



DIRECTORATE FOR FINANCIAL, FISCAL AND ENTERPRISE AFFAIRS
COMMITTEE ON FISCAL AFFAIRS

**ANALYSIS OF THE REPLIES TO THE QUESTIONNAIRE ON ACCESS TO
INFORMATION GATHERED BY ANTI-MONEY-LAUNDERING AUTHORITIES**

(Note by the Secretariat)

This note is submitted FOR INFORMATION under Item IX of the Draft Agenda of the Committee on Fiscal Affairs at its 58th Session, to be held on 26-27 January 2000.

This note will be submitted to the Financial Action Task Force for the joint informal meeting with the CFA to be held on 3 February 2000. Greece, Hungary, Iceland, Mexico and Turkey have not yet submitted responses to the questionnaire [DAFFE/CFA/WP8(99)5/REV1] and are asked to do so by 31 January 2000. The FATF will be invited to submit comments on the responses contained in this note.

Contact person: Ms. Grace Perez-Navarro, Tel: (33 1) 45 24 18 80
and/or Mr. Robert Van der Have, Tel: (33 1) 45 24 80 87
Fax: (33 1) 44 30 61 36

85797

Action Required

This note is submitted to the CFA for information. It will be used for the joint meeting of the CFA and the FATF at 3 February 2000. The following countries have not yet submitted their responses to the questionnaire: Greece, Hungary, Iceland, Mexico and Turkey. They are asked to do so by 31 January 2000.

ANALYSIS OF THE RESPONSES TO THE REVISED QUESTIONNAIRE ON ACCESS TO INFORMATION GATHERED BY ANTI-MONEY LAUNDERING AUTHORITIES

Executive Summary

1. In May 1998, the G7 Finance Ministers encouraged international action to enhance the capacity of anti-money laundering systems to deal effectively with tax related crimes. The G7 considered that international action in this area would strengthen existing anti-money laundering systems and increase the effectiveness of tax information exchange arrangements. On 18 January 1999, representatives of the FATF and the OECD Committee on Fiscal Affairs (CFA) held an informal contact meeting to discuss how to follow up the G7 proposals to enhance the capacity of anti-money laundering systems to deal effectively with tax related crimes. At that meeting it was agreed that the FATF would take the lead on the first objective of the G7 initiative, that is, looking for ways to close the potential "fiscal excuse" loophole in suspicious transaction reporting systems. Furthermore it was agreed that the CFA would take the lead on the second objective of the G7 initiative, that is, the provision of money laundering information to tax authorities to support the investigation of tax related crimes.

2. The CFA agreed to mandate its Working Party No.8 on Tax Avoidance and Evasion to undertake a country survey on tax authorities' access to information obtained from anti-money laundering activity. After the March 1999 meeting of Working Party No.8, the Revised Questionnaire on Access To Information Gathered by Anti-money Laundering Authorities [DAFFE/CFA/WP8(99)5/REV1] was finalised and submitted to Member countries with the request to provide responses before 1 July 1999. The questionnaire contains questions related to the responsibility for anti-money laundering programmes; the types of information gathered by, or available to, anti-money laundering authorities; and confidentiality requirements.

3. As of 15 December 1999, 24 Member countries and the Slovak Republic have responded. Responses have been received from Austria, Australia, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Ireland, Italy, Japan, Korea, Luxembourg, the Netherlands, New Zealand, Norway, Poland, Portugal, Spain, Sweden, Switzerland, the United Kingdom and the United States. In Canada BILL C-81 has introduced new anti-money laundering legislation. The responses of Canada have been based on this bill, as this will reflect the new Canadian position, if the bill becomes law. Korea reported it has not yet a comprehensive money laundering systems. However, there are some anti money laundering measures. A bill for a comprehensive system has been submitted to Parliament. A review of the responses is given in this analysis. The country responses are reproduced in separate documents [Room document 2, WP nr.8 meeting on 27-28 October 1999, DAFPE/CFA/WP8/RD(99)2, DAFPE/CFA/WP8/RD(99)12 (Norway), DAFPE/CFA/WP8/RD(99)13 (Japan), DAFPE/CFA/WP8/RD(99)14 (Austria) and DAFPE/CFA/WP8/RD(99)20 (Ireland Italy and Korea)].

4. The responses to the questionnaire show that a variety of different systems have been adopted to implement the FATF-recommendations on anti-money laundering. Restrictions on the exchange of information between money laundering authorities and tax authorities differ widely. There are countries where tax authorities have full access to all suspicious transaction reports, while in other countries indirect access is possible. In some other countries the anti-money laundering legislation explicitly stipulates that information on suspicious transactions may only be used to combat money laundering.

TABLE OF CONTENTS

ANALYSIS OF THE RESPONSES TO THE REVISED QUESTIONNAIRE
ON ACCESS TO INFORMATION GATHERED BY
ANTI-MONEY LAUNDERING AUTHORITIES 3

Executive Summary 3

Analysis of the responses to the Revised Questionnaire on access to
information gathered by anti-money laundering Authorities (DAFFE/CFA/WP8(99)5/REV 1 5

II. Access to Suspicious Transaction Reports 9

III. Access to Other Reports 26

IV. Other Criminal Intelligence 34

V. Access to Information Gathered in the Context of a Specific Investigation 37

VI. Exchange of Information with Tax Treaty Partners 46

VII. Usefulness of Information 49

Analysis of the responses to the Revised Questionnaire on access to information gathered by anti-money laundering Authorities (DAFFE/CFA/WP8(99)5/REV 1

As of 15 December 1999, responses have been received from twenty four Member countries: Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Ireland, Italy, Japan, Luxembourg, the Netherlands, New Zealand, Norway, Poland, Portugal, Spain, Sweden, Switzerland, the United Kingdom, and the United States. Canada's responses are based on BILL C-81, which introduces new anti-money laundering legislation. The United Kingdom provided information on the position of Inland Revenue and HM Customs and Excise. The Slovak Republic also has responded to the questionnaire. Korea reported that it does not yet have a comprehensive money laundering system. However, it has enacted some anti money laundering measures. A bill for a comprehensive system has been submitted to Parliament. Korea did not think it useful to respond to the questionnaire on the basis of the proposed legislation, but gave an overview of the current anti-money laundering measures. Its current money laundering system relies on reporting systems and the granting of access to financial information for other enforcement or regulatory functions:

- 1.the Real Name, Financial Transactions and Guarantee of Secrecy Act;
- 2.the Foreign Currency Transaction Act, which requires reporting of certain transactions over \$US 20.000 to the Tax and Customs Services;
3. the Special Act on the Prevention of Illicit Traffic in Narcotic Drugs, which requires reporting to the Prosecutor General of possible illicit earnings or money laundering activities related to or resulting from illegal drug trafficking, and
4. The Anti-Public Corruption Forfeiture Act, which indirectly deters money laundering by authorising confiscation of illegal proceeds from public corruption.

See DAFPE/CFA/WP8/RD(99) 20 for the full response by Korea.

I. Money Laundering and Tax Crimes

- A.** *Is there a national government agency or body that is primarily responsible for co-ordinating anti-money laundering activities in your country? If so, please identify the agency.*

Sixteen Member countries have an institution that is responsible for co-ordinating anti-money laundering activities. In seven other countries there are no centralised institutions.

Country	Responsible Authority
Austria	EDOK-Meldestelle, which is part of the Federal Ministry of Internal Affairs
Belgium	The CTFI/CFI (Cellule de Traitement des informations Financières/ Cel voor Financiële informatieverwerking)
Czech Republic	The Financial Analytical Unit, which is the competent organisational component of the Ministry of Finance
Denmark	The Money Laundering Secretariat (under the Public Prosecutor for Serious Economic Crime)
Finland	The National Bureau of Investigation/Money Laundering Clearing House (Rahansposun selvittelykesku/Keskurikopoliisi)
France	TRACFIN, service spécialisé du Ministère de

	l'Economie des Finances et de l'Industrie
Ireland	An Garda Siochána, Garda Bureau of Fraud Investigation (GBFI)
Italy	Ufficio Italiano dei Cambi (UIC) as part of the Central Bank together with the Bank of Italy
Japan	FIU (Financial Intelligence Unit) at the Financial Supervisory Agency
Luxembourg	le Service Anti-Blanchiment auprès du Parquet du tribunal d'arrondissement de Luxembourg
New Zealand	The New Zealand Police, Financial Investigation Unit
Norway	The national Authority for Investigation and Prosecution of Economic and Environmental Crime in Norway (ØKOKRIM).
Portugal	The Judiciary Police
Spain	Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias (CPBCIM)
Sweden	Finanspolisen
Switzerland	l'Administration fédérale des finances, Division Monnaie, Economie, Marché financiers
United Kingdom	The Economic Crime Unit of the National Criminal Intelligence Service (NCIS)

In **Australia**, the Australian Transaction Reports Analysis Centre (AUSTRAC) collects financial intelligence and disseminates information to a range of government agencies in order to assist them in the investigation of suspected money-laundering activities. These agencies include the National Crime Authority (NCA), the Australian Taxation Office (ATO), the Australian Federal Police (AFP) and the Australian Customs Service (ACS). The National Crime Authority (NCA) has primary responsibility for co-ordinating money laundering investigations.

In **Canada**, the Royal Canadian Mounted Police (RCMP) is the lead law enforcement agency responsible for the investigation of money laundering offences. However, all police services in Canada share this mandate. Money laundering policy issues are dealt with by an inter-departmental working group led by the Department of Finance, and consisting of representatives from the Department of Solicitor General, the Department of Justice, Foreign Affairs and International Trade, Revenue Canada (Taxation and Customs) and the RMCP. The Department of Finance will be responsible for FTRACC and also has the lead on the development of Bill C-81.

In **Germany**, the prosecution of money laundering activities is almost exclusively in the hands of the police, judicial authorities of the constituent states (the "Länder") and customs investigation offices. However, the Federal Investigation Office (Bundeskriminalamt) serves primarily as a central agency, in particular as far as co-operation with foreign authorities is concerned.

In **Italy** set up its FIU in 1997, when the Ufficio Italiano dei Cambi (UIC) was designated as the only recipient of suspicious transactions reports and was charged with performing supervisory and financial intelligence tasks aimed at detecting and preventing money laundering in the financial system. A 1998 Legislative Decree, while specifying that the UIC is part of the Italian Central Bank together with the Bank of Italy. Consequently, it acts in an independent way in Italy as the co-ordination point of anti-money laundering efforts in the financial area. A "high supervision" function, consisting of providing for the necessary political coherence in all anti money laundering activities, is assigned to the Ministry of the

Treasury. Police forces keep all their competencies as far as anti-money laundering investigative activities are concerned.

In the **Netherlands**, the Minister of Finance and the Minister of Justice are primarily responsible for the co-ordination of anti-money laundering activities. Several governmental and non-governmental specialised bodies are involved in anti-money laundering activities. These bodies are only responsible for anti-money laundering activities within the areas they work. In order to co-ordinate their activities, the relevant partners in the fight against money laundering participate in a number of co-ordination fora.

The aims of the responsible government agency in **Spain**, the Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias (CPBCIM), are to prevent and hinder money laundering connected to the proceeds of drug trafficking, terrorism and organised crime, which could be carried out through the financial system or through certain professional or commercial activities (such as casinos, real estate undertakings or immovable property purchasing and sales). The CPBCIM (created by Law 19/1993) is supported by two organs in performing its tasks, the Commission's Secretariat and the Commission's Executive Service (SEPBLAC). The SEPBLAC, run by the Bank of Spain, is of a mixed nature, midway between an administrative unit and a police unit, and acts as Spain's Financial Intelligence Unit (FIU) in the context of the Egmont Group.

In the **Slovak Republic**, the Ministry of Interior, the Bureau of Financial Police and the Supreme Supervision Office are responsible for co-ordinating the anti-money laundering activities.

In **Sweden**, Finanspolissen is also the clearinghouse for financial information.

In the **United Kingdom**, the Economic Crime Unit of the National Criminal Intelligence Service (NCIS) is the Financial Intelligence Unit responsible for co-ordinating the law enforcement response to money laundering. Policy responsibility for money laundering rests with the Home Office (in respect of the criminal justice system) and the Treasury (in respect of the financial regulatory issues; and international initiatives, including FATF).

In the **United States**, the investigative authority rests with a number of agencies in the United States Departments of Treasury and Justice. The United States "FIU" is the Treasury's Financial Crimes Enforcement Network of "FinCEN". In addition, a number of states have made money laundering within their jurisdictions a crime and thus have investigative authority within the state. Finally, both national and state financial supervisors and other regulators include maintenance of anti-money laundering controls by financial institutions under their respective jurisdictions.

B. *Do your domestic laws or regulations on money laundering cover crimes involving fiscal fraud or other tax crimes? If so, please describe the nature of tax crimes covered.*

Money laundering regulations cover crimes involving fiscal fraud or other tax crimes in **Austria** (only evasion or fraud of import and export duties), the **Czech Republic, France, Germany, Ireland, Italy, the Netherlands, Norway, Spain** and **Sweden**. The domestic laws or regulations on money laundering do not directly cover fiscal fraud or other tax crimes in **Australia, Belgium, Canada, Denmark, Finland, Japan, Luxembourg, New Zealand, Poland, Portugal, the Slovak Republic, Switzerland**, and the **United States**. However, in these countries, domestic laws or regulations on money laundering may indirectly cover fiscal fraud and other tax crimes. This could be the case, e.g. if the fiscal fraud or the other tax crimes are committed as part of a criminal offence concerning money laundering such as fraud, false representation, conspiracy, etc.

In **Austria**, customs fraud and evasion of import and export duties are included as money laundering offences.

In the **Czech Republic**, there is a special provision in the Criminal Code relating to money laundering. Section 251a of the Criminal Code determines the terms of this crime as follows:

- A person, who enables another person to disguise the origin of or the identification of the origin of a thing acquired by criminal activities shall be punished by imprisonment for a period of up to two years or by a pecuniary penalty.
- The offender shall be punished by imprisonment for a period ranging from one to five years
 - (a) if he has committed a crime under subsection (1) as a member of an organised group;
 - (b) if he has acquired a substantial benefit from such a crime.
- The offender shall be punished by imprisonment for a period ranging from two to eight years or by confiscation of property,
 - (a) if he has committed a crime under subsection (1) in relation to the things coming from the business activity with stupefying or psychotropic substances or by some other especially serious crime, or
 - (b) if he has acquired a large-scale benefit from such a crime under subsection (1).

France includes tax crimes as money laundering offences.

In **Germany**, money laundering is regarded as a criminal offence in relation to assets deriving from certain other criminal offences. Among these are the following offences specified in the German Fiscal Code ("Abgabenordnung"):

- gainful evasion of import duties and taxes;
- gainful import, export or transit of contraband in contravention of monopoly regulations;
- evasion of import duties and taxes or handling contraband using a weapon or other implement or means to prevent or overcome the resistance of another person by force or the threat of force, or using a firearm;
- commission of such offence as member of a gang set up for the repeated evasion of import duties and taxes or the handling of contraband, in collaboration with another member of the gang.
- any persons purchasing or otherwise acquiring for own account or for account of a third person tax-evaded, duty-evaded or contraband goods, or selling or helping to sell such goods with the aim of enriching themselves or a third person, are liable to punishment for the offence of handling untaxed goods. The smuggled goods involved in the evasion of taxes is also deemed to derive from one of the above mentioned offences.

In **Ireland**, Section 31 of the Criminal Justice Act 1994 deals with the offence of money laundering. It covers the proceeds of drug traffic and "other criminal activities". The latter reference would include tax evasion, which is a criminal offence.

In **Italy**, according to the Italian Penal Code, all intentional crimes can constitute predicate offences for money laundering; consequently, all intentional tax crimes are relevant for the application of anti-money laundering regulations.

In the **Netherlands**, if the MOT (i.e. the Dutch Office for the disclosure of unusual transactions), suspects a crime on the basis of the received data (prima facie or after further investigation) it has to be reported to the (fiscal) law enforcement authorities. This obligation also applies when tax crimes are suspected.

In **Norway**, domestic laws on money laundering cover all crimes. If the institution suspects that a transaction is connected with a crime with maximum penalty of more than 6 months imprisonment, the institution must report the transaction. If it suspects that the transaction is connected with a crime with maximum penalty of only six months of imprisonment, the institution is not obliged to conduct further examination. It is considered a legal offence according to Norwegian Law if a person, with intention or serious negligence, does one of the following:

- gives the tax authorities incorrect or incomplete information, if he understands or ought to understand that this might lead to tax advantages,
- prepares an incorrect document, if he understands or ought to understand that the document might enable him to achieve tax advantages,
- violates the rules given in the Act of Foreign Exchange Regulations, if he understands or ought to understand that this violation might serve as a means of enabling him to achieve tax advantages, in any other way makes an essential violation to the regulations given in the Assessment Act.

In **Spain**, Article 301 of the Penal Code states that money laundering will be considered the "legitimization" of the proceeds of any serious crime (tax crimes included). Nevertheless, within the framework of preventing the financial system from being used for money laundering, the Law 19/93 (which adapts the provisions of Directive 91/308 EEC) only obliges the persons/entities referred to in the said law exclusively in connection with the underlying crimes of drug trafficking, terrorism and organised crime.

In **Sweden**, criminalised fiscal fraud and other tax and customs duty crimes are covered.

The **United Kingdom's** money laundering laws cover tax crimes. Tax-related offences are not in a special category: the proceeds of an indictable tax-related offence may, like the proceeds of a financial fraud, robbery or burglary, be the subject of money laundering offences, under the Criminal Justice Act 1988. All relevant tax-related offences are indictable, including frauds against the Inland Revenue. "Proceeds of crime" for the purposes of the 1988 Criminal Justice Act includes the proceeds of criminal conduct, which occurred in another jurisdiction, where the same conduct would be regarded as an indictable offence if it had taken place in the UK.

II. Access to Suspicious Transaction Reports

A. *Are suspicious transactions required or permitted to be reported in your country? If not, proceed to Part III of the questionnaire.*

In all the states that responded to the questionnaire suspicious transactions are required to be reported.

B. *What constitutes a suspicious transaction under your laws, regulations or guidelines? Do your laws, regulations, or guidelines provide a definition of suspicious transactions or guidelines that describe what may constitute a suspicious transaction? If so, please provide the definition and/or guidelines.*

In ten Member countries that responded to the questionnaire (**Australia, the Czech Republic, France, Italy, Japan, New Zealand, Norway, Spain, Switzerland,** and the **United States**) and in the **Slovak Republic** there is a definition of “suspicious transaction”. In **Austria, Belgium, Canada, Denmark, Finland, Germany, Luxembourg, Ireland,** the **Netherlands, Poland, Portugal, Sweden,** and the **United Kingdom,** a “suspicious transaction” is not defined but the meaning may be derived from anti-money laundering regulations.

Most definitions have in common the element of an out of the ordinary, unusual commercial transaction or behaviour in relation with the person effecting it. Some definitions also have a link to transactions related to drug trafficking or activities of organised crime.

Countries with a definition of suspicious transactions

In **Australia,** the latest guidelines issued by AUSTRAC define a "Suspicious Transaction" as any transaction which causes a cash dealer to have a feeling of apprehension or mistrust about a transaction considering:

- its unusual nature or circumstances;
- the known background of the person or persons conducting the transaction;
- the production of seemingly false identification in connection with the transaction;
- admissions or statements of involvement in tax evasion or criminal activities;
- regular or unusual transactions involving known narcotic source or transit countries;
- the personal appearance and behaviour of the person or persons conducting the transaction.

Section 16(1) of the Financial Transaction Reports Act 1988 (FTR Act) specifies where:

- (a) a cash dealer is party to a transaction; and
- (b) the cash dealer has reasonable grounds to suspect that information that the cash dealer has concerning the transaction:
 1. may be relevant to investigation of an evasion, or attempted evasion, of a taxation law;
 2. may be relevant to investigation of, or prosecution of a person for, an offence against a law of the Commonwealth or of a Territory; or
 3. may be of assistance in the enforcement of the "Proceeds of Crime Act 1987" or the regulations made under that Act;

the cash dealer, whether or not required to report the transaction under Division 1 or 3, shall, as soon as practicable after forming that suspicion:

- (c) prepare a report of the transaction; and
- (d) communicate the information contained in the report to the Director (AUSTRAC).

The Director of AUSTRAC has the power under law to issue guidelines to assist Cash Dealers to apply a subjective test.

In the **Czech Republic**, there is a definition in the Money Laundering Act officially known as The Act on Measures against Legalisation of the Proceeds from Criminal Activity No. 61/1996 Coll., as amended by Act No. 15/1998 Coll. in the Czech Republic. For the purpose of this Act, “an unusual transaction” is one, which by its character, content or peculiarity clearly differs from the customary scope or characteristics of transactions of a particular kind or person. “Proceeds” under this Act is understood to be any economic benefit arising from any activity having the characteristics of a criminal act. Failure to discharge a tax liability, non-payment of charges (fees) or non-fulfilment of similar liability is not regarded as an economic benefit under this Act.

In **France**, the Act of 12 July 1990 gives the following definition: The amounts and transactions, which appear to be derived from drug trafficking or the activities of organised crime.

In **Italy**, great importance is attached to the active co-operation which is requested from the entities obliged to report in detecting transactions which are likely to involve funds of illegal origin. Such entities are helped in performing their task by the definition of suspicious transactions, which is provided for by the Law. According to article 3 of Law n 197/1991, the transactions to be reported are those which, by virtue of their characteristics, entity or nature, or by virtue of any other circumstances that are recognised because of the function performed, also taking into account the economic capacity of and the activity carried out by the entity to which it refers, leads one to believe, based on the facts available to him, that the money, assets or goods involved may derive from crimes covered under Articles 648-bis and 648 ter of the Penal Code.

To provide further assistance in the detection of suspicious transactions, some guidelines have been issued by the Bank of Italy in which several indicators of anomaly have been specified of banks’ and insurance companies’ transactions. Such guidelines are applicable also for other categories of reporting entities, provided that the relevant differences are taken into account. The guidelines are subdivided into different sections dealing with indicators related to, respectively, anomalies for: cash transactions, securities transactions, cross-border transactions, other transactions and services, use of accounts and customer behaviour.

Some general indicators specified in the guidelines, applicable to all types of transactions, are in particular worth mentioning. Transactions should be deemed as anomalous if:

- They appear to be disproportionately large or economically unwarranted in relation to the person effecting them or the account with the intermediary;
- They are of the same kind repeated at a single establishment in a way that suggests the purpose is concealment (e.g. subdividing transactions in order to avoid recording requirements);
- They are carried out frequently on behalf of third parties who never appear in person, unless they clearly reflect the practical or organisational needs of the customers, especially when pretexts or unverifiable reasons are adduced (e.g. illness, other engagements)
- They are requested through order containing obviously false or incomplete information that suggest the purpose is the deliberate concealment of essential information, especially in connection with the persons involved.

In **Japan**, Article 54 of the Law for Punishment of Organised Crimes, Control of Crime Proceeds and Other Matters stipulates as follows:

Any bank or other financial institution provided for in the Cabinet Ordinance or any other person provided for in the Cabinet Ordinance (hereinafter referred to as a “financial institution or the like” in this article) shall promptly report to the Minister in charge (the Commissioner of the Financial Supervisory Agency in case where the Minister in charge is the Financial Reconstruction Commission, and a prefectural governor in case of a financial institution or the like specified in the Cabinet Ordinance) those matters provided for in the Cabinet Ordinance in accordance with the provisions of the Cabinet Ordinance, when there is a suspicion that the property received by such financial institution or the like in the course of its business provided for in the Cabinet Ordinance is crime proceeds or the like or drug crime proceeds or the like, or

when it is deemed that there is a suspicion that the other party to a transaction for such business of such financial institution or the like is committing an act constituting an offence provided for in Article 10 or in Article 6 of the Anti-Drug Special Law in connection with such business.

In **New Zealand**, Guidance Notes for Financial Institutions were issued by the NZ Police, Financial Intelligence Unit, following the enactment of the Financial Transactions Reporting Act 1996. The guidelines define a “suspicious transaction” as: A transaction that is inconsistent with a customer's known, legitimate business or personal activities or with the normal business for that type of customer. The following guidelines may be used as indicators of suspicious transactions:

1. For no apparent or logical reason the individual travels a great distance to use an institution's services when it is known that the equivalent is available much closer to their home.
2. Unusually large cash deposits made by an individual or company whose ostensible business activities would normally be generated by cheques and other instruments.
3. Substantial increases in cash deposits of any individual or business without apparent cause.
4. Customers who seek to exchange large quantities of low denomination notes for those of higher denomination.
5. Frequent exchange of cash into other currency where there appears no logical explanation for such activity.
6. Customers transferring large sums of money to or from overseas locations with instructions for payment in cash.
7. Large cash deposits locations using ATM or drop boxes thereby avoiding direct contact with the bank staff.
8. Customers who insist on using an institution's services for transactions not within that institution's normal business and for which there are other firms with publicly acknowledged expertise.
9. Customers who are reluctant to co-operate with verification of their identity or provide false or misleading information.
10. Customers who wish to buy an insurance or investment product and seem to be more interested in cancellation or surrender terms.
11. Customers who for no apparent or logical reason ask to cancel or surrender a long term investment soon after setting up the contract.
12. Customers who wish to invest significant sums using cash, or make top-up payments using cash.
13. Customers who wish to make an investment that has no obvious purpose.
14. Customers who ask for settlement to a third party where there appears to be no apparent reason for the investor to be acting on someone else's behalf and where it would appear simpler or more logical for payment to be made to the original investor.

In **Norway**, regulations as well as guidelines give guidance on what may constitute suspicious transactions. Regulations on Identification and Measures to Combat Money Laundering laid down by the Ministry of Finance provide:

Among the circumstances that may trigger the duty to carry out enquiries, are

- that the transaction appears to lack a legitimate purpose,
- that the transaction is unusually large or complex,

- that the transaction is unusual in relation to the customer's habitual commercial or personal transactions,
- that the transaction is done with a customer in a country or area without satisfactory actions against money laundering, or
- that the transaction is otherwise of an anomalous nature.

In the guidance notes (laid down by "Kredittilsynet", The Banking, Insurance and Securities Commission of Norway) some other signals of suspicious transaction are mentioned:

- Swift and extraordinary payment of loans by cash
- Use of banker's drafts that are constantly renewed
- Large exchange operations when old notes become invalid
- Large exchange operations at the introduction of EURO
- Use of unusual means of payment in relation to the underlying operation
- Large cash-transactions

Use of payment-cards when unusually many transactions take place within a short time-period

In the **Slovak Republic**, the definition of a suspicious bank operation is defined according to §1 of the Decree of the Ministry of Interior no. 181/1997 (Coll. of Laws) on the Suspicious Bank Operations:

- (a) single deposit or withdrawal of cash in amount from 500 000 SKK (USD 12 000) and above or its equivalent in foreign currency;
- (b) high frequency of cash deposits in amount from 500 000 SKK (USD 12 000) and above or its equivalent in foreign currency that has accumulated significant amount or transferred to other places not usually used by the client;
- (c) non-cash deposits of a client and the third persons and subsequent cash withdrawals for the purposes where other means of payment (cheques, letter of credit, bonds) is usually used;
- (d) frequent deposits of bank notes with little nominal value;
- (e) utilisation of a letter of credit or other means of payment traditionally used abroad but incidental (or unusual) to the regular business activity of a client,
- (f) frequent buying and re-selling of traveller's cheques in foreign currency to banks;
- (g) payments in cash for bank bonds or other negotiable documents;
- (h) frequent foreign currency exchanges with no deposits;
- (i) deposits and immediate withdrawals or transfers to other accounts;
- (j) activity of a client related to opening of bank accounts the number of which are not in accordance with the client's regular business activity and transfers among these bank accounts;
- (k) money transfers inadequate to the amount or nature of the regular business activity of a client;
- (l) when a client refuses to provide the bank with information related to the bank operation or provides such information that the bank could prove it only with difficulties or not at all;
- (m) an effort by a client to sign a contract with the bank or to make a bank operation on the basis of vague projects;

- (n) the movement on the account of a client (the number of transfers or amount of transfers within a day or two) is not consistent with the regular movements in his/her bank account;
- (o) sudden money transfer from abroad to a sleeping account (with no activity);
- (p) provision of a credit covered by a cash deposit in foreign currency deposited by the third person that is not as known to the bank as the client to whom the credit was granted;
- (q) payment of a credit before the due date, especially when the source of the funds is unclear or the client used to have difficulties with paying the credit;
- (u) repeatedly returned transfers of financial means to and from foreign banks with place of business in offshore zones;
- (v) buying and selling of securities beyond the regular activities of a client.

In **Spain**, a suspicious transaction is defined as any deed or operation that raises indications or the certainty of being related to money laundering derived from drug trafficking, terrorism and organised crime, as well as any subsequent circumstance connected with that deed or operation.

In any event, information on the following operations should be furnished to the SEPBLAC;

- (a) Those which entail physical movements of cash, traveller's cheques, cheques or other documents etc. (unless they are credited or debited in a customer's account), involving a sum amounting to Pts. 5 million or more or its countervalue in a foreign currency;
- (b) Those carried out by individual persons or legal entities resident in territories or countries considered to be tax havens, involving a sum amounting to Pts. 5 million, or its countervalue in a foreign currency.

Apart from this general classification of suspicious transactions, the financial institutions follow specific guidelines, which give numerous examples of what may constitute a suspicious transaction. Those guidelines (supervised by the SEPBLAC) are issued by the national organisations representative of the financial institutions (such as the Asociación Espangola de Banca, AEB. see Circulares 660 end 674).

In **Switzerland**, Article 9 of the Law on Money Laundering provides that a financial intermediary, who knows or suspects on well based grounds, that property rights are connected to money laundering, originate from a crime, or are in the power of a criminal organisation, should immediately inform the 'Bureau de communication en matière de blanchiment d'argent'.

In the **United States**, depository institutions are required to file reports on transactions involving at least \$5,000 where the depository institution knows, suspects, or has reason to suspect that:

1. the transaction involves funds derived from illegal activities or is intended or conducted in order to hide or disguise funds or assets derived from illegal activities (including, without limitation, the ownership, nature, source, location, or control of such funds or assets) as part of a plan to violate or evade any federal law or regulation or to avoid any transaction reporting requirement under federal law or regulation;
2. the transaction is designed to evade any requirements of the Bank Secrecy Act record keeping or reporting requirements; or
3. the transaction has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the depository institution knows of no

reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

Countries without a definition of suspicious transactions

The Banking Act in **Austria** does not provide for a definition of suspicious transactions. However, EDOK-Meldestelle has published guidelines with certain indicators for suspicious transactions (available only in German). Apart from that, EDOK is regularly organising awareness campaigns at banking institutions concerning detection and enforcement of money laundering activities. See also the answer to question C.

Belgian legislation does not explicitly define a suspicious transaction. It obliges certain persons and bodies (see C) to report to the CFTI if they know or suspect that a transaction is connected with money laundering or if they have knowledge of a fact that might be an indication of money laundering.

In **Canada**, there is no definition of a suspicious transaction. However, Bill C-81, which introduces new anti-money laundering legislation but is still under discussion with parliament, provides for transactions considered being indicative of money laundering to be set out in regulations to the Act. These regulations will be developed in consultation with those entities required to report. Furthermore, the Office of the superintendent of Financial Institutions and some self-regulating organisations have issued guidelines to help deter and detect money laundering.

In **Denmark**, there is no legal definition of suspicious transactions. However, the Money Laundering Act imposes a duty on persons/entities, covered by the Act to have anti-money laundering guidelines. These guidelines - which usually are made by the relevant professional organisation, e.g. the Bankers Association - give some examples of suspicious transactions which should be reported.

In **Germany**, the Money Laundering Act provides no definition of a suspicious transaction. In accordance with the Guidelines of the Federal Banking Supervisory Office on measures to be taken by credit or financial services institutions, a suspicious transaction involving a reporting obligation is deemed to exist where there are objective indications of a transaction by which illicit funds are to be rendered inaccessible to the law enforcement authorities or by which the source of unlawfully acquired assets is to be concealed, and criminal connections cannot be ruled out. The law enforcement authorities have also drawn up in collaboration with the banking industry and distributed to the institutions a list of "criteria suggestive of money laundering".

In **Finland**, when there is a reason to doubt the legal origin (doubt that it is legally obtained) of the property used in a transaction or other property, the person who is liable to report suspected money laundering cases has a duty to take care and this duty is the basis for using discretion (the amount of money is exceptionally high, unordinary services are used etc.).

In **Luxembourg**, in general everything that may be an indication of money laundering has to be reported. La Commission de Surveillance du Secteur Financier has informed the financial sector by letter of 25 November 1994 when there is an indication of a suspicious transaction, which ought to be reported.

In **Ireland**, Sections 57 of the Criminal Justice Act 1994 requires the reporting by persons to whom section 32 of the Act applies of information concerning offences under sections 31 and 32 of the Act. This includes reports of transactions suspected of involving the proceeds of crime.

In the **Netherlands**, instead of a legal definition of an "unusual transaction", there is a wide range of guidelines on which the provider of the financial services decides whether a transaction is 'unusual' or not. In particular, each large transaction must be checked against the guidelines (indicators) to see if it has to be reported as 'unusual'. These guidelines consist of both objective as well as subjective indicators. For

instance, one of the objective criteria is the amount of the money concerning the transaction. If according to the guidelines - a transaction is considered to be unusual, a report has to be made to the MOT. Finally - after investigation of a reported unusual transaction - the MOT decides whether a transaction will be passed on to the law enforcement authorities as a suspicious transaction.

Portuguese law does not establish a definition of a suspicious transaction. However, there are some guidelines in different legislation. As a result, a suspicious transaction may be described as those, which by their amount or by their nature are not in accordance with the common standard rules or behaviour.

In **Sweden**, any suspicious transaction that indicates money laundering is to be reported to Finanspolisen. According to the Bill on Money Laundering (prop. 1992/93:207 pp. 19-21), the amount of the transaction and the way it is carried out might indicate money laundering. Also other factors, such as the behaviour of the customer, can be indicative. The following examples serve as a guideline:

- one or several transactions seem unusual regarding the institute's experience of the involved persons
- the set up of a transaction implies that its underlying purpose is illicit or that the economical incentive cannot be grasped
- big amounts are deposited and shortly thereafter withdrawn without, as known, that the customer carries out any business that explains the transactions
- that a transaction apparently deviates from what is normal for the institute or the customer, and
- that an account that has been inactive is suddenly and without explanation being used to a great extent.
- According to the Financial Supervisory Authority's guidelines (FFFS:8, 4 §) specific attention should be paid to:
 - transactions involving persons or companies in countries without acceptable money laundering legislation or where it is otherwise difficult to obtain information about the customer, and
 - transactions connected to the conversion of national currencies into euro.

United Kingdom legislation does not define in detail what constitutes a suspicion of criminal conduct. That assessment can only be made in the context of the knowledge that a financial institution should have about their customers' business, and on the nature of the transaction in question. Industry guidelines, and anti-money laundering training programmes, can however assist those working in financial institutions to make that assessment. Suspicion is personal and subjective and falls short of proof based on firm evidence. A person would not be expected to identify the exact nature of a suspected criminal offence or that the particular funds were definitely those arising from that crime. The combined effect of the legislation is to make it an offence for any person to provide assistance to a criminal to obtain, conceal, retain or invest funds if that person knows or suspects (or – in some cases – “should have known or suspected”) that those funds are the proceeds of criminal conduct. Such assistance is punishable on conviction by a maximum of 14 years' imprisonment, or an unlimited fine, or both. It is a defence that the person concerned reported his/her knowledge or suspicion to the law enforcement agencies at the first available opportunity. The term “criminal conduct” includes any conduct wherever it takes place, which would constitute an indictable offence, if it took place in the UK, i.e. an offence serious enough to be tried in a Crown Court. This includes drugs trafficking offences, terrorism crime, theft and fraud, robbery, forgery and counterfeiting, illegal deposit taking, blackmail and extortion.

C. *Please identify the types of persons/entities required to report suspicious transactions.*

In all Member states that responded to the questionnaire, banks are required to report suspicious transactions. In some of these countries, this obligation is not limited to banks. In these countries the financial sector as a whole or specific parts of it, like investment companies, stock brokers, credit card companies, foreign currency dealers, mortgage companies and so on, are put under this obligation (**Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Ireland, Italy, Japan, Luxembourg, the Netherlands, New Zealand, Norway, Poland, the Slovak Republic** in the near future, **Spain, Sweden, Switzerland, United Kingdom, and United States**). Other countries also require insurance companies to report suspicious transactions (**Australia, Canada, Germany, France, Ireland, Luxembourg the Netherlands, New Zealand, Norway, Spain, Sweden, and the United Kingdom**). Some Member countries require the gambling sector to report suspicious transactions (**Australia, Belgium, Canada, the Czech Republic, Denmark, Finland, Italy** in the near future, **Germany, Luxembourg, New Zealand, Spain and Switzerland**) and some countries include estate agents as well in this obligation (**Belgium, Finland, France, Italy** in the near future, **New Zealand, and Spain**). In **Portugal**, all financial and non-financial entities, including the Central Bank, the Portuguese institute of insurance, which supervises the insurance companies, the General Inspection of Economic Activities and the General Inspection of Gambling are obligated to report suspicious transactions. In **Spain**, persons and entities involved in the trade of jewels, precious stones, precious metals, works of art, antiques or in investment in philately and numismatics are included as well. In the **United Kingdom**, the effect of the law described in section B, is that there is a *de facto* obligation on all persons and businesses to report suspicious transactions. However financial institutions, solicitors and accountants conducting financial business, financial intermediaries, insurance companies, bureaux de change, money transmission etc are subject to additional administrative requirements under the Money Laundering Regulations 1993, to establish and maintain specific policies and procedures to guard against their businesses and the financial system being used for the purposes of money laundering.

- D.** *Please identify the national agency or body with which suspicious transaction reports are required to be filed. If the reports are required to be filed with more than one agency or body, please describe briefly the responsibilities that each agency or body has with respect to the information (e.g., compilation of data, analysis of data, identification of transactions to investigate).*

In	reports are required to be filed with
Australia	Austrac
Austria	EDOK-Meldstelle
Belgium	CTIF
Canada	The Financial Transactions and Reports Analysis Centre of Canada
The Czech Republic	Ministry of Finance, Financial Analytical Unit
Denmark	The money Laundering Secretariat
Finland	The National Bureau of Investigation/Money Laundering Clearing House (Rahansposun selvittelykesku/Keskurikopoliisi)
France	TRACFIN, service spécialisé du Ministère de l'Economie des Finances et de l'Industrie
Germany	Responsible law enforcement authorities
Ireland	Money Laundering Unit (GBFI)
Italy	Ufficio Italiano dei Cambi (UIC)
Japan	Financial authorities supervising a financial institution in question
Luxembourg	Service Anti-Blanchiment at the Parquet du Tribunal

	d'arrondissement de Luxembourg
The Netherlands	Dutch office for the disclosure of unusual transaction (MOT)
New Zealand	New Zealand Police, Financial Investigation Unit
Norway	ØKOKRIM, The National Authority for Investigation and Prosecution of Economic and Environmental Crime in Norway
Poland	The Prosecutor
Portugal	Ministério Público
Slovak Republic	Bureau of the Financial Police, Financial Intelligence Unit
Spain	The executive service of Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias (SEPBLA)
Sweden	The Swedish Financial Unit at the National Criminal Investigation Department
Switzerland	Money-Laundering Reporting Office Switzerland (MROS)
The United States	FinCEN
The United Kingdom	In practice the Economic Crime Unit of the National Criminal Intelligence Service

In **Germany**, suspicious financial transactions must be reported to the responsible law enforcement authorities. The Money Laundering Act does not provide any further details. In practice, reports are made to the central financial investigation unit at the Bureau of Criminal Police of the respective Lander or to specific public prosecutor's offices. The central financial investigation units at the Bureau of Criminal Police of the Länder are staffed principally by criminal investigation officers of the police service and by customs investigation officers. These units compile and analyse the reports they receive and in co-ordination with the public prosecutor's office - either conduct the necessary investigations themselves or assign them to other law enforcement authorities.

In **Italy** the UIC is since 1997 the sole recipient of suspicious transaction reports. It carries out financial analysis of the reports, asking the intermediaries to provide further specific data or information and availing itself of all the databases at its disposal. It can also ask for the co-operation of the sector supervisory authorities and exchange information with foreign anti-money laundering units. After the analysis, which is performed from a purely financial standpoint, the UIC passes the reports on to the competent investigative bodies (the Nucleo Speciale di Polizia Valutaria of the Guardia di Finanza, which is the Italian Financial Police and Antimafia Investigate Directorate) which carry out all the necessary investigations. According to the structure of the entire procedure, a precise deadline exists in Italy between financial analysis activity of the suspicious transaction reports and investigative activities. In performing the former, the UIC cannot have access to the police databases; on the other hand, the police bodies start the investigation on suspicious transactions on the ground of the content of the technical report issued by the UIC.

In **Japan**, where the reporting institution has two Ministers in charge, suspicious transaction reports are required to be filed with both Ministers.

In **Poland**, information concerning suspicious transactions is transferred directly to the investigative body, which is the prosecutor; there is no intermediary agency.

The **United Kingdom** legislation requires suspicious transactions to be reported to "a constable"; a definition which applies to the Police and the Customs and Excise. In practice, however, the Economic

Crime Unit of the National Criminal Intelligence Service receives all suspicious transaction reports (STRs). These reports are then searched against databases and allocated according to whether the subject is under investigation or the intelligence is most suitable for HM Customs and Excise (HMCE) or Police. Other interested bodies (including Inland Revenue, HMCE, regulatory authorities such as Financial Services Authority, Stock Exchange, Gaming Board) may - under certain circumstances (see below) - be copied relevant intelligence, for the purpose of criminal investigations within their sphere of responsibility.

E. *These questions relate to situations where tax authorities have direct access to information provided in suspicious transaction reports.*

1. *Is the information obtained from suspicious transaction reports maintained in a centralised database? If so, do the tax authorities have access to the database? If so, under what circumstances do they have access?*
2. *If the information is not maintained on a database, do the tax authorities have access to the information? If so, under what circumstances do they have access?*
3. *Are there restrictions on the use of the information by the tax authorities (e.g., for the pursuit of tax crimes only and not for other tax purposes?)*

Of the countries that responded to the questionnaire, only **Australia** and the **United States** grant tax authorities direct access to information on suspicious transactions. In the **United Kingdom**, HM Customs and Excise has direct access to suspicious transaction reports. (See section F, for the position of Inland Revenue). In **Austria** (apart from customs fraud and evasion of import and export duties) **the Czech Republic, Finland, Ireland, Italy, Luxembourg, and Poland**, tax authorities have no access to suspicious transaction reports. In **Belgium, Canada, Denmark, France, Germany, Japan, the Netherlands, New Zealand, Norway, Portugal, Spain, the Slovak Republic, Sweden, Switzerland, and the United Kingdom** (as far as Inland Revenue is concerned), tax authorities may have, sometimes under strict conditions, access to reported suspicious transactions. See F.

In **Australia**, the information obtained from suspicious transaction reports is maintained on a centralised database at AUSTRAC. The Australian Tax Office (ATO) has direct access to all Suspicious Transactions provided to AUSTRAC. The ATO has full access, under both law as provided by the FTR Act and in accordance with a Memorandum of Understanding (MOU) between the ATO and AUSTRAC, to utilise AUSTRAC's centralised database.

There are no specific restrictions on the use of information by the tax authorities. Section 4(1) of the FTR Act specifies "The principal object of the Act is to facilitate the administration and enforcement of taxation laws", whilst further objects of the Act are to facilitate the administration and enforcement of laws of the Commonwealth and Territories (other than taxation laws). A further objective is to make the information collected available to State authorities to facilitate the administration and enforcement of the laws of the States. The MOU between the ATO and AUSTRAC restricts access to Suspicious Transactions information to specified officers.

In the **United Kingdom**, HM Customs and Excise receives copies of all suspicious transaction reports from NCIS in their capacity as an investigating and prosecuting authority. NCIS designates to HMCE all reports relating to known drug case suspects and those cases it believes will relate to HMCE's assigned matters including VAT and Excise. HMCE's investigators can contact police forces directly if they believe they have an interest in reports designated to police and vice versa. Use of the information is not restricted to drugs and equally covers tax related offences.

In the **United States**, the Criminal Investigation Division of the Internal Revenue Service and the Office of Investigations of the United States Customs Service have on-line access to the database of suspicious activity reports maintained by FinCEN. The Examination Division of the Internal Revenue Service has on-line access to the same database in its capacity as an auditor of Bank Secrecy Act compliance by non-bank financial institutions. It does not have access to the data for civil tax examination purposes, but it may receive particular suspicious activity reports in connection with particular examinations following a name-specific request for such information to FinCEN.

F. *These questions relate to situations where the anti-money laundering authority has the authority to provide information about specific suspicious transaction reports to the tax authority (e.g., spontaneously) or where the tax authority may make requests for information about specific transaction reports.*

1. *Are the anti-money laundering authorities which receive suspicious transaction reports permitted to pass suspicious transaction reports on to tax authorities which they believe may involve a tax related crime (spontaneously or pursuant to a request)?*
2. *If so, how is the determination made? Are any guidelines given to anti-money laundering authorities to make this determination? If so, please provide a copy.*

In **Australia, the United Kingdom**, as far as HM Customs and Excise is concerned, and the **United States**, the tax authorities have direct access to information provided in suspicious transaction reports, so this question is not applicable to them. In **Austria** (apart from customs fraud and evasion of import and export duties) **the Czech Republic, Finland, Ireland, Luxembourg, and Poland**, tax authorities have no access to suspicious transaction reports. In **Finland, France, and Luxembourg**, the anti-money laundering legislation stipulates that information on suspicious transactions may only be used to combat money laundering, although France covers tax crimes as a money laundering offence. In **Belgium, Canada, Denmark, France, Germany, Italy, Japan, the Netherlands, New Zealand, Norway, Portugal, Spain, the Slovak Republic, Sweden, Switzerland, and the United Kingdom** (as far as Inland Revenue is concerned), tax authorities may have, access to reported suspicious transactions. Sometimes there are very strict conditions to this access, or there is only indirect access through a judicial or law enforcement authority.

In **Austria**, the tax authorities do not have direct access to the data bank of the FIU. The Austrian FIU may only pass on information to fiscal authorities when the suspicious activity relates to customs fraud and evasion of import - export duties. Purely fiscal offences are specifically prohibited from being disclosed by the FIU to fiscal authorities.

In **Belgium and France**, the entities where suspicious transaction reports are required to be filed (in **Belgium**; CTIF and in **France**; TRACFIN) are not allowed to provide the tax authorities with any information. However, in **Belgium** judicial authorities have the obligation to provide the tax authorities on their request with any information they have to ensure taxation. Furthermore, the Public Prosecutor has the obligation to inform the Ministry of Finance immediately on any suspicion of fraud they have concerning direct and indirect taxes. In **France**, the other authorities involved in combatting money laundering, like the judicial authorities, may send any information to the tax authorities in order to have it verified or to start a fiscal investigation.

In **Canada**, the information obtained from suspicious transaction reports will be maintained in FTRACC database. There is no direct access for the tax authorities. However, if FTRACC has reasonable grounds to suspect that the “designated information” would be relevant to investigating or prosecuting both money laundering and tax evasion offences, FTRACC will provide Revenue Canada only with limited “designated information”. Revenue Canada may use this information for the pursuit of any tax matter. The Centre

would be able to disclose this information to Revenue Canada in cases where it determines that a) a reasonable suspicion of money laundering exists; and b) the information is relevant to an offence of evading or attempting to evade taxes or duties imposed under an Act of Parliament administered by the Minister of National Revenue. Suspicion of money laundering is the key criteria and must be met first and foremost. If the centre has reason to suspect tax evasion, but no money laundering, it could not disclose this information to Revenue Canada.

In **Denmark**, the Money Laundering Secretariat or the police district handling further investigation - informs the tax authorities of the relevant facts. There are no guidelines since this exchange of relevant information between public authorities is a normal part of the co-operation between Danish authorities. This is the case regardless of whether the information is from a STR (Suspicious Transaction Report) or from other sources on which no special restrictions are imposed.

In **Germany**, the tax authorities have no direct access to information provided in suspicious transaction reports. Once criminal proceedings have been instituted for a money laundering offence, the tax authorities must be informed of this and must be notified of the facts on which the proceedings are based. Hence there is no need to determine whether or not the information is of use to the tax authorities. The tax authorities may make unrestricted use of such information both for taxation purposes and for criminal proceedings in tax fraud cases. Notwithstanding the reporting obligations under the Money Laundering Act, all courts and authorities are, in principle, obliged to notify the tax authorities if there are grounds to suspect tax fraud.

In **Ireland**, the legislation does not specifically permit a transfer of reports to the tax authorities. Discussions are currently taking place in relation to establishing administrative arrangements to allow access to certain reports (which appear to relate solely to tax evasion) by the tax authorities.

Italy pointed out that article 6 of the 91/308/CEE Directive states as a general rule that the information provided to the competent authorities of the Member States can be utilised only for anti-money laundering purposes. In order to strengthen the efficiency of the anti-money laundering measures and enhancing the collaboration of the disclosing entities, Italian legislation provides for a strict confidentiality regime applicable to the suspicious transactions reports filed with the UIC. The issuing of the reports is, in itself, confidential; as to their content, it can be disclosed only to the investigative agencies to which the UIC transmits the reports after the analysis conducted on the financial profile of the transactions involved. All the information held by the UIC related to the implementation of the suspicious transactions reports procedure is covered by official secrecy, even with respect to Public Administration entities. Official secrecy applies even when a penal proceeding is started. The identity of the persons and of the intermediaries involved in the reports may be revealed only when the judicial authorities, in a warrant specifying the grounds, hold that it is indispensable for the criminal investigation they are conducting. The information obtained from suspicious transactions is maintained by the UIC in a centralised database.

In **Japan**, tax authorities do not have direct access to the information gathered by money-laundering authorities. However, the information can be provided indirectly to tax authorities via law enforcement authorities in the following case. Law enforcement authorities compare the interest of preventing harm to the investigation or judicial proceedings which might be caused by the provision of the information to tax authorities on one hand, and the interests of providing the information to tax authorities on the other. When the latter interests are given priority, the information can be provided to tax authorities.

In the **Netherlands**, if the MOT assesses the reported transactions as suspicious of any crime (including tax-crimes), the reports are passed on to the Prosecutors Office and the Police. The tax authorities have access to the database of suspicious transactions within the framework of an ongoing fiscal-criminal

investigation, if they need this information for an investigation that they are conducting. After the conclusion of the criminal case the public prosecutor can give his consent to the tax-authorities to use the information which has been gathered for tax purposes. No specific guidelines are applicable. If the MOT finds an unusual transaction to be suspicious, directly or after further investigation, it will pass the information on to the law enforcement authorities.

In **New Zealand**, tax authorities have no direct access to the Police database. The information is obtained under a Memorandum of Understanding between the Police and the Inland Revenue Department and/or directly by the tax authority using Section 17 of the Tax Administration ACT 1994. There are no restrictions on the use of information by the Inland Revenue Department. No guidelines have been issued for the determination of having the Inland Revenue Department informed as all suspicious transaction reports are made available to the IRD, which then decides what action to take. The Memorandum of Understanding, The Tax Administration Act 1994, the Official Information Act and the Privacy Act all govern the use and dissemination of information obtained.

In **Norway**, in accordance with the Financial Services Act, information provided in suspicious transaction reports may only be used in connection with the work of the prosecuting authority. The prosecution authority/the police will usually not forward such information to other public authorities, unless this is a part of their own investigation of legal offences. This means that investigations must have been started before information provided in suspicious transaction reports can be forwarded to the tax authorities. However, the need for the Norwegian tax authorities to receive this information is limited, since tax avoidance and evasions are legal offences in Norway, and since these types of crimes are being investigated by the police/prosecuting authority and not the tax authorities.

In **Portugal**, tax authorities do not have access to information on suspicious transactions because it is constitutionally forbidden. Access to information related to tax crimes is only possible through a certificate from a judicial authority (Ministério Público) drawn out from the judicial inquiry into a money laundering crime. The information obtained can only be used to pursue tax crimes and to enforce tax assessments.

In the **Slovak Republic**, the Bureau of the Financial Police is an authority receiving the reports on the suspicious bank information authorised to use the received reports only for the purposes of the tasks imposed by the Law on the Police Force no. 171/1993 (Col. of Laws). The tasks of the Bureau of the Financial Police are specified in §2 par. 1 e) and d) of the given Law as detection of crimes and identification of relevant perpetrators, co-operation in detection of tax evasion and illegal financial operations. In this context, the Bureau of the Financial Police is authorised to use the information involved in the reports on the suspicious bank operations also for the purposes of detection of tax related crimes. In view of the fact that the Slovak tax authorities are not in charge of documentation and (criminal) investigation of tax crimes, they are not provided with information from reports on suspicious bank information (spontaneously). However, there may be some jointly implemented measures with the relevant tax-office in specific cases of reported suspicious bank information with the aim of checking the suspicion of a committed crime. That means the tax authorities could be involved and would have the right to access the reports of suspicious bank information when the data from such reports relate also to the taxation.

In **Spain**, information about specific suspicious transaction reports is not passed on to tax authorities. However, indirectly, through the Office of the Public Prosecutor and only in cases involving organised crime, information is provided by the SEPBLAC to the tax authorities.

In **Sweden**, information may be passed on to the tax authorities but the Swedish Financial Unit has to examine the material before passing it on to the tax authorities (i.e. information can be passed on spontaneously or pursuant to a request, but not automatically). This possibility is laid down in the secrecy

law, but the Swedish Financial Unit has no experience so far in applying the law. If the information is passed on to the tax authorities, the Financial Unit has to consider the inconvenience for the person involved compared with the public damage, e.g. the aggravation of crime.

In **Switzerland**, tax authorities have no direct access to information on suspicious transactions obtained by the Bureau de Communication. However, indirect access is possible to information that the Bureau de communication has sent to the cantonal criminal magistrate's court. Tax authorities also may have access in cases where the fiscal law contains a provision on internal mutual assistance. On the information obtained, the fiscal pledge of secrecy has to be respected.

In the **United Kingdom**, there is a central database to which the Inland Revenue may have access in certain controlled circumstances. The information may only be accessed by the Inland Revenue Special Compliance Office (SCO), who has responsibility for cases involving serious fraud. SCO may make a search request for existing intelligence, or receive spontaneous intelligence from the suspicious transaction reports. Each report is analysed and those considered to have potential tax implications are passed to the Inland Revenue officer on secondment. If this officer identifies significant potential tax implications within the scope of the IR SCO's responsibilities, a report is made for transmission to IR. Every report is suitably "sanitised" (i.e. irrelevant and unnecessary information is excised, as well as the identity of the suspicious transaction reporter) and is given to the Head of the Economic Crime Unit for approval that it is properly disclosed before dissemination. Restrictions on the use of information are recorded in a Memorandum of Understanding between the National Criminal Intelligence Service and the Inland Revenue. This provides that information/ intelligence passing from NCIS to SCO may not be disseminated to other parties or agencies without the agreement of NCIS. In fact, we understand that under no circumstances would NCIS give permission for either a copy of or the substance of the intelligence to be passed to any other person, including the taxpayer concerned. To do so would be a breach of the "tipping off" provisions of the money laundering legislation. Intelligence from STRs passed from NCIS to the Inland Revenue can be used only by SCO for the purposes of a fraud investigation. As a means of ensuring that these restrictions are complied with, there are arrangements within SCO for all review papers which relate to intelligence received from NCIS to be filed separately from other papers, and to be given the appropriate level of additional security. The reports cannot be used directly as evidence in the SCO investigation. Their purpose is to provide the background intelligence, which can help the SCO know where to look. (See section B, for HM Customs and Excise).

G. *Please describe briefly the confidentiality provisions which may restrict the disclosure of information contained in suspicious transaction reports by anti-money laundering authorities. If possible, please provide a copy of such provisions.*

In **France, Finland and Luxembourg**, the anti-money laundering legislation stipulates that the information on suspicious transactions may be disseminated only to combat money laundering. In **Austria**, the FIU may only pass on information concerning customs fraud and evasion of import and export duties; purely fiscal offences are specifically prohibited from being disclosed to the fiscal authorities. In **the Czech Republic, Finland, Ireland, Luxembourg, and Poland**, tax authorities have no access to suspicious transaction reports. All countries have strict confidentiality provisions on the information obtained by the anti-money laundering authorities. In the countries where the tax administration has access to this information, there is a legal basis to provide this access. If this access is provided there are generally no restrictions other than that the information may be used for tax purposes only.

In **Australia**, pursuant to the secrecy provisions contained in the Financial Reports Acts 1998 (FTR Act), a member of the staff of AUSTRAC shall not make a record of any information or divulge or communicate to any person any information obtained by the person in the course of performing duties under the FTR Act, except where it is necessary to do so for the purposes of carrying into effect the provisions of the FTR Act.

In **Belgium**, the CTIF is subject to a very strict professional secrecy. Besides the cases where testimony is required in court, the staff of the CTIF may only provide information to the judicial authorities, foreign organisations which have the same assignment as the CTIF, the European Committee Unit that co-ordinates the combat of fraud and in some cases to the guardianship board.

In **Canada**, as mentioned under F, only designated information may be provided to Revenue Canada. All other disclosure of the Centre to Revenue Canada is prohibited.

In the **Czech Republic**, the person making a report shall keep secret the report on an unusual transaction or on steps taken by the Ministry under the Money Laundering Act in respect of third persons, including persons whom the reported information concerns; the obligation to maintain this confidentiality applies to every employee of the reporting institution as well as to every person who acts on his behalf on the basis of a contract. The special Act stipulates the obligation of employees of the Ministry to maintain confidentiality about steps taken under the Money Laundering Act and about the information obtained in the course of its implementation.

In **Denmark**, exchange of information with non-law enforcement authorities is carried out in accordance with the principles of section 28 of the Danish Public Administration Act. This provision concerns the exchange of information between Danish authorities. According to this provision, exchange of confidential information can be carried out, e.g. when the following conditions are fulfilled: 1) private or public interests are more important than the secrecy of the confidential information, 2) the information is necessary for the requesting authority, so that it can carry out its tasks concerning supervision or control or 3) the information is of essential importance for the activities of the authority or for a decision, which the authority is going to make. Before every exchange, an individual assessment concerning the compliance with the conditions needs to be made. For the Danish STR-system there are no general restrictions in relation to tax crimes. If the Money Laundering Secretariat receives STR-information from other countries for restricted use, the tax authorities have only access to the information in so far as it is accepted by that country. This is not formulated in a provision but is the accepted interpretation of the scope of the mentioned provision in the Danish Public Administration Act.

In **Germany**, the information contained in a suspicious transaction report under the Money Laundering Act may not be used for the prosecution of criminal offences punishable by a term of imprisonment not exceeding three years. This does not apply to its use for taxation purposes and for criminal proceedings in tax fraud cases.

In **Ireland**, the legislation does not yet specifically permit a transfer of reports to the tax authorities.

In **Japan** the confidentiality regulation derives from the duty to protect privileged information based on the provisions of the National Public Servant Law.

In the **Netherlands**, there are no specific secrecy laws, which restrict the reporting of unusual transactions to the MOT. The relation between financial service providers and clients is based on a contract. The rules of the civil code, which are applicable to this contractual relation, ensure confidentiality of all information a financial institution possesses about a client. However, according to Dutch law in the field of tax and criminal investigation, investigators have access to the information.

In **New Zealand**, there are no restrictions on the information provided by the New Zealand Police to the Inland Revenue Department. The information gathering provisions of the Tax Administration Act 1994 override the Privacy Act.

For **Poland**, due to the lack of disclosure of information on suspicious transactions, this question is not applicable.

As far as **Portugal** is concerned, in principle the information is restricted by the Bank Secrecy (Decree-Law no 298/92 of 31st December), by the Fiscal Secrecy (Lei Geral Tributária) and by the Justice Secrecy (Código do Processo Penal). So, only in special conditions, as referred to in sections E2 and E3, can the information be revealed.

In the **Slovak Republic**, the protection of classified information is dealt with by:

1. Law No. 100/1 996 (Coll. of L.) about the Protection of the Governmental Secrecy (i.e. the highest possible level of the protection of classified information), Official Secrecy (i.e. the second highest level of the protection of classified information) and the Cipher Protection of Information (encryption); and
2. the § 2 of the Decree of the Ministry of Interior No. 181/1997 (Coll. of L.) of the Suspicious Bank Operations; and
3. the § 38, par. 3) of the Law No. 21/1992 on Banks (as amended).

In **Spain**, the confidentiality obligation extends (by virtue of the duty of professional secrecy), to all persons who are working or have worked for the Commission and have gotten to know about its operations or of data meant to be kept secret. Even after having ceased in his/her post, those persons are not allowed to publish, pass on or show confidential data or documents, unless they are expressly authorised by the Commission. The law contains a few exceptions;

- (a) if the person concerned gives his/her consent,
- (b) for statistical purposes, etc;
- (c) following a request from Parliamentary Committees or from Judiciary or Administrative authorities.

This confidentiality obligation also extends to persons, agencies or authorities receiving confidential information from the Commission, information which then could be used only in the framework of their legally defined functions. The confidentiality is circumscribed to the scope of the Law, that is to say preventing the financial system from being used for money laundering in relation to the proceeds of criminal activities connected to drug trafficking, terrorism and organised crime.

In **Sweden**, the information received by disclosures have the same secrecy level as the information contained in the criminal register. Practically, this implies that other police units can obtain information on demand if it is of importance in their investigation.

In **Switzerland**, Article 32 of the “Loi sur le Blachiment d’Argent” (LBA) provides that the co-operation of the MROS with the foreign penal prosecution authorities is laid down by article 13, second paragraph, of the Federal Act of 7 October 1994, concerning “les Offices centraux de police criminelle de la Confédération”. In addition, the MROS may provide personal information to foreign authorities if this is set forth in an act or international convention, or if the information is required exclusively to combat money laundering, or a Swiss request for information is in the interest of the person whom it concerns, in which case either the person involved must have consented or the circumstances allow the presumption of his consent.

In the **United Kingdom**, the National Criminal Intelligence Service may pass intelligence to other competent investigating bodies only for the purpose of criminal investigations within their province. In relation to reports to the Inland Revenue, disclosure is made under the conditions of the Memorandum of Understanding between NCIS and IR SCO (see section F). HM Customs and Excise has a Memorandum of Understanding with NCIS relating to the security of the information.

In the **United States**, the access to suspicious transaction reports are limited only by the general provisions of the statute called The Privacy Act of 1974, with whose terms the above described arrangements comply. Accordingly, tax authorities generally have access to information gathered by anti-money laundering authorities for purposes of investigating tax-related crimes and in certain other circumstances.

III. Access to Other Reports

In addition to suspicious transaction reports, some countries require reports of other types of financial activity. These may include reports of large currency transactions, cross-border movements of currency, electronic transfers of funds in and out of the country, and reports of other transactions.

A. *Please identify and describe any other types of transaction reports that are required or permitted to be filed with an anti-money laundering authority.*

In **Austria, Belgium, Denmark, Finland, France, Germany, Japan, Luxembourg, the Netherlands, New Zealand, Poland, Portugal, Sweden, and Switzerland**, no reports of other types of financial activity are required to be filed. **Australia, Canada, the Czech Republic, Germany, Ireland, Italy, Norway, the Slovak Republic, Spain, the United Kingdom** and the **United States** require other types of transactions to be reported. The transactions mainly concern cross border cash or other financial transactions and transactions related to drug trafficking.

In **Australia**, the following reports are required to be filed with Austrac:

1. Significant Cash Transaction Reports (Cash transactions involving the transfer of currency (cash) of not less than \$A 10,000 in value are reported by cash dealers and solicitors/lawyers to AUSTRAC as Significant Cash Transactions).
2. International Currency Transfer Reports (International Currency Transfer Reports are prepared by persons who transfer currency of \$A 10,000 or more, or its foreign currency equivalent, into or out of Australia. Most commonly, this information is collected by the Australian Customs Service at international departure and arrival points and forwarded to AUSTRAC.)
3. International Funds Transfer Instructions (An International Funds Transfer Instruction is an instruction for a transfer of funds (no minimum limit) that is transmitted into or out of Australia electronically or by telegraphic transfer.)

In **Belgium**, the CITF may exchange any information that it finds useful to accomplish its task not only on behalf of the financial organisations and other institutions regarded by the law, but also on behalf of the police and the Service of the Administration of the State. Furthermore, the CTIF may carry out an on-site examination of useful documents belonging to or in the possession of the financial organisations and other institutions covered by the law.

In **Canada**, the bill provides for a regime which requires that all persons who import/export large amounts of currency and other monetary instruments to/from Canada report these movements to Revenue Canada (Customs). The bill also requires the reporting of "prescribed transactions". What will constitute such transactions is being developed through consultations with the reporting entities.

In the **Czech Republic**, there is a special obligation for the customs authorities to report facts to the Ministry if, during the performance of their duties or in connection with them, they ascertain that valid banknotes, coins, cheques or traveller's cheques in an amount exceeding CZK 200.000 (about USD 5.500), have been transported. Same reporting duty applies also to a person (entity) whose business activity

includes postal services under a special Act, if a postal order to be sent abroad exceeds CZK 200.000 (about USD 5.500).

In **France**, TRACFIN may collect information on criminal aspects of a financial operation at the police, the gendarmerie and the offices of the Public Prosecutor.

Germany carries out checks on cross-border transport of cash. If such checks give grounds to suspect money laundering, the officers conducting the checks (customs officers or border guards) will report the case to the responsible customs investigation office or, in most of the Länder, to a joint police/customs financial investigation group. These reports are maintained in a centralised database on suspected money laundering. The tax authorities do not have direct access to the database. The reports may be passed on spontaneously to the tax authorities where there is reason to suspect the transport of cash or equivalent means of payment for the purpose of money laundering. There are no specific guidelines for determining which cases are passed on to the tax authorities. However, if there are only grounds to suspect tax evasion and no indications of money laundering, the personal data acquired in the course of the check may not be passed on to the tax authorities. These restrictions on disclosure are governed by the special arrangements for checks on cash reports.

In **Ireland**, not only suspicious transactions concerning money laundering have to be reported but any suspicion on transactions concerning drugs trafficking or other criminal activity.

In **Italy**, any physical transfer of cash, securities and valuables at the border or by postal parcel, to or from a foreign country, by residents and non residents, in an amount exceeding 20 million Lire or the equivalent must be declared to the Ufficio Italiano dei Cambi.

The declarant has to indicate, in particular:

- a. his personal data and the details of his identification card as well as, if a resident, his tax code;
- b. the personal data of the person on behalf of whom the transfer is made as well as the person's tax code, if he resides in Italy.
- c. the amount of the cash, securities and valuables being transferred.
- d. the transfer is to or from a foreign country.

Furthermore, financial intermediaries are requested to transmit to the UIC on a monthly basis data in an aggregated form concerning their overall operation. The aggregations are made on information related to financial transactions exceeding the threshold of 20 million Lire.

The UIC performs on such data analyses aimed at identifying possible money-laundering phenomena on a local basis. The UIC is authorised to gather the aforementioned data, even through direct access from the electronic archive held by each intermediary.

In **New Zealand**, in relation to every transaction conducted through a financial institution, the financial institution shall keep such records as are reasonably necessary to enable the transaction to be readily reconstructed at any time. There is no requirement for a financial institution to report a normal business transaction although when the transaction exceeds NZD \$ 9,999,99, it triggers various responsibilities under the Financial Transaction reporting.

Norway gave a description of *some* of the financial activities that banks, etc are instructed to report:

- Authorised foreign exchange banks are instructed to report the capital turnover by using a special computer based reporting system to the Central Bank of Norway,
- Persons or entities that are residents of Norway are instructed to report to the Central Bank of Norway when an account in a foreign bank has been established. There is, however, an exception for private bank accounts.
- Any other bank transaction or the establishment of a payment arrangement with a non-resident must be reported to the Central Bank of Norway.

Both residents and non-residents are instructed to report any import or export of currency while entering or leaving Norway, if the amount exceeds NOK 25.000 per person per passage. There is a corresponding duty connected to delivery by post.

In the **Slovak Republic**, under the Foreign Exchange Act No. 202/95 Col. of Laws, in the sense of the Decree 203/95 Col. of Laws (in the wording of the Decree 335/96 Coll. of Laws), transmission of foreign currency in cash over 150 000. - SKK must be reported.

In **Spain**, the so-called documents B1 and B3 refer to Customs declarations of cross border movements of currency (inflow and outflow), as well as the systematic reporting, on a monthly basis, of the operations in paragraph II, section B (physical movements of cash, travellers cheques or other documents and operations carried out by individual persons or legal entities resident in tax havens involving a sum amounting to PTS 5 million or more.

In the **United Kingdom**, the focus of the anti-money laundering intelligence is on suspicious transaction reports. However, HM Customs and Excise maintains a database of cases where cash is detained or seized at borders under the Drugs Trafficking Act. That database can be accessed by NCIS for drugs related cases.

In the **United States**, the Bank Secrecy Act also requires the filing of numerous other reports of financial activity, including: 1. currency transactions in excess of \$10,000, 2. maintenance by U.S. citizens or residents of bank or brokerage accounts outside the U.S. with balances of at least \$10,000, and 3. transportation of at least \$10,000 in currency and bearer instruments into or out of the United States. Certain exceptions apply to these broad reporting definitions.

B. *For each of the reports mentioned in paragraph A, identify the persons/entities required to file the report(s).*

In the countries where these transactions have to be reported, persons and entities that carry out the transactions are required to file the reports.

In **Australia**, cash dealers are required to report on Significant Cash Transaction Reports and International Funds Transfer Instructions. The persons who transfer the currency are required to report under the International Currency Transfer Reports.

In **Canada**, concerning cross-border reporting, in the case of hand carried movements, by the person carrying the goods. In the case of commercial shipments, an initial report will be expected from the carrier to identify the currency movement following which a detailed report will be expected from the importer and in the case of export shipments, from the exporter. In case of shipments sent by mail or courier, by the person exporting the goods from Canada or by the persons who sent the shipment to Canada. As far as Prescribed Transactions are concerned, the reporting entities are the same as those for suspicious transactions.

In the **Czech Republic**, the customs authorities and the subject who carries out postal services have to file these reports.

In **Ireland**, all the persons and entities that have to report the suspicious transactions on money laundering also have to report.

In **Italy**, concerning the transfer of cash etc., every physical person, even if transferring the amount on behalf of third parties or a legal entity, has to report. Concerning the financial intermediaries, every intermediary who, according to the law is authorised to channel payment or transfer in cash or in bearer

instruments exceeding 20 million Lire, has to report. They are: officers of the public administration, banks, securities firms, stockbrokers, securities investment fund management companies, trust companies, insurance companies and Monte Titoli S.p.A.

In the **Slovak Republic**, all physical persons crossing the border have to report if they meet the criteria.

In **Spain**, with reference to documents B1 and B3; as far as inflow of currency is concerned, non-residents carrying a sum amounting to PTS 1 million or more to be invested in Spain; as far as outflow of currency is concerned, any person planning to take out of the Spanish territory a sum of 1 million pts or more. With reference to the operations described in paragraph II, section B the corresponding persons/entities subject to the obligation to furnish information, particularly the ones mentioned in paragraph II, section.C, points a) to h).

In the **United Kingdom**, HM Customs and Excise's National Investigation Service (NIS) Financial Investigation Branch (FIB) maintain the database of cash detention cases.

In the **United States**, reports of currency transactions in excess of \$10,000 are filed by most financial institutions (with the exception of insurance companies and commodities futures merchants). U.S. citizens or residents must report on their tax returns if they hold bank or brokerage accounts outside the U.S. with balances of at least \$10,000 and persons entering the U.S. must report cross-border transportation of at least \$ 10,000 in currency and bearer instruments.

C. For each of the reports mentioned in paragraph A, identify the national agency or body with which the report is required to be filed. If the report is required to be filed with more than one agency or body, please describe briefly the responsibilities each agency or body has with respect to the information (e.g., compilation of data, analysis, of data, identification of transactions to investigate).

In the countries concerned, the reports have to be filed with the national FIU, the Central Bank or with Customs.

In	Reports have to be filed with
Australia	Austrac
Canada	Revenue Canada
Czech Republic	Ministry of Finance, Financial Analytical Unit
Ireland	Garda Bureau of Fraud Investigation
Italy	UIC
Norway	Central Bank
The Slovak Republic	Customs Directorate
Spain	Sepblanc
United Kingdom	HM Customs and Excise
United States	IRS

In **Canada**, all cross-border reports are received by Revenue Canada (Customs) and reports resulting from prescribed transactions will be forwarded to the Financial Transactions and Reports Analysis Centre.

In **Italy** the declaration of cross-border movement is received by the UIC through customs offices, banks, post offices or Guardia di Finanza officers that collect and transmit them. The data are utilised by the UIC for purposes of combating money laundering and for other institutional purposes. As derogation to the official secrecy rule, the information received by the UIC can be transmitted to the tax authorities, which utilise them for their institutional ends. The aggregated data transmitted by the financial intermediaries are filed only with the UIC

In the **Slovak Republic** the transmission of foreign currency must be filed to the Customs Directorate. Its responsibilities are the data compilation, analysis of data, identification of transactions and also investigation of these transactions.

In the **United Kingdom**, HM Customs and Excise have primacy for dealing with cash seizure cases. HMCE and the National Criminal Intelligence Service are responsible for the intelligence.

In the **United States**, reports of currency transactions in excess of \$1 0,000 are filed with the IRS. U.S. citizens holding bank or brokerage accounts outside the U.S. with balances of at least \$10,000 report such information to the Department of the Treasury, and cross-border transportation of at least \$10,000 in currency and bearer instruments is reported to the U.S. Customs Service.

D. *Please answer the questions below with respect to each type of report mentioned in paragraph A. These questions relate to situations where tax authorities have direct access to the information provided in the reports.*

- 1. Is the information obtained from the report maintained in a centralised database? If so, do the tax authorities have access to the database? If so, under what circumstances do they have access?*
- 2. If the information is not maintained on a database, do the tax authorities have access to the information? If so, under what circumstances do they have access?*
- 3. Are there restrictions on the use of the information by the tax authorities (e.g., for the pursuit of tax crimes only and not for other tax purposes?)*

In **Australia, the Slovak Republic, the United Kingdom and the United States**, the reports are maintained in centralised databases. Except for the **Slovak Republic**, tax authorities have access to these reports. **Canada, the Czech Republic, Ireland, Italy, and Norway** did not provide information on a database; in these countries tax authorities have no access to the reports.

In **Australia**, the information is stored on AUSTRAC's centralised database. The ATO has access by law and through the MOU. There are no specific restrictions in Australia on the use of information by the tax authorities. Section 4(1) of the FTR Act specifies "The principal object of the Act is to facilitate the administration and enforcement of taxation laws", whilst further objects of the Act are to facilitate the administration and enforcement of laws of the Commonwealth and Territories (other than taxation laws). A further objective is to make the information collected available to State authorities to facilitate the administration and enforcement of the laws of the States. The MOU between the ATO and AUSTRAC restricts access to Suspicious Transactions information to specified officers.

In **Canada**, tax authorities do not have direct access to the information provided in the import/export reports on currency.

In the **Czech Republic**, the tax authorities have no access to the information provided in the reports.

In **Ireland**, the legislation does not specifically permit a transfer of these reports to the tax authorities.

In **Italy**, it is foreseen that any information collected by the UIC on cross-border movements over 20 million Lire, as described at Question III, section A, are transmitted to the Ministry of Finance for tax purposes. Said Procedure has not been implemented yet.

In **Norway**, the need for the Norwegian tax authorities to receive this information is limited, since tax avoidance and evasion are legal offences in Norway, and since these kinds of crimes are being investigated by the police/prosecuting authority and not the tax authorities. The questions raised in III D, E and F are, therefore, of little relevance to Norway.

In the **Slovak Republic** the information obtained from the report is maintained in a centralised data base and the tax authorities do not have free access to the data base, they may obtain information only upon a written request. There are certain restrictions on the use of this information by the tax authorities - Article 23 - Obligation to preserve secrecy of the Law on Tax and Fees Administration (No. 511/1992 Coll. of Laws). It is possible to pass information only to courts, authorities active in criminal proceedings and to provide the treaty partner with tax information according to the relevant Article of the Tax Convention.

In the **United Kingdom**, Inland Revenue has direct liaison with HMCE with regard to HMCE's reports of the seizure of cash suspected to be the proceeds of drugs-related crime, and there is therefore no need for them to receive information from NCIS in these cases. IR interest is in particular in those seizures where drugs involvement is not established and the cash is therefore returned. There may be cases where this intelligence is relevant to an inquiry into tax fraud.

In the **United States**, generally all of the information described in the sections A, B and C is available to federal tax authorities and is maintained on-line by both the Internal Revenue and Customs Services. In addition, federal tax authorities receive reports (for example, reports of the receipts of more than \$10,000 in currency by non-financial trades or businesses) that they may use in money laundering investigations that also involve income tax charges but that may not be shared with other federal or state investigators. The same condition, of course, applies to tax returns themselves.

E. *These questions relate to situations where the anti-money laundering authority has the authority to provide information about a specific report to the tax authority (e.g., spontaneously) or where the tax authority may make a request for information about a specific report.*

1. *Are the anti-money laundering authorities which receive the reports identified in paragraph A permitted to pass specific reports on to tax authorities which they believe may involve a tax related crime (spontaneously or pursuant to a request)?*
2. *If so, how is the determination made? Are any guidelines given to anti-money laundering authorities to make this determination? If so, please provide a copy.*

In **Austria** and the **Czech Republic**, tax authorities have no access to the reports identified in Section A. In **Australia**, **Canada** (with restrictions), **Italy**, the **Slovak Republic**, **Spain**, **Sweden**, the **United Kingdom**, and the **United States**, the reports identified in section A, are accessible by the tax authorities.

In **Austria**, the FIU may only pass on information concerning customs fraud and evasion of import and export duties; purely fiscal offences are specifically prohibited from being disclosed to the fiscal authorities.

AUSTRAC is permitted under **Australian** law to pass all financial transaction reports information on to the ATO. Other anti-money laundering authorities, which are responsible for the investigation of crimes associated with money laundering activities are authorised to pass information to the ATO regarding tax-related crime (subject to relevant MOU). In respect of AUSTRAC, there is no requirement for a determination to be made as the ATO has access to all financial transaction reports held by the AUSTRAC. This negates the need for any guidelines, notwithstanding the provisions of the MOU between the ATO and AUSTRAC.

Canada referred for this question to the answer on part II, section F, question 2, where Canada noted that, the information obtained from suspicious transaction reports will be maintained in FTRACC database. There is no direct access for the tax authorities. However, if FTRACC has reasonable grounds to suspect that the “designated information” would be relevant to investigating or prosecuting both money laundering and tax evasion offences, FTRACC will provide Revenue Canada only with limited “designated information”. Revenue Canada may use this information for the pursuit of any tax matter. The Centre would be able to disclose this information to Revenue Canada in cases where it determines that a) a reasonable suspicion of money laundering exists; and b) the information is relevant to an offence of evading or attempting to evade taxes or duties imposed under an Act of Parliament administered by the Minister of National Revenue. Suspicion of money laundering is the key criteria and must be met first and foremost. If the centre has reason to suspect tax evasion, but no money laundering, it could not disclose this information to Revenue Canada.

In the **Czech Republic**, the tax authorities have no access to the information provided in the reports.

In **Italy**, the Legislative Decree n. 125/1997 specify that the nominative data and information gathered by the UIC concerning physical cross-border movements of valuables for anti-money laundering purposes must be transmitted to the tax authorities which can utilise them for their fiscal purposes.

In the **Slovak Republic** The anti-money laundering authorities which receive the reports identified in paragraph A are permitted to pass reports on to tax authorities which they believe may involve a tax related crime and this can be done spontaneously. There are no guidelines in this regard.

In **Spain**, in the present situation, it is possible in respect of documents B1 and B3, when the information contained in those documents is requested by the tax authorities. Regarding the systematic reporting, the criterium indicated in paragraph II, section F.1. applies. Spain responded to the question concerned that information about specific suspicious transaction reports is not passed on to tax authorities. However, indirectly, through the Office of the Public Prosecutor and only in cases involving organised crime, information is provided by the SEPBLAC to the tax authorities. As far as documents B1 and B3 are concerned, the determination is made on the basis of the tax authorities’ specific request; as far systematic reporting, the criterium indicated in paragraph II, section F.1. applies.

In **Sweden**, if the Swedish Financial Unit detects a suspicious transaction indicating tax crime, the information can be passed on to tax authorities under the conditions given in II F 2 above.

In the **United Kingdom**, these reports may be made spontaneously to Inland Revenue, although as mentioned above the IR has direct liaison arrangements with HM Customs and Excise with regard to seizure reports. Any reports from the intelligence officers at the Economic Crime Unit are made via the Inland Revenue officer on secondment. The reports are assessed and if there are significant potential tax implications within the scope of the Inland Revenue Special Compliance Office’s responsibilities a report

is made for transmission to IR. The Head of unit gives permission before dissemination to the IR.HM Customs and Excise receives the reports directly, as described above.

In the **United States**, FinCEN does not spontaneously forward such reports to the IRS (because, as noted, the IRS has, full on-line access to this information).

F. *Please describe briefly the confidentiality provisions which may restrict the disclosure of information contained in the reports identified in A¹ by anti-money laundering authorities. If possible, please provide a copy of such provisions*

In **France, Finland and Luxembourg**, the anti-money laundering legislation stipulates that the information on suspicious transactions may be disseminated only to combat money laundering. In **Austria** the FIU may only pass on information concerning customs fraud and evasion of import and export duties; purely fiscal offences are specifically prohibited from being disclosed to the fiscal authorities. In **the Czech Republic, Finland, Ireland, Luxembourg, and Poland**, tax authorities have no access to suspicious transaction reports. All countries have strict confidentiality provisions on the information obtained by the anti money laundering authorities. In the countries where the tax administration has access to this information, there is a legal basis to provide this access. If this access is provided there are generally no other restrictions than that the information may be used for tax purposes only.

In **Australia**, pursuant to the secrecy provisions contained in the FTR Act, a member of the staff of AUSTRAC shall not make a record of any information or divulge or communicate to any person any information obtained by the person in the course of performing duties under the FTR Act, except where it is necessary to do so for the purposes of carrying into effect the provisions of the FTR Act.

In **Canada**, FTRACC can only pass on limited “designated information where it has reasonable grounds to suspect that the “designated information” would be relevant to investigating or prosecuting both money laundering and tax evasion offences. Revenue Canada (Customs) may only disclose information to the police where they have reasonable grounds to suspect a money laundering offence. They may not provide copies of any cross border currency reports to the police or other law enforcement officials. All reports must be forwarded to the Centre who may, in turn disclose information where they have reasonable grounds to suspect a money laundering offence. Confidentiality provisions pertaining to cross border currency reports are contained in sections 37 and 38 of the bill.

In the **Czech Republic**, the person making a report shall keep secret the report on an unusual transaction or on steps taken by the Ministry under the Money Laundering Act in respect of third persons, including persons whom the reported information concerns; the obligation to maintain this confidentiality applies to every employee of the reporting institution as well as to every person who acts on his behalf on the basis of a contract. The special Act (Labour Code) stipulates the obligation of employees of the Ministry to maintain confidentiality about steps taken under the Money Laundering Act and about the information obtained in the course of its implementation. Moreover, the special provision on the Duty of Confidentiality, which is defined in the Administration of Taxes Act, is applied to the customs authorities.

In **Italy** the UIC can pass the information processed in its anti-money laundering activities only to the competent investigative agencies. This applies for both the suspicious transaction reports and the results of the analysis conducted on aggregated data transmitted by the intermediaries. The confidentiality provisions, which impede to disclose information related to suspicious transaction reports to tax authorities, have been indicated at Question II, sections E, F and G.

1. In the questionnaire this question referred to suspicious transaction reports, which was incorrect as that subject had been dealt with in Paragraph II, section G.

Spain referred for the confidentiality provisions to those indicated in paragraph II, section G.

In **Sweden**, information of this kind is protected under the general provisions of the secrecy law and special regulations regarding police register. Generally, information can be given to other authorities further to the conditions laid down in the secrecy law.

In the **United Kingdom**, for Inland Revenue the restrictions described above would apply to any reports of this type made to the Inland Revenue. The agreement between HM Customs and Excise and the National Criminal Intelligence Service restricts the disclosure of original suspicious transaction reports to the NIS case investigators. Information within the reports can be disclosed to Inland Revenue under information sharing arrangements.

In the **United States**, the information can generally be obtained by federal tax authorities without restrictions.

IV. Other Criminal Intelligence

Anti-money laundering authorities may also gather or otherwise have access to criminal intelligence information other than that received through suspicious transaction reports or other reports. This type of information could include information concerning patterns or trends in money laundering activities.

A. Do the tax authorities have access to criminal intelligence information (other than the reports referred to in Parts II and III) gathered or accessed by anti-money laundering authorities?

In **Austria, Canada, the Czech Republic, Finland, Ireland, Norway, Poland, Portugal** and the **Slovak Republic**, tax authorities have no access to this information. Annual reports on activities including pattern and trends in money laundering are published in **Belgium** by the CTIF, in **Luxembourg** by The Service Anti-Blanchiment and in **France** by TRACFIN. These reports are publicly available and may be used by the tax administrations. In **Australia, Japan, Italy, the Netherlands, Spain, Sweden** and the **United States**, tax authorities have full access to this information, whereas in **Germany** and **Switzerland** only indirect access through a judicial or law enforcement authority is possible.

The **Australian** and **New Zealand** Tax Office have full access to criminal intelligence information, as do Inland Revenue and HM Customs and Excise in the **United Kingdom**.

In **Denmark**, the tax authorities can have all information, which is relevant either for tax crimes or the prevention of tax crimes. Furthermore, they can have all information, which might be useful for their role in the anti-money laundering system. This role is based on the normal co-operation between public authorities. The Central Customs and Tax Administration has sent circular letters to all customs and tax authorities to ensure that these authorities report to the Money Laundering Secretariat. There is no distinction between information from STRs and other information held by the Money Laundering Secretariat.

In **Japan**, criminal intelligence information (other than the reports referred to in Parts II and III) gathered or accessed by anti-money laundering authorities, can be provided indirectly to tax authorities via law enforcement authorities. It depends on law enforcement authorities what information can be provided

In **Germany**, tax authorities have no direct access to this information but all authorities and courts are, in principle, obliged to notify the tax authorities if there are grounds to suspect fraud.

In **Italy**, there are no limitations as to the exchange of information between anti-money laundering authorities and tax authorities concerning general typologies of transactions that come to light, as well as patterns or trends in money laundering activities.

In the **Netherlands**, the investigation tax authorities have in principle access to all criminal intelligence information, but not to the unusual transaction reports, since these are not yet suspicious. Nevertheless, information gathered by the MOT can be used by tax authorities for analysing patterns or trends and other studies of (tax) crimes in general.

In **Spain**, information concerning patterns or trends in money laundering activities is normally included in reports or memoranda from national bodies (such as SEPBLAC or the Police) or international bodies (such as the FATF). Consequently, they are common knowledge and easily accessible, in particular when they are published. In that sense, it seems irrelevant to talk about confidentiality provisions, which may restrict or hinder access on the part of tax authorities. On the other hand, tax authorities can, as a general rule and by virtue of Art. 112 of the Ley General Tributaria, request from other authorities and from any public official, data which the former deem to be of fiscal importance, being the latter obliged to provide them.

In **Sweden**, the tax authorities have direct access to this information.

In **Switzerland**, only indirect access is possible to information that the Bureau de communication has sent to the cantonal criminal magistrate's court. Access is possible as far as the information is necessary for the application of the fiscal law. In any case, the fiscal secrecy rules must be applied.

In the **United States**, tax authorities generally have broad access to criminal intelligence information gathered or accessed by anti-money laundering authorities, but in general, only for the investigation of tax-related crimes.

B. *If so, what type of information does this include and under what circumstances do the tax authorities have access?*

Apart from annual reports on patterns or trends in money laundering, which are generally publicly available, the information, if available to tax authorities, would be restricted to information necessary for the assessment of taxes.

In **Australia**, the information sought would generally be limited to information relevant to establishing a person's Australian tax liability. In **Belgium**, the annual report of the CTIF contains information on the activities of the Committee, especially international activities, a typological analysis of the cases which the Committee has sent to the judicial authorities, statistics on the cases dealt with, and a summary on case law concerning money laundering. In **Luxembourg**, the annual report of the Service Anti Blanchement contains a section with the latest trends on money laundering and other information not related to specific cases. Other information obtained by the Service Anti Blanchement (e.g. as a result of exchange of information with foreign anti-money laundering authorities) which relates to specific cases may not be sent to the tax authorities. In **Japan**, the information that can be provided would depend on the law enforcement authorities. In **New Zealand**, the Inland Revenue Department can access any information, which is required for the enforcement of the Act. This includes Customs movement checks, assets held overseas, financial transactions (business and personal). In **Sweden**, the names of individuals, companies and transactions can be passed on to the tax authorities under the above-described conditions. In addition, the Swedish Financial Unit can pass on all kinds of information concerning new modus operandi and strategic information. The **United Kingdom's** National Criminal Intelligence Service is a multi-agency intelligence organisation, which gathers intelligence from a wide range of sources. Any intelligence raising potential tax implications would be reviewed by the Inland Revenue officer on secondment in the NCIS Economic

Crimes Unit and, if significant potential tax implications within the scope of the Inland Revenue Special Compliance Office's responsibilities are identified, handled in the same way as intelligence from suspicious transaction reports. HM Customs and Excise's investigators have access to the Police National Computer (PNC) system through the links with their own intelligence record system (CEDRIC). Information beyond that held on PNC would be requested through NCIS. NCIS have access to CEDRIC information relating to drugs cases.

In the **United States**, the types of information include so-called "pattern and trend" information (which law enforcement agencies typically compile to determine likely activity patterns and preferred methods of operation of financial criminals).

C. Please describe briefly the confidentiality provisions which may restrict the disclosure of this type of information.

Disclosure of this type of information may be restricted in cases where disclosure might be prejudicial to other agencies' own investigations, by regulations on legal professional privilege, by the fact that the material is strictly secret (e.g. if the material is sensitive information in a strategic report) or permission is denied by those responsible for the intelligence.

In **Australia**, disclosure of this information to the Australian tax authorities would not generally be precluded by privacy principles or other confidentiality provisions. However, disclosure may be precluded in circumstances where disclosure might be prejudicial to other agencies' own investigations.

In **Belgium** and **Luxembourg**, the annual reports are, as mentioned before, public.

In **Denmark**, the disclosure of this information is governed by section 28 of the Danish Public Administration Act. See Paragraph II, section G.

In **Japan** the confidentiality regulation derives from the duty to protect privileged information based on the provisions of the National Public Servant Law.

In the **Netherlands**, the privacy of persons and reporting institutions is safeguarded by the Act on the disclosure of unusual transactions. This act prohibits the persons and institutions who have a task under this law, to make further or other use of any data or information supplied or received in accordance with the act or to disclose such data or information for any purpose other than what is required by the performance of his duties or by the act.

In **New Zealand**, the only information, which the Inland Revenue Department cannot access, is information, which is governed by legal professional privilege. However, this does not include details of financial transactions.

In **Sweden**, if there is sensitive information in a strategic report or modus operandi, the Swedish Financial unit has the possibility to classify the material as strictly secret.

In **Switzerland**, Article 110 of the "Loi sur l'Impôt fédéral direct" requires the persons in charge of the application of the Act and those with whom they collaborate to keep secret all facts they get knowledge of in the course of their duties as well as the discussions of the authorities and must refuse consultation of fiscal files to third parties. Information may be obtained only in cases where the federal law provides an explicit legal basis for the disclosure.

In the **United Kingdom**, permission of those responsible for the intelligence (e.g. National Criminal Intelligence Service) would be sought before disclosure to Inland Revenue. At HM Customs and Excise

information is kept in a secure system able to be accessed through designated secure CEDRIC terminals by designated users where each enquiry is logged and can be checked.

In the **United States**, these types of criminal intelligence are generally available to the IRS only for purposes of investigating tax related crimes.

V. Access to Information Gathered in the Context of a Specific Investigation

A. *Please identify the governmental bodies or agencies with principal responsibility for the investigation of potential money laundering offences and briefly describe their roles in money laundering investigations.*

In **Austria, Denmark, France, Germany, Italy, Japan, the Netherlands, Norway, Poland, Spain, the Slovak Republic, Sweden, Switzerland, the United Kingdom, and the United States** there is a shared responsibility between governmental bodies for the investigation. In ten Member countries that responded to the questionnaire, there is a governmental body or agency, which is principally responsible for the investigation.

In	the responsible authority is
Australia	the Australian Federal Police
Belgium	l'Office Central de lutte contre la delinquance économique et financière organisé
Canada	The Royal Canadian Mounted Police
Czech Republic	Agency for disclosure of corruption and serious economic criminal activity part of the Police of the Czech Republic
Finland	the Money Clearing House
France	(no answer to this question)
Ireland	GBFI
Luxembourg	la Section criminalité organisée du Service de police judiciaire sous le Service Anti-Blanchiment auprès du Parquet du tribunal d'arrondissement Luxembourg
New Zealand	the New Zealand Police, Serious Fraud Office
Portugal	the Ministério Público through the Judiciary police

In **Australia**, the AFP are the principal investigative arm of the Commonwealth providing policing throughout Australia in relation to the detection and prevention of crime. The NCA also performs an active role in the investigation of money laundering, particularly in the co-ordination of multi-agency task forces drawn together for investigative purposes.

In **Belgium**, the OCDEFO is a police service that is in charge of combating all economic, financial or serious fiscal infringement related to organised crime. This includes money laundering, the crime of insider dealing, abuse of public money, financial swindle, and serious fiscal infringements where complicated schemes are used. The OCDEFO is a central office, which works in the Commisariat général de la Police under the control of a judicial official appointed by the General Committee of Public Prosecutors.

In **Canada**, the Royal Canadian Mounted Police (RCMP) is the lead law enforcement agency responsible for the investigation of money laundering offences, however, all police services across Canada share this

mandate. Under the leadership of the RCMP, 13 Integrated Proceeds of Crimes (IPOC) Units currently exist across Canada. These units are dedicated solely to targeting proceeds of crime, including money laundering. They represent a collaborative effort between the RCMP, local police services, forensic accountants, the Department of Justice and Revenue Canada. However, only the police representatives have peace officer status.

In the **Czech Republic**, besides the Financial Analytical Unit, which is a component of the Ministry of Finance, there is a special agency for disclosure of corruption and serious economic criminal activity. This agency, which is a component of the Police of the Czech Republic, is responsible for investigation of potential money laundering crimes.

In **Denmark**, money laundering offences are normally investigated in the 54 police districts. Some of the cases are investigated by the Public Prosecutor for Serious Economic Crime who has an attached police force or by the Money Laundering Secretariat (which is placed under this prosecutor).

In **France**, the authorities engaged in combatting against money laundering are TRACFIN, the Judicial Authorities and the Judicial Police.

In **Germany**, while the Federal Banking Supervisory Office and the Federal Insurance Supervisory Office are mandated to ensure that the provisions of the Money Laundering Act are implemented in the banking, insurance and financial services industries, they have no powers of conducting investigations into criminal offences. The investigation of possible money laundering offences lies in principle in the sphere of responsibility of the police services of the Länder and the Federation, the customs investigation services and the public prosecutor's offices. The location and the factual content will determine which authority investigates a specific case.

In **Italy** a special authority in the field of money laundering offences is attributed to Direzione Investigativa Antimafia – DIA – (Antimafia Investigative Directorate) and to Nuclea Speciale di Polizia Valutaria (Special Monetary Police Unit) of Guardia di Finanza. It is to be underlined that Guardia di Finanza is a military corps under the Minister of Finance, having a special competence in tax and economic field. The Nuclea Speciale di Polizia Valutaria carries out monetary police tasks differing from the ones of tax nature usually carried out by the Guardia di Finanza, mainly in the field of assessment, thus supporting the activity of the Tax Administration. As a consequence, the information collected on suspicious transactions by the Special Monetary Police cannot be used for tax purposes (not even by Guardia di Finanza itself).

In **Japan**, the public prosecutor, a public prosecutor's assistant officer, a judicial police official, a customs officer, and an official of the Securities and Exchange Surveillance Commission, are responsible for the investigation of potential money laundering offences.

In **Luxembourg**, the investigation of money laundering offences is conducted by the Section criminalité organisée du Service de police judiciaire under the responsibility of the Service Anti Blanchement.

In **Norway**, the police/prosecuting authority is investigating money laundering offences.

In **Poland**, the competent bodies responsible for carrying out an investigation in the case of money laundering offences are prosecutors, who can assign the conduct of such an investigation to the police.

In **Portugal**, the governmental body responsible for the investigation is the Ministério Público through the Judiciary police. At the Judiciary police there exists a department mainly devoted to combating corruption and economic and financial fraud (Direcção central para o combate à Corrupção, fraude e infracções

Económicas e Financeiras) both at national and international levels. This department collects information and asks for inquiries, inspection and other measures of financial crime or an act of corruption.

In **Spain**, the governmental bodies with responsibility for the investigation of potential laundering offences are, apart from the SEPBLAC, the investigative units of the Security Forces (Fuerzas y Cuerpos de Seguridad, FSC) with the following qualifications. Both at the level of the national territory as a whole and at the level of its administrative subdivisions, the FCS have at their disposal special units of Judiciary Police devoted to the investigation of those crimes. In particular, at the national level, the Civil Guard (Guardia Civil, CG) and the National Police Corps (Cuerpo Nacional de Policia, CNP) have investigative units specialised in money laundering, whereas at the level of the Autonomous regions (Comunidades Autónomas) of Catalonia and the Basque Country, and along with the aforementioned CG and CNP their respective Autonomous Police also have investigative units to this effect.

In the **Slovak Republic**, the Bureau of Investigation of the Police Force, Prosecution, Courts and the Supreme Supervision Office are the authorities, which are responsible for investigation of all crime including investigation of the cases of legalisation of proceeds of crime in compliance with Art. 252 of the Criminal Code.

In **Sweden**, when a preliminary investigation is opened the information has to be handed over to an investigation department.

In **Switzerland**, the Bureau of Communication receives the information concerning suspicious transactions and sends it to the canton involved. The responsible authorities for the prosecution are the cantons. In the future, this criminal procedure will be centralised at the federal level.

Under present **United Kingdom** legislation, the only bodies with responsibility for investigating money laundering are the police, HM Customs and Excise, the Financial Services Authority and the Serious Fraud Office.

In the **United States**, the investigation of money laundering offences is not assigned to any particular law enforcement agency. Rather, responsibility is shared by a large number of agencies, depending upon the nature of the underlying predicate crime. For example, the Federal Bureau of Investigation (FBI) has responsibility for investigating a wide variety of money laundering offences, but other agencies, such as the Securities and Exchange Commission (SEC), the U.S. Customs Service, and the Immigration and Naturalization Service (INS) also investigate money laundering offences that relate to their areas of expertise.

1. *Are these anti-money laundering authorities permitted to provide (either as a spontaneous exchange or in response to a specific request) information to tax authorities pertaining to a possible tax related crime? If so, under what circumstances?*

Money laundering authorities can send information to tax authorities in **Canada, the Czech Republic, Denmark, Germany, Ireland, Japan, the Netherlands New Zealand, Poland, the United Kingdom** and the **United States**. They are not allowed to do so in **Austria, Finland, Spain** and **Sweden**. In **Belgium, France, Luxembourg and Portugal** this is only allowed through a certificate from a judicial authority. In **Switzerland**, it depends on the criminal law of the canton concerned and these laws may differ in the cantons.

In **Austria** the FIU may only pass on information concerning customs fraud and evasion of import and export duties; purely fiscal offences are specifically prohibited from being disclosed to the fiscal authorities.

In **Australia**, when required, the ATO participates with the Australia Federal Police, the National Crime Authority and other Commonwealth Agencies in relation to money laundering investigations but generally only when revenue is at risk.

In **Belgium**, the members of the OCDEFO are not allowed to send information gathered while fulfilling their duties, to the tax authorities. There is no direct exchange of information organised between the police and the fiscal authorities. Nevertheless, fiscal authorities may gather certain information through the judicial authorities. The Public Prosecutors at the courts are obliged to inform directly the Ministry of Finance of any information they get which might be an indication of fraud concerning direct or indirect taxes.

In **Canada**, the RCMP has the authority to investigate violations of all federal statutes. Revenue Canada may request and obtain access to documents seized and retained by the RCMP pursuant to a Criminal Code warrant as long as there are no explicit restrictions in the original detention order, obtained under section 490 of the Criminal Code, pertaining to 'persons who have an interest in what is detained' in other words, to persons who have a bonafide legal interest or a legal concern for the purpose of administration and enforcement of a statute (in this case, Revenue Canada). Furthermore, it should be noted that to have access to the seized documents does not necessarily include making copies of them. To make copies, an order under subsection 490(15) of the Criminal Code is necessary. There is no legal statutory restriction binding the ability of the police to allow Revenue Canada access to the seized documents. Indeed, the RCMP has full authority to investigate violations of federal law, which includes investigations of violations of Revenue Canada statutes. In summary, it must be shown that

- Revenue Canada is an interested party;
- There is a basis for the party's interest and
- access is required for the administration of a Revenue Canada statute.

In the **Czech Republic**, the Agency for disclosure of corruption and serious economic criminal activity is authorised to provide information pertaining to a potential tax related crime under the provision of the Administration of Taxes Act.

In **Denmark**, the Money Laundering Secretariat or the police district handling further investigation informs the tax authorities of the relevant facts. There are no guidelines since this exchange of relevant information between public authorities is a normal part of the co-operation between Danish authorities. This is the case regardless of whether the information is from an STR (Suspicious Transaction Report) or from other sources on which no special- restrictions are imposed.

In **Finland**, the anti-money laundering authorities are not allowed to inform the tax authorities, as information concerning a money laundering case may be disseminated only for combating money laundering.

In **France**, the judicial authorities and the judicial police are allowed to provide information obtained in the course of an investigation, to the tax authorities.

In **Germany**, once criminal proceedings have been instituted for a money laundering offence, the tax authorities must be informed of this and must be notified of the facts on which the proceedings are based. The tax authorities may make unrestricted use of such information both for taxation purposes and for criminal proceedings in tax fraud cases. Notwithstanding the reporting obligations under the Money Laundering Act, all courts and authorities are, in principle, obliged to notify the tax authorities if there are grounds to suspect tax fraud.

In **Ireland**, there is no specific legislative requirement, but information may be provided either spontaneously or on request.

In **Japan**, tax authorities do not have direct access to the information gathered by money-laundering authorities. However, the information can be provided indirectly to tax authorities via law enforcement authorities in the following case. Law enforcement authorities compare the interest of preventing unreasonable effect to the investigation or judicial proceedings which might be caused by the provision of the information to tax authorities on one hand, and the interest of providing the information for tax authorities on the other. When the latter interests are given priority, the information can be provided to tax authorities.

In **Luxembourg**, the Public Prosecutor may prosecute if it appears in the course of an investigation that a tax related crime is involved.

In the **Netherlands**, the Public Prosecutors' Office provides guidance to the investigators of the police or the Tax Information and Investigation Office (FIOD) which is part of the Tax Administration.

In **New Zealand**, the tax authorities will receive this information under Section 17 of the tax administration Act 1994.

In **Poland**, the prosecutor may transfer information to the competent tax authorities if in the course of investigation the prosecutor considers that the information obtained may be useful for tax purposes.

In **Portugal**, access to information related to tax crimes is only possible through a certificate from a judicial authority (Ministério Público) drawn out from the judicial inquiry into a money laundering crime. The information obtained can only be used to pursue tax crimes and to enforce tax assessments.

In **Spain**, the SEPBLAC takes care of streamlining and analysing the information provided by the persons/entities obliged to furnish it. If, after analysing it, signs of money laundering can be detected, preliminary proceedings start. Depending on the seriousness of the potential irregularity detected, the investigation follows either a purely administrative course of action or, if indications of a crime are apparent, a judicial course of action. The investigation can be carried out either by the police unit attached to the SEPBLAC or by any other specialised unit belonging to the FCS, the decision being made on the basis of criteria fixed by the SEPBLAC.

In the **Slovak Republic**, in March 1999 an Agreement was signed between the Board of the Police Force, Central Tax Directorate and Customs Directorate on mutual assistance

In **Sweden**, the Swedish Financial Unit has the main responsibility for gathering and analysing relevant information and detecting money laundering. When a preliminary investigation is opened the information has to be handed over to an investigation department and the Swedish Financial Unit does not take active part in the investigation.

In **Switzerland**, there is no such authority at the federal level. The criminal law procedures concerned may differ in the cantons.

In the **United Kingdom**, the National Criminal Intelligence Service may pass on information. NCIS acts as the conduit to the Inland Revenue and HM Customs and Excise for any such reports from the police, FSA and SFO. HMCE and IR share information under internal arrangements.

In general, in the **United States**, case-specific information is shared among law enforcement agencies (including the IRS's Criminal Investigation Division) through multi-agency task forces and other

inter-agency co-ordination groups. Law enforcement agencies generally share case-specific information according to their own internal policies (i.e., they are not required to share information with other agencies), but the inter-agency process is generally characterised by a significant amount of co-operation with respect to information sharing. In addition, law enforcement agencies often conduct joint investigations of possible financial crimes, and the IRS's Criminal Investigation Division is a regular participant in such joint investigations.

2. *Are tax authorities permitted to participate in money laundering investigations that may also involve tax-related crimes? If so, under what circumstances? Is there a specific legal basis for such participation?*

In principle joint investigations are possible in **Australia, Canada, the Czech Republic, Denmark, Germany, Japan, the Netherlands, Portugal, Spain, the Slovak Republic, Sweden the United Kingdom**, and the **United States**. In **Belgium, Finland, France, Luxembourg, New Zealand, Poland** and **Switzerland** these joint investigations are not possible.

In **Australia**, the Commissioner's statutory authority to administer the various taxing statutes provides sufficient legal basis for him to participate with other agencies in the discharge of his revenue collection duties. In more serious matters, it is also open to the Commissioner to refer taxation matters to the NCA, the AFP or the Director of Public Prosecution for further investigation and prosecution under the Crimes Act 1914.

In **Belgium**, a new regulation is on its way, which provides for the possibility of secondment of fiscal civil servants at the OCDEFO in order to improve the efficiency of this body in cases of fiscal fraud. During their secondment, these fiscal civil servants are not allowed to communicate any information they obtain while fulfilling their duties. Neither are they allowed to take up any cases in which they were involved at the tax administration.

In **Canada**, tax authorities are permitted to assist in money laundering investigations by lending their expertise to police officers in identifying developing relevant documentation, e.g., developing net worth information for the purpose of pursuing a "criminal proceeds of crime investigation", amongst other things. The assistance of tax authorities intensifies and enhances the effectiveness of enforcement efforts by IPOC units by creating a co-ordinated approach to targeting those profiting from crime and depriving such individuals of criminally obtained assets, thereby disrupting organised crime.

In the **Czech Republic**, the tax authorities participate in money laundering investigations that may involve tax avoidance.

In **Finland**, a joint investigation is not possible because information on money laundering cases may only be used for combating money laundering.

In **France**, information obtained by TRACFIN may only be used for combating money laundering and may not be used for other purposes.

In **Denmark**, if the expertise of the tax authorities is needed or the participation will result in a shorter period of investigation, the tax authorities participate in the investigation. In other cases, they are kept informed. This co-operation has no specific legal basis.

In **Germany**, joint action between law enforcement and tax authorities (tax investigation agencies) is conceivable in specific instances; it should be noted, however, that as a rule the tax authorities are only

informed when criminal proceedings in respect of a money laundering offence have already been instituted.

In **Ireland**, an agency has been established in 1996, called the Criminal Assets Bureau (CAB), to co-ordinate the actions of the Tax Authorities, the Social Welfare authorities and the Garda Síochána (Irish Police) in relation to the taking of measures to deprive criminals of the benefit of proceeds of crime generally, but in particular in relation to drug trafficking. The CAB is staffed by both Tax officials, Social Welfare officials and Police officers. Money laundering investigations concerned with individuals involved in organised crime would usually come within the ambit of the CAB who would use the tax code and other non-tax legislation to achieve their objective of depriving the criminals of their assets.

In **Japan**, tax authorities are permitted to participate in money laundering investigations that may also involve tax related crimes as an independent status only for a tax purpose.

In **Luxembourg**, there is no legal basis for joint activities and the tax authorities do not participate in investigations on money laundering.

In the **Netherlands**, the Tax Information and Investigation Office (FIOD), as part of the Tax Administration, does participate in money laundering investigations that (also) involve tax related crimes. The law enforcement authorities are in principle permitted to give any information regarding tax-related crimes to the FIOD, but not to the general tax authorities. In this respect, it should be noted that close co-operation exists between the police and the Tax information and Investigation Service (FIOD).

In **New Zealand**, the Inland Revenue does not participate in joint investigations with other agencies due to the secrecy provisions. However, it may conduct an independent tax investigation.

In **Poland**, tax authorities are not permitted to participate in anti-money laundering investigations.

In **Portugal**, a joint investigation is possible if it is requested by the Ministério Público, e.g. if a fiscal investigation is necessary.

In **Spain**, if, in the process of the money laundering investigation, the FCS would get to know about a possible tax crime, the relevant facts would be communicated to the Judiciary Authority supervising the money laundering investigation, as well as to those units of the FCS specialised in investigating tax crimes.

In the **Slovak Republic**, under the Law on Police Force No. 171/1993, par. 29a, the tax authorities are permitted to participate in money laundering investigations that may also involve tax related crimes and they may, together with the Police Force enter the premises determined for undertaking and co-operate with the Police Force.

In **Sweden**, when a preliminary investigation has been opened the prosecutor can demand assistance from the tax authorities according to the Swedish Code of Judicial Procedure.

In **Switzerland**, there is no legal basis for a joint investigation.

The various Crown prosecuting authorities in the **United Kingdom** have entered into a convention governing the work of prosecutions in which more than one agency has an interest. This convention would allow Inland Revenue officials to be invited by other investigating authorities (e.g. the police) to participate in money laundering investigations involving a tax crime, but to date no such cases have been undertaken. In the event of a joint investigation, any intelligence gathered by Inland Revenue officials other than under the Inland Revenue's own powers could not be used by the Inland Revenue directly as evidence. The participating Inland Revenue officials would also remain bound by the generally applicable statutory

prohibition on disclosure of information obtained or held in the exercise of their tax functions. The effect of this is that they could not contribute such information to a money-laundering investigation unless this was necessary in order to take forward their own tax investigations. HM Customs and Excise conducts money laundering investigations and prosecutions in its capacity as an investigating and prosecuting authority.

In the **United States**, although there is no specific legal basis for such participation, the long-standing practice in the law enforcement community has been to conduct joint investigations when appropriate.

B. *Please describe briefly the confidentiality provisions, under either domestic law or international agreements, which may restrict the disclosure of information gathered in the context of a specific money laundering investigation.*

If the information gathered in the context of a specific money laundering investigation could be shared with tax authorities, in general this information may only be shared as far as taxes are concerned.

In **Australia**, where other agencies participate with the ATO in the investigation of a taxation offence, specific provisions governing secrecy prevail and flow with the information supplied to the participating agencies. Where information is passed to the NCA for a tax related investigation that it is pursuing, obligations that arise under the secrecy provisions still apply, but tax information may be passed to other agency task force members by virtue of their status as National Crime Authority task force members. Information received by the ATO under International Agreements is generally received on the basis that it cannot be disseminated elsewhere. However, if necessary, consent could be sought from the international source.

In **Canada**, tax authorities generally are not permitted to disclose information obtained for tax purposes (i.e. section 241 of the income Tax Act) for non-tax purposes. Information may be shared with the police only under the following circumstances:

- (a) where a criminal information (charge) has been laid (paragraph 241(3)(a) of the Income Tax Act), and the information requested is relevant to the accused person, or
- (b) where the police acquire a court order (section 462.48) under the Criminal Code for access to tax information in relation to designated drug offences only.

In the **Czech Republic**, there is a particular provision relating to confidentiality in the Act of the Police of the Czech Republic. Under this provision, the Agency for disclosure of corruption and serious economic criminal activity is entitled to keep security of its agent who is/was connected in the investigation of any criminal activity. In this case, some restrictions of providing information can arise.

In **Denmark**, the exchange of information with non-law enforcement authorities is carried out in accordance with the principles of section 28 of the Danish Public Administration Act. See the Danish answer to paragraph II, section G.

In **Germany**, the tax authorities may use the information transmitted by the law enforcement authorities (cf. II. F) for taxation purposes and in criminal proceedings for tax fraud. For the rest, in ratifying the Convention of 8 November 1990 on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime, Germany refrained from making a declaration pursuant to Article 32 (2). Under this provision, the requested Party may stipulate that information will be provided only on condition that such information or evidence is not used or transmitted without its consent by the authorities of the requesting party in investigations or proceedings other than those specified in the request. However, this merely implies that there are no general reservations against the requesting State using the information supplied for other

criminal prosecution purposes. Any use for other than criminal prosecution purposes will require the prior consent of the German authorities. The same applies with respect to information exchanged upon request if no bilateral or multilateral agreement exists.

In **Ireland**, to the extent that information of the CAB comes into the hands of Irish tax authorities, the normal domestic confidentiality rules concerning taxpayer information would apply. Such information could be exchanged in accordance with the exchange of information provisions in a double taxation treaty.

In **Japan**, the confidentiality regulation derives from the duty to protect privileged information based on the provisions of National Public Servant Law, the Local Public Servant Law and the Code of Criminal Procedure.

In the **Netherlands**, in the different areas of the governmental responsibilities, special legislation about privacy is applicable; e.g. the law on judicial information regulates:

- the kind of information that has to be collected for judicial reasons,
- for what periods of time that information is stored, and
- under which conditions the information can be disclosed.

The act on the police registers regulates how the police forces have to store information and under which conditions the information can be made available to other law enforcement agencies in the Netherlands or abroad. The law on police registers is also applicable to the information exchange of the Netherlands Office for the disclosure of unusual transactions (MOT).

In **New Zealand**, there are no confidentiality provisions, which apply to other enforcement agencies when providing information to the Inland Revenue Department. However, IRD does not provide any information to other enforcement agencies. International information is obtained through the Double Taxation Agreements, which the Inland Revenue Department has with twenty-five countries. However, to obtain international information through a New Zealand enforcement agency, once again there are no confidentiality provisions. The information must be made available on request by the Inland Revenue Department although the agency may specify that the information may be used for reference only and not form part of any Court proceedings.

In **Poland**, information obtained in the course of investigation may constitute a state official secrecy, bank secrecy, fiscal and professional secrecy.

Spain (see answers in paragraphs II, section G and III section F). Information of a strictly police nature can be disclosed to the appropriate authorities, with the logical confidentiality limitations. However, if the piece of information or the documents at issue are subject to procedural secret, their possible disclosure is conditioned upon the authorisation of the appropriate Judge. As for disclosing information to those units of the FCS specialised in investigating tax crimes, that could be done using the internal channels previously established for exchange of information. With reference to possible exchanges with other countries, Police Corps of police information gathered in the context of a specific investigation on money laundering, the rule is to stick to the guidelines laid down in the International Agreements, taking into account the reciprocity principle.

In the **Slovak Republic**, the confidentiality provisions under domestic law which restrict the disclosure of information gathered in the context of a specific money laundering investigation are:

1. Article 2 of the Decree of the Ministry of Interior No. 181/1997(Coll. of Laws) on the Suspicious Banking operations;
2. Article 38, par 3) of the Banking Act No. 21/1992 (as amended);
3. Criminal Law No. 140/1961 Coll. of Laws, as amended - Article 122 (Menacing the business secrecy, banking secrecy or tax secrecy) and Article 178 (An unauthorised disclosure of personal information)

The **Swedish** secrecy law has to be observed even where there are international agreements. Concerning exchange of information with other countries; the Swedish Financial Unit has to apply the international law of legal aid.

In the **United Kingdom**, the National Criminal Intelligence Service may pass intelligence to other competent bodies only for the purpose of criminal investigations within their province. In the case of any such information passed to the Inland Revenue, the confidentiality of the intelligence information in the hands of Inland Revenue officials is protected under the statutory prohibition on disclosure of information obtained or held in the exercise of their tax functions. This is provided for under Section 182 of the Finance Act 1989.

In the **United States**, as a matter of practice among law enforcement agencies, case-specific information is available only for the purpose of crimes. Accordingly, the IRS would have access to such information only in the context of investigating tax-related crimes.

VI. Exchange of Information with Tax Treaty Partners

- A.** *If the tax authorities have access to the information described in Parts I and/or II, are there any restrictions that would apply to providing such information to a treaty partner (assuming the requirements of Article 26 or the relevant exchange of information instrument are otherwise met)? If so, please describe the restriction and its legal basis.*

In **Austria** (apart from customs fraud and evasion of import and export duties) **the Czech Republic, Finland, France, Ireland, Italy, Luxembourg, and Poland**, fiscal authorities have no access to the information described in Parts I and II, so this information cannot be exchanged under tax treaties. In the **Slovak Republic**, if this information is available to the tax authorities, it may not be exchanged under tax treaties. In the other countries this information, if available, may be exchanged, but sometimes only after consultation with the money laundering authorities.

Since in **Austria**, under the current legislation only customs duties and similar duties would be affected by disclosure of money laundering information, Article 26 provisions of tax treaties would not be applicable to this information.

In **Australia**, agreements based on the OECD Model Tax Convention Exchange of Information Article 26 containing the provision that the requested state is not obliged to supply information where there is

- Lack of reciprocity (i.e. the requesting State could not legally or would not in practice obtain or supply similar information); or
- There is a risk of disclosure of business or professional secrets; or
- Cases where disclosure of information would be contrary to public policy.

The Australian Financial Transaction Reports Act provides that tax authorities are entitled to access to Financial Transaction Reports (FTR) information. Nevertheless, FTR information may be provided by AUSTRAC to a foreign country under certain conditions. Those conditions are that:

- The financial intelligence unit of a foreign country (if such a unit exists) must have signed a MOU with AUSTRAC, setting out the conditions under which financial intelligence in the form of FTR information may be provided to that foreign country.
- FTR information provided to the financial intelligence unit of a foreign country in accordance with an MOU described above may only be provided to assist the foreign country in the investigation of criminal matters. The FTR Act specifies that FTR information provided to a foreign country shall be in accordance with the relevant provisions of the *Mutual Assistance in Criminal Matters Act, 1987*.

Foreign financial intelligence units that AUSTRAC has established a Memorandum of Understanding with, are: TracFin (France); FinCEN (United States); CTF/CITF (Belgium); NCIS (United Kingdom); The Danish Money Laundering Secretariat (Denmark); and The New Zealand Police Financial Intelligence Unit.

In **Belgium**, if the fiscal authorities are in the possession of information that they think would help to make a correct assessment of taxes on income or capital, they may exchange that information with treaty partners. Belgium notes that the same is true for indirect taxes under a European Union directive. The conditions for the information sent to foreign fiscal administrations are the same as those for information received by the Belgian fiscal administration.

In **Canada**, there are no restrictions on the type of information that can be exchanged other than those established by the tax treaties.

In **Denmark**, there are no general restrictions but, based on specific problems in a case, there might be cases where the information is not passed on at the early stage to the Danish tax authorities or is passed on with restrictions concerning further use (in Denmark or abroad) for the time being. Such a decision will normally relate to a very difficult or sensitive investigation (e.g. in a period with wire tapping).

In **Germany**, under the exchange of information clauses in double taxation agreements, the competent authority exchange the information required for the application of the agreement or the domestic law of the Contracting States relating to the taxes covered by the agreement. The information may be disclosed by the other Contracting State only to persons or authorities (including courts) concerned with the assessment, collection, enforcement, prosecution or decision on appeals in respect of taxes which are the subject of the agreement. Such persons or authorities may use the information only for those purposes. The same applies to the exchange of information between tax authorities of the Member States of the EU (Directive 77/799/EEG of 19 December 1977). On this basis, the tax authorities may make information obtained from anti-money laundering authorities available to foreign tax authorities.

In **Italy**, Tax Authorities have no access to information on suspicious transactions. As to the cross-border movements over 20 million Lire, it seems that there will not be any obstacle to the exchange of information between the Italian Ministry of Finance and the Tax Authority of the other countries, once the procedures allowing the Ministry of finance to collect regularly such data are in operation.

In **Japan**, the information obtained through suspicious transaction reports can be provided to a treaty partner to the extent that tax treaties allow.

In the **Netherlands**, with the consent of the Public Prosecutor, after the criminal case has been concluded, the information in possession of the money laundering authority can be passed on to the tax authorities. If this would be relevant to the treaty partner, this information could be provided spontaneously, assuming that the underlying treaty permits the exchange of information for the application of the domestic laws of the treaty partner, that reciprocity is foreseen, and that the information concerns taxes mentioned in the treaty.

In **New Zealand**, the Inland Revenue Department may withhold information under the following circumstances:

- i. Disclose information, which is subject to an obligation of confidence and would prejudice the supply of information from that source in the future.
- ii. Disclose the name of the person who supplied the information where there was a promise of confidentiality.
- iii. Endanger the safety of any person.
- iv. Prejudice any negotiations.
- v. Constitute contempt of Court or Parliament.
- vi. Prejudice the economic interests of New Zealand.

The above circumstances and further non disclosure provisions are covered, under the Official Information Act, Privacy Act and Part IV of the Tax Administration Act 1994.

In **Poland**, there are no restrictions on providing such information to treaty partners.

In so far as the **Spanish** tax authorities have access to this information, it is possible in principle to pass it on (as the case may be) to a treaty partner's tax authorities, provided that the treaty permits the exchange of information. The information thus exchanged shall be dealt with by the other State with due regard to the limitations contained in the relevant articles of the bilateral treaty, which usually follow the pattern established in Article 26 of the OECD Model Convention.

The principle laid down in the **Swedish** secrecy law is that secret information cannot be passed on to foreign agencies or organisations. However, there are two important exceptions to this rule. 1) Information can be supplied when this is provided for in a law or a government regulation. 2) Information can also be supplied if, in a similar situation, it could have been passed on to a Swedish agency and disclosure is apparently in line with Sweden's interests. The exception under 1) above means that information can be passed on to a treaty partner to the extent that the treaty provides for exchange of information.

In the **United Kingdom**, the MOU between Inland Revenue and the National Criminal Intelligence Service contains an undertaking by the Inland Revenue that information will not be passed on without the express consent of NCIS. The Head of the Economic Crime Unit may authorise disclosure to a foreign FIU, which may include Revenue staff i.e. AUSTRAC.

In the **United States**, in general, all of the information provided by anti-money laundering authorities to other law enforcement agencies (including the IRS) may be restricted from further disclosure by the so-called "Third Agency Rule." This rule, which is designed to protect those involved in law enforcement (such as undercover agents or informants) from possible injury or death if such information was disclosed to the public or the target of an investigation, prohibits a law enforcement agency from passing on information provided by another agency to any third party (including a treaty partner) without the permission of the agency that provided the information. This rule is not codified, but it is the long-standing and nearly universal practice among law enforcement agencies in the United States. Accordingly, if the IRS received a request from a treaty partner concerning information that it has received

from another law enforcement agency the IRS would generally consult with that other agency regarding exchange of the information.

VII. Usefulness of Information

A. *For those countries that have some access to information gathered by anti-money laundering authorities, please indicate:*

I. *What is your experience regarding co-operation with anti-money laundering authorities?*

In the countries where tax authorities have full access to the suspicious transaction reports (**Australia**, the **United Kingdom** and the **United States**) the co-operation proved to be very successful. In the countries where access is restricted, the co-operation was considered very useful. The **Czech Republic**, **France**, **Finland**, **Ireland**, **Japan**, **Norway**, **Poland**, **Portugal**, **Sweden**, and **Switzerland** had no experiences on this matter to report.

In **Australia**, there has always been a strong level of co-operation between the ATO and AUSTRAC. The ATO has a national team of five officers who work closely with AUSTRAC officers in an endeavour to maximise the use of FTR information. Furthermore, in the interests of enhancing its relationship with Australia's major financial investigative agencies, AUSTRAC provides office accommodation to officers from the ATO, the NCA, the AFP and the ACS.

As indicated before, in **Belgium**, neither the CTIF nor the OCDEFO can exchange information with the fiscal authorities. This information can only be provided to the fiscal authorities through the judicial authorities. Although the judicial authorities transfer information to the fiscal administration, it is only very rarely that they send information originating from the CTIF. Nevertheless in the second half of 1998, the fiscal administration is provided, through the judicial authorities, with all the charges the CTIF has sent to the judicial authorities concerning international schemes to avoid indirect taxes. These charges do not only reveal violations of the indirect tax legislation but also of the income tax. It appeared that this information is very useful for the fiscal administration to counteract this type of fiscal fraud. The fiscal authorities have asked the judicial authorities to accelerate the information originating from the CTIF and to add some additional information like the origin and the destination of the money, so that the fiscal administration can react more promptly to these fraudulent schemes.

In 1972, Revenue **Canada** created the Special Enforcement Program (SEP) within the Investigations Directorate in response to the seriousness of organised crime and the negative impact proceeds of crime can have on our society. SEP has been very successful in removing the unreported wealth of persons accumulated from proceeds of crime by enforcing the Income Tax Act. Recently, our investigators have co-located with the RCMP, other police forces, and other departments to address the problem of money laundering, proceeds of crime, organised crime and tax evasion in Integrated Proceed of Crime (IPOC) units. This co-location should lead to an increased cross departmental involvement in investigations and an increased sharing of information on a timely basis. Currently, Canadian banks have the option to voluntarily report suspicious transactions to the police, however, this has not led to many reports, and if a report is received, there is usually a confidentiality agreement which excludes the disclosure of the information to Revenue Canada for tax issues. The recent introduction of Bill C-81, the new Proceeds of Crime (Money Laundering) Act, will require the mandatory reporting of suspicious transactions by financial institutions which could lead to the disclosure of tombstone information to Revenue Canada when tax evasion and money laundering are both suspected. When the police collect information through their own investigations there is co-operation with Revenue Canada investigators, however, information is usually only forwarded to Revenue Canada if and when the police believe they will not be able to restrain

or seize assets under the Criminal Code. Thus, generally in these cases, Revenue Canada will be utilised as a last resort in order to deprive the criminal of his assets.

The **Danish** tax authorities have a positive co-operation with the Money Laundering Secretariat, which is carried out in accordance with the rules described under II, IV and V. With a view to intensifying the co-operation on anti-money laundering a Co-ordination Committee on the Control of Economic Crime against the State, etc. has proposed in a recent report that the Central Customs and Tax Administration - in co-operation with the anti-money laundering authorities - should arrange courses for the field staff of all the customs and tax administrations and the municipal tax administrations on the laundering of the proceeds of crime. These courses will be arranged as soon as possible.

In **Germany**, the obligation of the law enforcement authorities referred to under II. F, above, to notify the tax authorities once criminal proceedings have been instituted for a money laundering offence has been in force since 9 May 1998. Reports by the customs authorities also (cf. III. A) have been forthcoming only since 9 May 1998. Hence, it is not yet possible for Germany to make any meaningful statement with regard to experience from co-operation. However, some initial reports received from a few tax investigation offices are very positive. For example, tax fraud proceedings with money laundering implications have been instituted in 60 instances in the period from 9 May 1998 to 31 December. 1998, some of them attributable to information received from the law enforcement authorities. Reports also indicate that in many cases information provided by credit institutions (see II.C.) ultimately leads to a tax fraud case rather than a money laundering case.

Luxembourg reported that although there is no exchange of information between the anti-money laundering authorities and the fiscal authorities, in the past the Service Anti Blanchement has exchanged information with foreign anti-money laundering authorities. It appeared that in some cases this information is only used by the fiscal authorities for a fiscal investigation. In this way the principle of the Luxembourg anti-money laundering legislation is disregarded. Since this occurred, the co-operation with the foreign anti-money laundering authorities has become more difficult, and it has also affected the intention of the concerned authorities to co-operate.

In the **Netherlands**, the Tax information and Investigation Service (FIOD) works directly together with the anti-money laundering authorities like the MOT, the Public Prosecutor and the Police. All crime related information is available for the FIOD. The information is most useful for the investigation of VAT fraud and other tax related crimes.

In **New Zealand**, there have been no problems in accessing information from the anti-money laundering authority. The important thing for the authority is to realise that money laundering is not only a criminal offence but also has serious tax implications. Further, in certain cases, it is difficult to prove a criminal offence due to the stringent evidential requirements and international laws that govern money laundering offences. In such instances, tax authorities can play a major role in bringing offenders to justice and stripping them of their ill-gotten assets.

The co-operation of Ministry of Finance of the Slovak Republic, Central Tax Directorate, Customs Directorate with anti-money laundering authorities is good, there are no problems so far.

In the **United Kingdom**, Inland Revenue's experience regarding access to information from suspicious transaction reports has been excellent. Since August 1998, the Head of the Economic Crime Unit has authorised 175 intelligence reports to SCO, of which 15 have been allocated within SCO for investigation by operational groups. In addition, SCO has made 85 requests for searches of the NCIS database, of which 31 have produced a response adding significant value to SCO's investigations. More widely, SCO has been able to benefit from intelligence from other law enforcement teams within NCIS as well as drawing

on the wide expertise within NCIS in tackling fraud. Benefits to NCIS have included the disruption of crime through IR prosecutions in appropriate cases as well as the ability to draw on the expertise of an experienced financial investigator through the secondment of an IR investigator. HM Customs and Excise conduct such investigations and resolve difficulties through the normal management liaison mechanisms.

Within the **United States**, co-operation between the different agencies that have jurisdiction over anti-money laundering efforts has been good. Each agency maintains a unique system of storing and cataloguing information useful in both anti-money laundering and tax investigations. As noted above, such agencies often allow sharing of the same computer databases, thus making it easier to obtain and exchange information. Internationally, the United States has had good experiences relating to exchanges of information with FIUs. Through FinCEN, the United States has requested and received financial information from FIUs located overseas that was useful in both anti-money laundering and tax-related investigations. Domestically, financial privacy laws (designed to protect the financial privacy of citizens) limit access to information gathered by anti-money laundering authorities. These disclosure laws sometimes prevent agencies from disseminating information, which was gathered for anti-money laundering or criminal tax purposes, to civil tax authorities. For example, the Bank Secrecy Act prevents the use of Suspicious Activity Reports for civil tax compliance.

2. *What difficulties have you encountered?*

Difficulties encountered vary from how to cope with the enormous inflow of information to how to stimulate the flow of information as money laundering authorities may not be aware of what information might be relevant to the tax authorities.

In **Australia**, difficulties that have been encountered have mainly related to the integrity of the data received by AUSTRAC and therefore its value to the ATO. That is, whilst AUSTRAC receives the great bulk of its financial transaction reports electronically, the integrity of the information contained in the reports is generally dependent on the accuracy and completeness of the information provided by the cash dealers. This is of particular importance in establishing the correct identity of the transacting parties. Nevertheless, AUSTRAC has in place a range of automated and manual systems and programs for improving the integrity of the data it receives from cash dealers.

Canada had no specific difficulties to report.

In **Germany**, in the brief period since these reporting obligations were introduced, some problems have of course been encountered, for example with regard to the scope of the reporting obligations or the extent to which tax authorities have access to the results of investigations by the law enforcement authorities.

In the **Slovak Republic** a co-operation with foreigner's police would be welcomed; in certain cases we have difficulties with the identification of a long-term stay of foreigners in the Slovak Republic

A major difficulty encountered in the **United Kingdom** before the secondment of an IR official into NCIS was the poor flow of information to the Inland Revenue due to the relative unfamiliarity of the money laundering authority with the potential tax implications of the intelligence at their disposal. An ongoing problem is the lack of information from money laundering authorities outside the UK, which do not recognise tax evasion as a crime, or have not made tax crimes offences for the purposes of their money-laundering regulations. Even where tax crimes are included for anti-money laundering purposes, there are differing standards and attitudes on the part of government agencies and institutions concerned which can affect the flow of tax-related information. There is still a low level of appreciation and acceptance on the part of UK financial institutions, solicitors and accountants that potential tax crimes are on all fours with other matters covered by the anti-money laundering regulations. (Of the total disclosures to the Economic Crime Unit in 1998, disclosures from solicitors and accountants represented only 1.9% and 0.7%

respectively.) Government powers to enforce compliance with the anti-money laundering need to be applied sensitively and in a way which fosters a co-operative approach. There is also the problem that restrictions on the disclosure of information currently received by Inland Revenue mean that this information cannot be used directly as evidence.

Internationally, the **United States**, authorities have experienced difficulties when information gathered pursuant to an MLAT request relating to a money laundering investigation cannot be used for a tax investigation.

3. *What types of information obtained from anti-money laundering authorities have proven to be most useful?*

All types of information have proven to be useful. Even publicly available pattern and trends information on money laundering has proven to be useful to tackle international fraud schemes on indirect taxes.

In **Australia**, all types of FTR information obtained by the ATO have proven to be useful. Whilst the major results achieved by the ATO from using FTR information have generally been attributed to the direct use of Suspect Transaction Reports and International Funds Transfer Instructions, these reports, when combined with reports of International Currency Transfers and Significant Cash Transactions have also proven to be of substantial value to the ATO.

As in **Canada** Bill C-81 has not yet been passed into law, Revenue Canada receives most of the information regarding money laundering from the Police. In all cases the following has proven useful:

- Information which helps to identify the person being investigated such as:
 - First, Last and Middle Names
 - Social Insurance Number
 - Date of Birth
 - Current Address
 - Current Employer
 - Former Addresses (if recently relocated)
- Financial information, such as:
 - Sources of income
 - Amount of income
 - Spouses' and family members' sources and amounts of income
 - Any other available information which would assist investigators in determining whether the person is paying their fair share of tax
- Banking information. such as:
 - Bank account numbers
 - Bank addresses
 - Safety deposit box
 - Account balances
 - Deposit and withdrawal habits and amounts
 - Information regarding wire transfers (domestic and international)
 - Accounts with brokerage houses
 - Amounts and activity of accounts

- Information relating to assets and lifestyle in order to assess taxes owing, such as:

Specific assets and evaluations if available

Monthly expenditures (to determine required cashflow to maintain lifestyle)

Holiday and travel habits of person and family

Any other information which would assist the investigator in determining whether the person's reported income can maintain their lifestyle

- Any information that has come from analysis, or that has come from research which would assist investigators determine whether the person is paying their fair share of tax (i.e. recent lottery winnings, inheritance, etc.).

In **Denmark**, the information received from the money laundering authorities has in most cases been useful for the purpose of investigating tax-related crimes, including VAT crimes.

Ireland stated that documentary evidence (bank statements, title documents, share certificates, invoices, written instructions etc) to establish ownership of financial and other assets by the taxpayer concerned, with supporting depositions by key witnesses where necessary, might be useful.

In **New Zealand** the following information has proved to be most useful:

- i. The name, address, date of birth, and occupation (or, where appropriate, business) of each person conducting the financial transaction(s).
- ii. The name, address, date of birth, and occupation (or, where appropriate, business) of any person on whose behalf the transaction is conducted.
- iii. Where a facility with a financial institution is involved in the transaction, the type of facility, details of the person in whose name the facility is operated and names of the signatories to the facility.
- iv. Nature of the transaction.
- v. Amount of the transaction.
- vi. Type of currency involved.
- vii. Date of the transaction.
- viii. Details of any documentary evidence that may assist in establishing the identity of the person who conducted the transaction and the person on whose behalf the transaction was conducted.
- ix. Details of the person and the financial institution, which provided the transaction report.

In the **United Kingdom**, the Inland Revenue has received a wide range of useful information from the National Criminal Intelligence Service, ranging from instances of complete disclosure of how tax has been evaded through a transaction or scheme of transactions, to information on isolated transactions or assets in relation to which tax evasion has only been established after considerable further investigation. Specific types of intelligence received have included information on unknown bank accounts, property transactions, vehicles, cash dealings through bureaux de change or cheque cashing agencies, details of commissions or other regular payments, and foreign currency exchanges. HM Customs and Excise reported that resources do not permit a follow-up investigation of every suspicious transaction report received from NCIS. But the existence of the database provides the means of building a case once an investigation of an individual or organisation is commenced.

In the **United States**, information obtained from Currency Transaction Reports ("CTRs") and Suspicious Activity Reports ("SARs") has been most useful. The financial data and identifying information contained within these reports are useful in both money laundering and criminal tax investigations when it is directly tied to a subject or a critical witness. CTRs have also been useful in civil tax compliance.

B. *What types of information would be most useful for tax authorities to obtain from anti-money laundering authorities for purposes of investigating tax-related crimes? Please explain briefly why the information would be useful.*

In general, tax administrations would prefer to have better access to information gathered by anti-money laundering authorities. Some countries provided extensive lists of information that might be useful, whereas other countries just provided some examples.

In the light of the current legislation **Austria** thought this question not applicable, but remarked that from the tax administration's view, access to information from money laundering authorities would be desirable at least in cases of commercial tax fraud.

Australia and **New Zealand** referred to the report types listed above under paragraph VII, section a, question 3. **Australia** added that recent evidence of the use of this information can be found in the fact that the ATO has issued assessments for additional tax and penalties with a value of in excess of \$A 93 million in the last two years which can be directly attributed to the ATO's use of FTR information. Furthermore, the ATO has recently completed a study, which concludes that the additional indirect benefit of the use of FTR information is estimated to be in the vicinity of 40% of the direct results. **New Zealand** added that it is difficult to identify the type of information, which would be useful, apart from that listed above. However, the information required will vary for each case and will have to be identified on a case by case basis.

In **Canada**, the police will continue to pass the above noted information which is most useful onto Revenue Canada in certain cases. Also, it is proposed that the FTRACC would forward tombstone information to Revenue Canada when they suspect money laundering and tax evasion. What will be considered tombstone information has not yet been determined. However, it will likely include name, birth date, dollar value of the transaction(s), and account(s) number(s).

Denmark reported that the investigation of tax-related crimes could be improved if the anti-money laundering authorities were permitted to pass any information on money laundering to the tax authorities.

Germany will provide information on this subject once the reports from local authorities in that respect have been received.

In **Japan** the discussion is under way as to what information would be useful. One example would be the information relating to the transactions conducted by Japanese taxpayers which is provided to foreign anti-money laundering authorities

The **Netherlands** thought that useful information would be the source of the income, the buyers and suppliers of goods, who transported them, who is behind certain bank account numbers. If investments have been made, where and how was the money invested.

In **Norway**, tax avoidance and evasion are legal offences in Norway and these kinds of crimes are being investigated by the police/prosecuting authority and not by the tax authorities. However, the tax authorities believe that access to the suspicious transactions reports received by ØKOKRIM, will increase the efficiency of anti-money laundering actions in Norway. The tax authorities have substantial information on

taxpayers, which when effectively connected with reports on suspicious financial transactions, will improve the selection of taxpayers for tax audits. The idea has recently been presented to the Ministry of Finance.

Poland reported that information on transactions between capital and personal connected companies and on foreign transfers in virtue of export/import transactions would be most useful.

Portugal thought it not possible to identify the most useful information because it depends on the type of investigation. However, as the tax authorities in Portugal have only access to the information related to tax crimes through a certificate drawn out from the judicial inquiry into money laundering crime, it is necessary to specify the type of information needed for each investigation.

Spain reported that the present co-operation between the Tax Agency and the anti-money laundering authorities could be enhanced in the future, with a view to improving, for their mutual benefit, the knowledge of the available information on suspicious transactions. From the perspective of the Tax Agency, it would be most useful to have access to a regular flow of data or information concerning those transactions. Regarding that flow, rather than information related to potential fiscal crimes or to the other underlying crimes which could also entail a fiscal crime (given that in Spain, penal prosecution of all those crimes, corresponds to the judiciary: see paragraph V, section A), it should be a question of having access to that information which would allow the Agency to perform its specific task of the correct assessment of taxes in a more efficient way.

In the **Slovak Republic**, the most useful information for the tax authorities would be the information about foreign bank accounts and keeping this information confidential in accordance with the domestic law.

The **United Kingdom** thinks data base enquiries and informal assistance of overseas FIU's in confirming intelligence, would be useful. Specifically, types of information sought would include details of bank accounts in foreign jurisdictions, and the details of beneficial owners of foreign companies, trusts or other property.

The **United States** considers information obtained from Currency Transaction Reports and Suspicious Activity Reports most beneficial. In addition, as noted above, certain institutions are generally required to report transactions where over \$10,000 in cash is received from customers, and such information has proven very useful in tax-related investigations. Other information required to be reported by state, local and federal laws could also be useful in investigating tax-related crimes. Such information can help identify the ownership or control of a corporation or other assets, can help document an unusual accumulation of wealth or assets, and can be critical in tracing and identifying funds disbursed or received by an individual who is under investigation.