receiving the request should identify if they want feedback on the usefulness of the information provided. When the FIU making the request is not able to provide such feedback, it should reply stating the reasons why the requested feedback cannot be provided.

27) Regarding quality of exchanged information, FIUs should consider the following elements:

- timeliness - timely assistance to the requesting FIU;
- coverage - the extent to which a response has covered the query;
- detail - the level of detail provided; and
- relevance - the added value provided relevant to the objective of the query.

FIUs are encouraged to communicate with one another, taking into consideration timeliness, coverage, detail and relevance of provided information.

Networking and multilateral co-operation

28) While in the midst of bilateral exchanges, FIUs may identify links or connections to additional countries. In such cases, the FIUs, upon consent, are encouraged to broaden the co-operation to include other relevant FIUs.

29) While acknowledging the prior consent rule, FIUs are encouraged to broaden co-operation when there are clear links to all countries involved.

Reciprocity

30) Differences in the available information or powers to access information for domestic analysis (which in turn depend upon differences in the analysis function carried out by FIUs) do not affect the condition of reciprocity *per se*.

31) Counterparts should be able to provide financial, administrative and law enforcement information and make use of the powers available for domestic analysis in order to obtain the requested information. FIUs involved in the exchange do not need to have access to, and the capacity to exchange, the same information.

Diagonal co-operation

- 32) The Egmont Group acknowledges that, under an FIU's national law, the FIU retains discretion on whether or not to engage in diagonal co-operation.
- 33) FIUs that decide to engage in diagonal co-operation with non-counterparts should consider using the FIU-to-FIU channel to ensure maximum protection and integrity of the STR information exchange. In such cases FIUs should consider the following process:
- When an FIU receives a request for STR information on behalf of a foreign non-counterpart, the response (which remains discretionary) should be sent to the counterpart FIU of the interested country to forward the information to the final recipient.
 - When an FIU wishes to request information which is needed for analysis from a foreign non-counterpart, it should approach the FIU of the interested country explaining the case, seeking direction on which authority should be approached, and asking that the request be forwarded to that authority.
 - The ESW or other recognized FIU-to-FIU channels should be used to exchange STR information.
- 34) However, in cases where FIUs, based on domestic legislation, are required or empowered to follow a different pattern of international co-operation, it is recommended that the FIU of the country where the non-FIU counterpart is located be informed about the request being filed or the information being provided.
- 35) It is recommended that foreign authorities inform the FIU receiving the request of the purpose of the request and expected use of the information. Any further use or dissemination should be specifically authorized by the FIU receiving the request.

GUIDANCE FOR OTHER FIU ACTIVITIES

Enhancing Information Exchange on Terrorism Financing Issues

- 36) FIUs should adopt and implement, to the greatest extent possible, initiatives to enhance information exchange related to terrorism financing issues in order to address key barriers identified by Egmont Group members, such as:

- Promoting the role of FIUs in the national counter-terrorism apparatus;
- Improving the quality of STRs;
- Overcoming barriers to sharing for intelligence purposes.

Examples of initiatives are attached as [Annex C](#).

Receipt function

37) In addition to STRs, FIUs may receive objective or threshold-based disclosures from reporting entities that relate to money laundering or the financing of terrorism. The scope and implementation of these reporting obligations will vary from one country to another based on national systems and obligations.

38) Examples of such disclosures that FIUs receive and use in their analytical work include:

- Reports of physical cross-border transportation of cash, bearer instruments or means of payment.
- Reports of transactions and payments in cash or bearer instruments, domestic or international.
- Reports on foreign currency transactions, domestic or international.
- Reports on wire transfers, domestic or international.
- Reports on complex, unusual large transactions.
- Reports on accounts held abroad by nationals or residents.
- Reports on the application of targeted financial sanctions.

39) When providing feedback to reporting entities on the effectiveness of the information received, or on the outcome and follow-up of the analysis conducted, FIUs can consider providing feedback as deemed feasible and include information on trends and patterns if useful. FIUs are encouraged to be mindful of judicial secrecy and presumption of innocence.

Analysis function

- 40) Based upon all the information available through STRs and other disclosures received, FIUs should seek to identify potential cases of money laundering or the financing of terrorism. The suspicion is higher if additional information compounds issues such as the complexity, strangeness or lack of legitimate rationale. The suspicion is lower if additional information points to legitimate rationale. Additional information can be obtained from the FIU's own databases or from external information sources. Cases or reports can then be graded as high priority (requiring full analysis and dissemination), medium priority (requiring ongoing analysis, more information) or low priority (requiring no immediate action).
- 41) Depending on the nature and the number of the STRs received, FIUs may perform analysis on individual STRs or bulk analysis using information technology (IT) tools. The number of STRs received by the FIU may result in a need to identify high priority STRs to be addressed rapidly, and low priority STRs to be addressed later.

Types of analysis

- 42) Operational analysis aims to identify specific targets (persons, assets, criminal networks etc.), possible proceeds of crime and the links between them². FIUs are highly encouraged to use effective IT tools to achieve the maximum advantage in analysis. Some components of operational analysis include:
- matching with predefined lists;
 - identifying all reports that pertain to the same entity, on the basis of various user defined attributes, such as first name, second name, date of birth, public identification (passport number etc.), and address components;
 - capturing all possible relationships, across multiple entities by comparing attributes such as surnames, phone numbers, addresses; and
 - analyzing relationships to form clusters of closely linked entities for various degrees of separation.
- 43) Strategic analysis aims to decipher the underlying patterns and trends that would enable an FIU to draw conclusions for the strategic prevention of money laundering and the financing of terrorism, and to provide input for policy formulation and for setting operational priorities. In

² FATF Recommendation 29, Interpretive Note paragraph 3.

an FIU context, this implies developing knowledge (strategic intelligence) as it relates to money laundering, the financing of terrorism and other threats to the security of a country's financial systems. Some components of strategic analysis include:

- examining data for patterns and similar concepts;
- developing a working hypothesis that addresses the “who”, “what”, “when”, “where”, “how”, and “why” of the activity;
- collecting, evaluating and collating further information as required;
- identifying connections or links between pieces of information, also used to support an inference;
- developing inferences (an inference is the best estimate of the truth that can be drawn from facts, opinions or other inferences); and
- constructing the argument, that is the logical flow of elements leading to the inference.

The sophistication of strategic analysis may vary based on the capacity and resources of the FIU.

Product ranges of strategic analysis may include:

- Typologies and trends — this is a systematic classification of a number of schemes that appear to be constructed in a similar fashion. These are built on a series of indicators that show how money was laundered, which in turn increases general understanding of an issue or method of money laundering or the financing of terrorism. When a typology occurs for any given event over a period of time, this can be classed as a trend. Changes in crime types or the way in which money is moved are examples of trends.
- Patterns — this is a recurring characteristic or trait that helps in the identification of a phenomenon/problem and that serves as an indicator or model for predicting future behaviour.
- Synthesis - This includes identifying connections that identify break-through ideas and opportunities in the detection of money laundering or the financing of terrorism.
- Geographical/regional analysis – This shows the area of influence or location of the phenomenon.
- Behavioural analysis - This shows the type of operations, institutions and products used by the group.
- Activity analysis - This focuses on identifying weaknesses of an economic sector or activity.
- Advanced intelligence products - These may include vulnerability assessments, risk assessments and significant event assessments.

Collection, evaluation, verification and collation of information and analysis

- 44) Analysis can be considered to be the conversion of information that has been collected, evaluated and collated into intelligence through the integration and interpretation of all data collected. Having reliable, accurate and timely information (often from diverse sources) is useful to perform both operational and strategic analysis. Starting with the information available from STRs and other disclosures received, the analyst can search the FIU database, and expand the search to other domestic sources and foreign partners. The search of domestic and foreign sources of information can include both closed (accessible to those with authority to access the information) and open (accessible to the general public) sources. FIUs are encouraged to have a policy about accessing websites to ensure that searches are not easily traceable.
- 45) The collection of information should ideally be planned, orderly and systematic, reducing the need for the analyst to be repetitive when searching for information, and ensuring conclusions are based on sound foundation. It is important to analyze the information source for reliability and validity. Data diagnostic involves evaluating data for its quality by evaluating its credibility (source), relevance (to the goal of the analysis), accuracy (for analysis to be reliable) and process to translate data into information.
- 46) After collecting all relevant information, it should ideally be collated to ensure that important information is not misplaced, misdirected or lost. Collation can be designed to effectively manage the information so as to maximize its usefulness. A good collation system will assist the analyst to: identify relationships between individuals and/or companies; determine significant events; identify patterns of activity; uncover information gaps; and clarify the significance of data collected. The source of information can be coded for easy retrieval later. IT tools can be used to collate large quantities of data. When it is necessary to work on smaller data sets out of a large volume of data, sampling, data grouping and sorting can be used, all of which can be performed through commercially available application software.
- 47) The relevant data, whether collected or already available in the FIU's databases, can be matched and linked to identify relationships. In operational analysis, where the emphasis is on case formation, it is important to match and link all relevant information, in order to have as complete a view of the case as possible. However, linking different reports for the same entity

or establishing relationships among different entities may pose a challenge due to factors such as variations in different attributes of the same entity (first name, surname, address etc.). Once all of the data is collected, evaluated and collated, it may be reviewed to ensure that all requisite information is available for analysis.

Power to obtain information from reporting entities

48) FIUs should be able to obtain and use additional information from reporting entities as needed to perform its analysis function³. The use of this power and its extent, including the range of the reporting entities from which the information should be obtained, is dependent on analytical needs. Relevant elements in this respect include:

- the features of the analytical tasks assigned to the FIU in that particular country;
- the information already available to the FIU as a consequence of the disclosures received under the receipt function (in principle, the wider this initial information, the less likely the need to obtain additional information from reporting entities subsequently); and
- the information available to the FIU via other sources.

49) Examples of the types of information that FIUs can obtain from reporting entities, depending on their analytical needs, include but are not limited⁴ to the following:

Source of information	Types of information
Reporting entities	Identification data of natural person:
	<i>a. Name and other identification data of the natural persons⁵</i>
	Identification data of legal person or legal arrangements:
	<i>a. Name, legal form and proof of existence (e.g. certificate of incorporation, a certificate of good standing, a partnership agreement, a deed of trust)</i>
	<i>b. The powers that regulate and bind the legal person or arrangement (e.g. the memorandum and articles of association of a company); the names of the</i>

³ FATF Recommendation 29, Interpretive Note section C (a) 5

⁴ Any other information gathered in the Customer Due Diligence (CDD) process, consistent with the risk circumstances and the type of CDD measures applied

⁵ E.g. data on the customer or the authorized person contained in the passport, identity card, driving license or other similar documents; date and place of birth; address information, etc.

	<i>relevant persons having a senior management position in the legal person or arrangement (e.g. senior managing directors in a company, trustee(s) of a trust).</i>
	<i>c. The address of the registered office, and, if different, a principal place of business.</i>
	Identification data of beneficial owner of the legal person or legal arrangements:
	<i>a. Identity of the natural persons who ultimately have a controlling ownership interest.</i>
	<i>b. Identity of the natural persons exercising control of the legal person or arrangement through other means.</i>
	<i>c. Identity of the relevant natural person who holds the position of senior managing official.</i>
	<i>d. For Trusts – the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust (including through a chain of control/ ownership)</i>
	<i>e. Other types of legal arrangements – the identity of persons in equivalent or similar positions.</i>
	Identification data of beneficiary of life insurance policies:
	<i>Name of the person, for beneficiary(ies) of life insurance, that are identified as specifically named natural or legal persons or legal arrangements</i>
	<i>Sufficient information concerning the beneficiary - for beneficiary(ies) of life insurance that are designated by characteristics or by class (e.g. spouse or children at the time that the insured event occurs) or by other means (e.g. under a will)</i>
	Other information on trustees:
	<i>Basic information on other regulated agents of, and service providers to, the trust, including investment advisors or managers, accountants, and tax advisors.</i>
	<i>The assets of the trust to be held or managed under the terms of the business relationship.</i>
	<i>The residence of the trustee.</i>

	The purpose and intended nature of the business relationship.
	Identification of person purporting to act on behalf of the customer and his authorities.
	The source of wealth and source of funds of PEP and the family members.
	Wire transfer originator information:
	<i>a. the name of the originator;</i>
	<i>b. the originator account number, or unique transaction reference number;</i>
	<i>c. originator's address, or national identity number, or customer identification number, or date and place of birth.</i>
	Wire transfer beneficiary information:
	<i>a. the name of the beneficiary;</i>
	<i>b. the beneficiary account number or a unique transaction reference number.</i>
	Bank account information
	Business correspondence
	Findings of analysis on customer/transaction ⁶

Power to access information from other sources

50) Examples of types of information that FIUs may obtain from other sources directly, through requests or direct access to the relevant databases, or indirectly, through another authority or entity holding the information. In any case, it is important that the access be prompt, confidential and secure. Depending on the FIU's analytical needs, these include but are not limited⁷ to the following types of information, where applicable:

⁶ E.g. inquiries to establish the background and purpose of complex, unusual large transactions.

⁷ Any other financial, administrative or law enforcement information required to conduct a case analysis.

Source of information	Types of information
Administrative authorities	Basic information on legal persons registered in the country:
	<i>a. company name, proof of incorporation, legal form and status, the address of the registered office, basic regulating powers (e.g. memorandum & articles of association), a list of directors.</i>
	<i>b. a register of company's shareholders or members, containing the names of the shareholders and members and number of shares held by each shareholder and categories of shares (including the nature of the associated voting rights)⁸.</i>
	Physical cross-border transportation of cash:
	<i>a. The amount of currency or BNIs declared, disclosed or otherwise detected;</i>
	<i>b. Identification data of the bearer.</i>
	<i>c. Origin of currency or BNIs and their intended use</i>
LEA	Information on money laundering and terrorist financing investigations, prosecutions and convictions.
	Law enforcement records (before court trial)
	Information on property frozen, seized and confiscated
	Information on mutual legal assistance
NPOs	<i>The purpose and objectives of NPOs' stated activities</i>
	<i>The identity of the person(s) who own, control or direct NPO's activities, including senior officers, board members and trustees</i>
	<i>Annual financial statements</i>
	Records of domestic and international transactions

⁸ May also include information on share warrants and other negotiable securities (IO 5).

51) Where applicable, examples of information that may be useful to FIUs include:

Source of information	Types of information
Administrative authorities	Natural persons register
	Marital status
	Social security information on physical persons (excluding medical data)
	Land and property ownership records, real estate register
Administrative authorities /LEAs	Citizenship records
	Fiscal information (declared income and taxes paid)
	Administrative liability measures
LEA	Customs records
	Export/import of goods
	Visa records
	Border crossing by physical persons
	Vehicle register
Supervisory bodies	Organisation's license and compliance information
Commercial databases	LexisNexis, World-Check, etc.

Table of Amendments

Date / reason for update	Amendment						
<p>June 2015.</p> <p>As a result of the OpWG FIU Powers to Access, Obtain and Exchange Information</p>	<p>37) Examples of such disclosures that FIUs receive and use in their analytical work include:</p> <ul style="list-style-type: none"> • Reports of physical cross-border transportation of cash, bearer instruments or means of payment. • Reports of transactions and payments in cash or bearer instruments, domestic or international. • Reports on foreign currency transactions, domestic or international. • Reports on wire transfers, domestic or international. • Reports on complex, unusual large transactions. • Reports on accounts held abroad by nationals or residents. • Reports on the application of targeted financial sanctions. 						
<p>June 2015.</p> <p>As a result of the OpWG FIU Powers to Access, Obtain and Exchange Information</p>	<p>48) Examples of the types of information that FIUs could be able to obtain from reporting entities, depending on their analytical needs, include but are not limited⁹ to the following:</p> <table border="1" data-bbox="657 1045 1906 1252"> <thead> <tr> <th data-bbox="657 1045 991 1089">Source of information</th> <th data-bbox="991 1045 1906 1089">Types of information</th> </tr> </thead> <tbody> <tr> <td data-bbox="657 1089 991 1170">Reporting entities</td> <td data-bbox="991 1089 1906 1170">Identification data of natural person:</td> </tr> <tr> <td data-bbox="657 1170 991 1252"></td> <td data-bbox="991 1170 1906 1252"><i>a. Name and other identification data of the natural persons¹⁰</i></td> </tr> </tbody> </table>	Source of information	Types of information	Reporting entities	Identification data of natural person:		<i>a. Name and other identification data of the natural persons¹⁰</i>
Source of information	Types of information						
Reporting entities	Identification data of natural person:						
	<i>a. Name and other identification data of the natural persons¹⁰</i>						

⁹ Any other information gathered in the Customer Due Diligence (CDD) process, consistent with the risk circumstances and the type of CDD measures applied

¹⁰ E.g. data on the customer or the authorized person contained in the passport, identity card, driving license or other similar documents; date and place of birth; address information, etc.

		<p>Identification data of legal person or legal arrangements:</p>
		<p><i>a. Name, legal form and proof of existence (e.g. certificate of incorporation, a certificate of good standing, a partnership agreement, a deed of trust)</i></p>
		<p><i>b. The powers that regulate and bind the legal person or arrangement (e.g. the memorandum and articles of association of a company); the names of the relevant persons having a senior management position in the legal person or arrangement (e.g. senior managing directors in a company, trustee(s) of a trust).</i></p>
		<p><i>c. The address of the registered office, and, if different, a principal place of business.</i></p>
		<p>Identification data of beneficial owner of the legal person or legal arrangements:</p>
		<p><i>a. Identity of the natural persons who ultimately have a controlling ownership interest.</i></p>
		<p><i>b. Identity of the natural persons exercising control of the legal person or arrangement through other means.</i></p>
		<p><i>c. Identity of the relevant natural person who holds the position of senior managing official.</i></p>
		<p><i>d. For Trusts – the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust (including through a chain of control/ ownership)</i></p>
		<p><i>e. Other types of legal arrangements – the identity of persons in equivalent</i></p>

		<p><i>or similar positions.</i></p>
		<p>Identification data of beneficiary of life insurance policies:</p>
		<p><i>Name of the person, for beneficiary(ies) of life insurance, that are identified as specifically named natural or legal persons or legal arrangements</i></p>
		<p><i>Sufficient information concerning the beneficiary - for beneficiary(ies) of life insurance that are designated by characteristics or by class (e.g. spouse or children at the time that the insured event occurs) or by other means (e.g. under a will)</i></p>
		<p>Other information on trustees:</p>
		<p><i>Basic information on other regulated agents of, and service providers to, the trust, including investment advisors or managers, accountants, and tax advisors.</i></p>
		<p><i>The assets of the trust to be held or managed under the terms of the business relationship.</i></p>
		<p><i>The residence of the trustee.</i></p>
		<p>The purpose and intended nature of the business relationship.</p>
		<p>Identification of person purporting to act on behalf of the customer and his authorities.</p>
		<p>The source of wealth and source of funds of PEP and the family members.</p>
		<p>Wire transfer originator information:</p>

		<p><i>a. the name of the originator;</i></p> <p><i>b. the originator account number, or unique transaction reference number;</i></p> <p><i>c. originator's address, or national identity number, or customer identification number, or date and place of birth.</i></p> <p>Wire transfer beneficiary information:</p> <p><i>a. the name of the beneficiary;</i></p> <p><i>b. the beneficiary account number or a unique transaction reference number.</i></p> <p>Bank account information</p> <p>Business correspondence</p> <p>Findings of analysis on customer/transaction¹¹</p>				
<p>June 2015.</p> <p>As a result of the OpWG FIU Powers to Access, Obtain and Exchange Information</p>	<p>Power to access information from other sources</p> <p>49) Examples of types of information that FIUs may obtain from other sources directly, through requests or direct access to the relevant databases, or indirectly, through another authority or entity holding the information. In any case, it is important that the access be prompt, confidential and secure. Depending on the FIU's analytical needs, these include but are not limited¹² to the following types of information, where applicable:</p> <table border="1" data-bbox="659 1211 1911 1334"> <thead> <tr> <th data-bbox="659 1211 989 1252">Source of information</th> <th data-bbox="995 1211 1911 1252">Types of information</th> </tr> </thead> <tbody> <tr> <td data-bbox="659 1256 989 1334">Administrative</td> <td data-bbox="995 1256 1911 1334">Basic information on legal persons registered in the country:</td> </tr> </tbody> </table>		Source of information	Types of information	Administrative	Basic information on legal persons registered in the country:
Source of information	Types of information					
Administrative	Basic information on legal persons registered in the country:					

¹¹ E.g. inquiries to establish the background and purpose of complex, unusual large transactions.

¹² Any other financial, administrative or law enforcement information required to conduct a case analysis

	authorities	<i>a. company name, proof of incorporation, legal form and status, the address of the registered office, basic regulating powers (e.g. memorandum & articles of association), a list of directors.</i>
		<i>b. a register of company's shareholders or members, containing the names of the shareholders and members and number of shares held by each shareholder and categories of shares (including the nature of the associated voting rights)¹³.</i>
		Physical cross-border transportation of cash:
		<i>a. The amount of currency or BNIs declared, disclosed or otherwise detected;</i>
		<i>b. Identification data of the bearer.</i>
		<i>c. Origin of currency or BNIs and their intended use</i>
	LEA	Information on money laundering and terrorist financing investigations, prosecutions and convictions.
		Law enforcement records (before court trial)
		Information on property frozen, seized and confiscated
		Information on mutual legal assistance
	NPOs	<i>The purpose and objectives of NPOs' stated activities</i>
		<i>The identity of the person(s) who own, control or direct NPO's activities,</i>

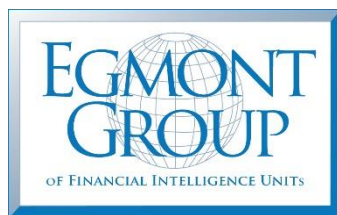
¹³ May also include information on share warrants and other negotiable securities (IO 5).

		<i>including senior officers, board members and trustees</i>																	
		<i>Annual financial statements</i>																	
		Records of domestic and international transactions																	
<p>June 2015.</p> <p>As a result of the OpWG FIU Powers to Access, Obtain and Exchange Information</p>	<p>50) Where applicable, examples of information that may be useful to FIUs include:</p> <table border="1"> <thead> <tr> <th data-bbox="659 444 989 464">Source of information</th> <th data-bbox="995 444 1908 464">Types of information</th> </tr> </thead> <tbody> <tr> <td data-bbox="659 469 989 797" rowspan="4">Administrative authorities</td> <td data-bbox="995 469 1908 545">Natural persons register</td> </tr> <tr> <td data-bbox="995 550 1908 626">Marital status</td> </tr> <tr> <td data-bbox="995 631 1908 708">Social security information on physical persons (excluding medical data)</td> </tr> <tr> <td data-bbox="995 712 1908 797">Land and property ownership records, real estate register</td> </tr> <tr> <td data-bbox="659 802 989 1052" rowspan="3">Administrative authorities /LEAs</td> <td data-bbox="995 802 1908 878">Citizenship records</td> </tr> <tr> <td data-bbox="995 883 1908 959">Fiscal information (declared income and taxes paid)</td> </tr> <tr> <td data-bbox="995 964 1908 1052">Administrative liability measures</td> </tr> <tr> <td data-bbox="659 1057 989 1433" rowspan="5">LEA</td> <td data-bbox="995 1057 1908 1133">Customs records</td> </tr> <tr> <td data-bbox="995 1138 1908 1214">Export/import of goods</td> </tr> <tr> <td data-bbox="995 1219 1908 1295">Visa records</td> </tr> <tr> <td data-bbox="995 1300 1908 1377">Border crossing by physical persons`</td> </tr> <tr> <td data-bbox="995 1382 1908 1433">Vehicle register</td> </tr> </tbody> </table>		Source of information	Types of information	Administrative authorities	Natural persons register	Marital status	Social security information on physical persons (excluding medical data)	Land and property ownership records, real estate register	Administrative authorities /LEAs	Citizenship records	Fiscal information (declared income and taxes paid)	Administrative liability measures	LEA	Customs records	Export/import of goods	Visa records	Border crossing by physical persons`	Vehicle register
Source of information	Types of information																		
Administrative authorities	Natural persons register																		
	Marital status																		
	Social security information on physical persons (excluding medical data)																		
	Land and property ownership records, real estate register																		
Administrative authorities /LEAs	Citizenship records																		
	Fiscal information (declared income and taxes paid)																		
	Administrative liability measures																		
LEA	Customs records																		
	Export/import of goods																		
	Visa records																		
	Border crossing by physical persons`																		
	Vehicle register																		

	Supervisory bodies	Organisation's license and compliance information
	Commercial databases	LexisNexis, World-Check, etc.
<p>February 2017</p> <p>As a result of the ISIL Project</p> <p>Phase I</p>	<p>Enhancing Information Exchange on Terrorism Financing Issues</p> <p>36) FIUs should adopt and implement, to the greatest extent possible, initiatives to enhance information exchange related to terrorism financing issues in order to address key barriers identified by Egmont Group members, such as:</p> <ul style="list-style-type: none"> • Promoting the role of FIUs in the national counter-terrorism apparatus; • Improving the quality of STRs; • Overcoming barriers to sharing for intelligence purposes. <p>Examples of initiatives are attached as Annex C.</p>	

The following forms are sample templates that are meant to be illustrative.

Annex A: Sample query form



The Egmont Group of Financial Intelligence Units
Request for FIU information

I. REQUESTOR REPRESENTATIONS

By using this form, the agency making the request agrees that upon receipt of information provided by the disclosing FIU that it will:

- maintain the confidentiality of any and all information provided to it by the disclosing FIU;
- not disclose the information outside of its agency without the prior written permission of the disclosing FIU; and
- limit the use of the information for the purpose(s) stated on this form.

II. REQUESTOR INFORMATION (all fields are mandatory)

Agency making the request:	
Country/territory:	
Case No:	
Date query submitted:	
Routine or urgent query:	
<i>If urgent, please indicate desired response date and reason for urgency:</i>	
Contact name & title:	
Telephone & fax:	
Email:	
Signature:	

Authorizing official :	
Position:	
Telephone & fax:	
Date:	
Signature:	

Agency receiving the request:	
-------------------------------	--

III. SUBJECT INFORMATION REQUESTED (attach additional sheets as necessary)

Subject Identification and Financial Information				
Name (surname, given, middle):		,		
		Alias(es):		
		Sex (m/f):		
		DOB (yyyy/mm/dd):		
	Address (1):		Number & Street	
		Apt. or Suite No.		
		City	Province/State	Country/Territory
	Address (2):		Number & Street	
		Apt. or Suite No.		
		City	Province/State	Country/Territory
	Phone No(s):	(1)	(2)	
	Passport No.:		Issuing Jurisdiction:	
	Other ID No:		Issuing Jurisdiction:	
	Professional Activity:			
Relationship to Investigation:				
	Place of Birth:	City	Province/State	Country/Territory
	Nationality:			
Bank Account No(s):				
Bank Name:				
	Address:		Number & Street	
		Apt. or Suite No.		
		City	Province/State	Country/Territory

Business Identification and Financial Information				
Related/associated Business (1):				
	Address:		Number & Street	
		Apt. or Suite No.		
		City	Province/State	Country/Territory
Relationship to Investigation:				
Bank Account No(s):				
Bank Name:				

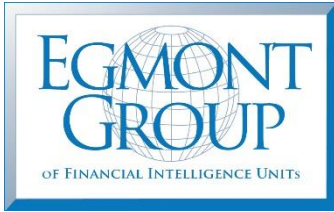
	Address:			
		Apt. or Suite No.	Number & Street	
		City	Province/State	Country/Territory
Related/associated Business (2):				
	Address:			
		Apt. or Suite No.	Number & Street	
		City	Province/State	Country/Territory
Relationship to Investigation:				
Bank Account No(s):				
Bank Name:				
	Address:			
		Apt. or Suite No.	Number & Street	
		City	Province/State	Country/Territory

IV. NATURE OF THE INVESTIGATION (attach additional sheets as necessary)

1. Describe the case under investigation and state the principal violation(s):
 Criminal Civil
2. Describe the link with the country of the disclosing FIU.
3. What information do you need from the disclosing FIU?
4. How and for what purpose(s) will the information requested be used?
5. Are there ongoing formal investigations or judicial proceedings?
6. Do you anticipate asset forfeiture or sequestration in this case?
7. State the amount and type, or nature, of assets involved in this case.
8. What other agencies or countries are involved in this investigation?

If applicable, number of additional sheets attached:

Annex B: Sample Spontaneous Disclosure cover letter



The Egmont Group of Financial Intelligence Units
Spontaneous Disclosure cover letter

Please attach this cover letter to the front of the spontaneous disclosure

I. RECEIVING FIU REPRESENTATIONS

The receiving agency shall agree that upon receipt of information provided by the disclosing FIU, the receiving agency will:

- maintain the confidentiality of any and all information provided to it by the disclosing FIU;
- not disclose the information outside of its agency without the prior written permission of the disclosing FIU; and
- limit the use of the information for the purpose(s) stated in this report.

II. DISCLOSING FIU INFORMATION (all fields are mandatory)

Submitting agency :	
Country/territory:	
Case No:	
Disclosure date:	
Contact name & title:	
Telephone & fax:	
E-mail:	
Signature:	

Authorizing official:	
Title:	
Telephone & fax:	
Date:	
Signature:	

Receiving agency:	
-------------------	--

**This report is provided for intelligence purposes only and does not require action on the part of the receiving agency*

Annex C: Promoting the role of FIUs in national counter - terrorism apparatus

The FIUs involved in the ISIL Project found that information exchange with intelligence services was crucial to be effective in performing the functions of an FIU in combating terrorism.

This approach is consistent with the Financial Action Task Force (FATF) Recommendation 29 Interpretative Note when addressing 'access to information'.¹⁴

A legislative mandate for FIUs also provides the basis to counter the financing of terrorism, including the collection of reporting, analysis and dissemination of intelligence.

In the context of countering the financing of terrorism (CFT), FIU relationships with, and access to information from, intelligence services is complemented by the same engagement with law enforcement and other relevant partners.

For FIUs to be an effective part of the national counter-terrorism (CT) effort the domestic relationships are enhanced by the FIU being part of a national CT apparatus, including:


A **national plan or strategy** to combat terrorism and/or terrorism financing that includes the FIU. Additionally, FIUs should help drive their national counter-terrorism financing strategy by having a central role in the national risk assessment; and

A **multi-agency body** which sets operational priorities for CT efforts, where the FIU seconds an officer and/or is a permanent member of a committee structure.

¹⁴ <http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html>

PROMOTING THE ROLE OF FIUs

A legislative framework that incorporates a CTF mandate for the FIU is the basis of being able to effectively play a role in the regime.




NATIONAL STRATEGIES

Poland's National Counter-Terrorist Program (2015-2019) defines strategic, operational and tactical coordination and agency responsibilities in CT, including priority setting and the sharing of information. FIU Poland (GIFI) is an agency with tactical responsibility for anti-terrorist protection of the country. This role is supported by the Inter-Ministerial Committee of Financial Security as a consultative and advisory body to apply special limiting measures against persons, groups and entities to counter terrorist financing.

Japan has *Guideline for Promotion of the Criminal Proceeds Control (2007)* released by the National Police Agency (which houses FIU Japan – JAFIC) which prescribes the principles to combat terrorism financing including the role of the FIU to collect, analysis and disseminate information.

Malaysia's AML/CFT/APF National Strategic Plan 2015-2020 has embedded plans for periodic sharing of intelligence to assist with targeting TF and developing TF intelligence.



MULTI-AGENCY BODIES

The Australian Counter-Terrorism Centre (ACTC) is a multi-agency body that facilitates the coordination of operational activity to combat terrorism. AUSTRAC (FIU Australia) is a member of the body and participates in its subcommittees.

The Macao SAR Government Anti-money Laundering Working Group consists of 15 government agencies, including the Financial Intelligence Office (GIF). The WG plays an important role of policy making & implementation and coordinating the AML/CFT issues.

In Paraguay, the Secretariat for Prevention and Investigation of Terrorism (SEPRINTE) operates under the National Police to plan, coordinate and execute all terrorism investigations.

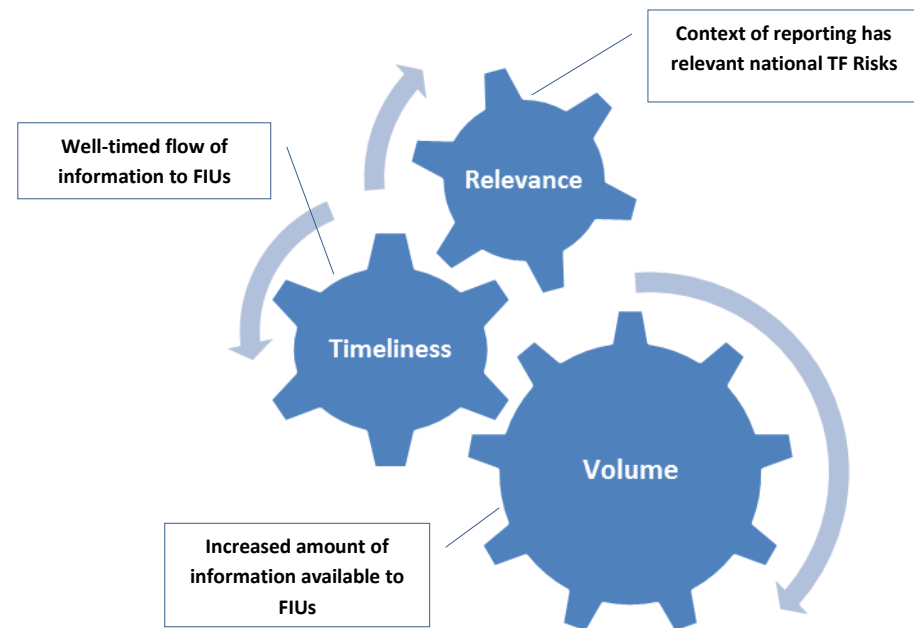
FINTRAC actively participates in the Counter-Terrorism and National Security Committee of the Canadian Association of Chiefs of Police, which works to strengthen communication, cooperation and coordination on CT operations. This committee consists of nation-wide representation by law enforcement agencies and partner government agencies that assess and address counter-terrorism and national security-related issues.

IMPROVING SUSPICIOUS TRANSACTION REPORT (STR) QUALITY

For an FIU to be effective in combatting terrorism financing, it requires relevant information to produce value-added intelligence for operational partners to act upon – consistent with FATF Recommendation 29 Interpretative Note and the FATF methodology for assessing effectiveness under Immediate Outcome 6¹⁵.

A key source of information for FIUs is the reporting entities that provide suspicious transaction reporting relating to terrorism financing. One way to assess the quality of STRs is to consider volume, timeliness and relevance.

FIUs can take a number of actions to ensure they have the right information to trigger actionable intelligence to counter terrorism financing. Diagram 2 outlines relevant aspects to consider.



¹⁵ <http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatfissuesnewmechanismstostrengthenmoneylaunderingandterroristfinancingcompliance.html>

Diagram 2



Share information about risk and methods with the private sector, focusing on those sectors most at risk.

This can include indicators of financing and characteristics of terrorists.

Engagement can include:

- regular meetings with key stakeholders
- managing the relationship through dedicated contacts
- Issuing alerts and advisories

Provide training and conduct outreach to reporting entities, especially sectors or businesses vulnerable to being misused to finance terrorism.

Engagement can include:

- Conferences
- Public/private sector forums
- Presentations

Use media to promote broader awareness of terrorism financing and where appropriate, acknowledge the work of the private sector in reporting relevant suspicious activity.

Engagement can include:

- Public statements
- Speeches
- Working with news companies and reporters

Ensure **STR formats** are consistent to make it easy for reporting entities to identify possible terrorism financing

Promote electronic reporting to further ensure consistency as well as timely receipt and analysis by the FIU.

Ensure **STRs capture all relevant information**, which may require **legislative amendments**, including geolocation data and unique identifiers that can be integrated with law enforcement and intelligence services sources of intelligence, for example:

- IP addresses if accounts are accessed online, especially offshore
- telephone numbers and email addresses

OVERCOMING BARRIERS TO SHARING FOR INTELLIGENCE PURPOSES

The FIUs involved in the ISIL Project found that several participating FIUs were unable to share information - either bilaterally or multilaterally – when there were:

- ongoing investigations,
or
- mutual legal assistance request in-progress.

Such national laws placed undue restrictions on FIU's ability to share information for intelligence purposes. These limitations restrict information exchange when it could be most useful: when there is an ongoing law enforcement or prosecutorial focus on a particular subject.

The FATF Standards are clear on international cooperation and unduly restrictive measures, for example as indicated in the Interpretive Note to Recommendation 40, paragraph 2. FIUs should continue to work with national partners to ensure domestic and multilateral measures do not impede information sharing for intelligence purposes.

Interpretive Note to FATF Recommendation 40, Paragraph 2

Countries should not prohibit or place unreasonable or unduly restrictive conditions on the provision of exchange of information or assistance. In particular competent authorities should not refuse a request for assistance on the grounds that:

- (a) the request is also considered to involve fiscal matters; and/or*
- (b) laws require financial institutions or DNFBPs (except where the relevant information that is sought is held in circumstances where legal privilege or legal professional secrecy applies) to maintain secrecy or confidentiality; and/or*
- (c) there is an inquiry, investigation or proceeding underway in the requested country, unless the assistance would impede that inquiry, investigation or proceeding; and/or*
- (d) the nature or status (civil, administrative, law enforcement, etc.) of the requesting counterpart authority is different from that of its foreign counterpart.¹⁶*

¹⁶ http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf