



810 Bank Secrecy Act & Anti-Money Laundering Issues for All Corporations

Bruce Baker

Executive Vice President & General Counsel
Illinois Bankers Association

Eileen Lyon

Senior Vice President and General Counsel
Far East National Bank

Brian L. Mannion

Senior Lead Counsel
Nationwide Mutual Insurance Company

Michael R. Nelson

Assistant General Counsel
JP Morgan

Faculty Biographies

Bruce Baker

Executive Vice President & General Counsel
Illinois Bankers Association

Eileen Lyon

Eileen Lyon is the senior vice president and general counsel of Far East National Bank, in Los Angeles, California. She is the primary legal and risk officer of the bank, and her responsibilities include management and oversight of the bank-wide regulatory compliance program. She chairs the compliance committee and is a member of the management, product development and benefits committees.

Prior to joining Far East National Bank, Ms. Lyon was senior vice president and general counsel of Hawthorne Financial Corporation, a \$2.5 billion financial institution in El Segundo, California, where she was responsible for implementation of initiatives related to the Sarbanes-Oxley Act. Prior to joining Hawthorne Financial, Ms. Lyon was a corporate securities and banking partner at Manatt Phelps & Phillips LLP, Los Angeles, California.

She currently serves on the boards of directors of several nonprofit corporations in Los Angeles, and is president of the school board of St. Cyril's School.

Ms. Lyon received her B.A. from UCLA and is a graduate of the University of Southern California Law Center.

Brian L. Mannion

Brian L. Mannion is a lead counsel with Nationwide Mutual Insurance Company. He has been with Nationwide for several years and practices in the areas of insurance, securities, Ecommerce, privacy, and anti-money laundering. For the past few years he has been the primary lawyer responsible for implementing the bank secrecy act for Nationwide, including its brokers, bank, mutual funds, and life insurance companies. He has spoken frequently regarding the application of anti-money laundering laws to the life insurance industry.

Prior to joining Nationwide, Mr. Mannion was an assistant vice president of a regional bank where he served as the Bank Secrecy Act Officer. He was also the deposit compliance manager focusing on creating policies and procedures to comply with the regulation E, DD, and CC.

He currently serves as the president of ACC's Central Ohio Chapter, and serves on the alumni board for his high school.

Brian is a graduate of the Capital University School of Law and received his B.A. from Miami University.

Michael R. Nelson

Michael R. Nelson is assistant general counsel for JP Morgan Chase Bank in London. In that capacity he works for the Bank's Worldwide securities services division in the EMEA region and is responsible for supporting product development, strategic and complex matters as well as day-to-day business and legal issues.

Mr. Nelson has worked in Europe for many years as a staff lawyer and as manager of in-house legal departments in Luxembourg and London. His legal career has included the securities clearing and global custody industry, derivatives and securities lending and high net worth private banking. He started his legal career as a law clerk in the U.S. Bankruptcy Court for the Northern District of Iowa and worked in private practice in Des Moines.

Mr. Nelson has served on the Board of ACC Europe. He also served a one-year term as a staff-elected member of a pension trustee board of directors. He is an occasional volunteer in a summer program that teaches softball skills to children and their parents in Luxembourg. In February he did a week of volunteer legal work for victims of Hurricane Katrina in a call center in Baton Rouge, Louisiana.

He has a M.A. and J.D. from the University of Iowa and an LL.M. from the University of Cambridge, England.

Program 810: Bank Secrecy Act and Anti- Money Laundering Issues for All Corporations

Presented by:

Bruce Jay Baker

*Executive Vice President and General Counsel
Illinois Bankers Association*

Eileen Lyon

*Senior Vice President and General Counsel
Far East National Bank*

Brian L. Mannion

*Lead Counsel
Office of the Chief Legal and Governance Officer
Nationwide Mutual Insurance Company*

Michael R. Nelson

*Assistant General Counsel
JP Morgan*

Association of Corporate Counsel Annual Meeting

*Hyatt Grand Manchester
San Diego, California
October 25, 2006*

I. Overview of Anti-Money Laundering Regulation in the United States

A. What is money laundering? Why it is done?

1. The colloquial meaning of the term "money laundering" is the process of turning ill-gotten gains, "dirty" money, into "clean money" so that the funds appear to be the proceeds of legal activities. In essence, it is a means of hiding the illegal source of funds. It also serves to

- a) Facilitate tax evasion
- b) Convert a large sum of currency into more manageable assets
- c) Distance illegal proceeds from the crime for purposes of avoiding prosecution and seizure

B. How it is done?

1. The Federal Financial Institutions Examination Council (the "FFIEC")¹, breaks money laundering down into three steps, all of which can occur simultaneously: placement, layering, and integration.

a) Placement

(1) The placement phase involves introducing unlawful proceeds into the financial system without attracting the attention of financial institutions or law enforcement. For example

(a) Dividing a large sum of money into smaller sums for deposit into one or more accounts so as to evade a depository financial institution's currency transaction reporting requirements (also known as "structuring")

(b) Commingling of currency derived from legal activity with currency derived from illegal activity

b) Layering

(1) Layering involves moving funds around the financial system in an attempt to create confusion and complicate the paper trail. For example

(2) Exchanging monetary instruments, such as money orders, for larger or smaller amounts

(3) Wiring money to and from several accounts in one or more financial institutions

¹ The Federal Financial Institutions Examination Council is comprised of one representative respectively from the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and Office of Thrift Supervision.

c) Integration

(1) Final phase of money laundering, and the ultimate goal according to the FFIEC, is integration of the illegal funds "to create the appearance of legality." Additional transactions are engaged in at this stage to "further shield the criminal from a recorded connection to the funds by providing a plausible explanation for the source of the funds. For example, the purchase and resale of real estate, investment securities, foreign trusts, or other assets."

C. Who regulates money laundering and how?

1. Agencies responsible for combating money laundering and terrorist financing.

a) The U.S. General Accounting Office report entitled *Combating Money Laundering: Opportunities Exist to Improve the National Strategy* (GAO-03-813) includes the following summary of the roles and responsibilities of various federal agencies in the fight against money laundering and terrorist financing:

b) Agencies under the Departments of the Treasury, Justice, and Homeland Security [(DHS)] are to coordinate with each other and with financial regulators in combating money laundering.

c) Within Treasury, the Financial Crimes Enforcement Network (FinCEN) was established in 1990 to support law enforcement agencies by collecting, analyzing, and coordinating financial intelligence information to combat money laundering.

d) In addition to FinCEN, Treasury components actively involved in anti-money laundering and antiterrorist financing efforts include the Executive Office for Terrorist Financing and Financial Crimes, the Office of International Affairs, and the Internal Revenue Service and its Criminal Investigation unit (IRS-CI).²

e) Department of Justice components involved in efforts to combat money laundering and terrorist financing include the Criminal Division's Asset Forfeiture and Money Laundering Section (AFMLS) and Counterterrorism Section, the Federal Bureau of Investigation (FBI), the Drug Enforcement Administration (DEA), and the Executive Office for U.S. Attorneys (EOUSA) and U.S. Attorneys Offices.³

² Among other duties, Treasury's Executive Office for Terrorist Financing and Financial Crimes is charged with developing and implementing the NMLS [National Money Laundering Strategy] and U.S. government strategies to combat terrorist financing. These duties were previously conducted by Treasury's Office of Enforcement, which was disbanded in March 2003.

³ Justice's Asset Forfeiture and Money Laundering Section (AFMLS) is the department's focal point for NMLS issues

f) With the creation of DHS in March 2003, anti-money laundering activities of the Customs Service were transferred from Treasury to DHS's Bureau of Immigration and Customs Enforcement (ICE).

g) The financial regulators who oversee financial institutions⁴ anti-money laundering efforts include the depository institution financial regulators that constitute the FFIEC (Federal Reserve Board (FRB), FDIC, Office of the Comptroller of the Currency (OCC), Office of Thrift Supervision (OTS), and National Credit Union Administration (NCUA)), as well as the Securities and Exchange Commission (SEC), which regulates the securities markets, and the Commodity Futures Trading Commission (CFTC), which regulates commodity futures and options markets.

2. Significant US money laundering legislation.

a) 1970 - Bank Secrecy Act (31 USC 5311 et seq., 12 USC §1829b, and §§1951-1959 and 31 USC §§5311-5332) ("BSA").

(1) In order to aid in the identification of the source, volume, and movement of currency and other monetary instruments, the Act established recordkeeping and reporting requirements for individuals and financial institutions. The principal BSA reporting and recordkeeping requirements created were the following:

(a) Currency Transaction Report ("CTR"). Financial institutions are required to file a CTR with the U.S. Department of the Treasury for each cash transaction (deposit, withdrawal, exchange or other payment or transfer) involving more than \$10,000.

(i) Aggregation of currency transactions. Multiple currency transactions must be treated as a single transaction if the financial institution has knowledge that they are by or on behalf of the same person and result in either cash in or cash out totaling more than \$10,000 during any one business day. According to the FFIEC, "[b]anks are strongly encouraged to develop systems necessary to aggregate currency transactions throughout the bank."

(2) For example, a financial institution should be able to aggregate the transactions conducted by one individual over the course of one business day conducted at all of

⁴ For purposes of the Bank Secrecy Act (BSA) and anti-money laundering laws, the term "financial institution" covers both depository and non-depository financial institutions. See Section II.A.3. This paper uses the term "financial institution" in the same manner, unless otherwise noted.

its US branches. If the aggregate of the transactions is greater than \$10,000, a CTR must be filed.

(i) In addition, transactions are not to be offset against one another: If there are both cash in and cash out transactions that are reportable, the amounts should be considered separately and not aggregated. However, they may be reported on a single CTR.

(3) Examples. The following examples appear in the instructions section of the CTR (FinCEN Form 104):

(4) A person deposits \$11,000 in currency to his savings account and withdraws \$12,000 in currency from his checking account. The CTR should be completed as follows: Cash In \$11,000, Cash Out \$12,000. This is because there are two reportable transactions. However, one CTR may be filed to reflect both.

(5) A person deposits \$6,000 in currency to his savings account and withdraws \$4,000 in currency from his checking account. Further, he presents \$5,000 in currency to be exchanged for the equivalent in French Francs. The CTR should be completed as follows: Cash In \$11,000 and no entry for Cash Out. This is because in determining whether the transactions are reportable, the currency exchange is aggregated with each of the Cash In and Cash Out amounts. The result is a reportable \$11,000 Cash In transaction. The total Cash Out amount is \$9,000, which does not meet the reporting threshold. Therefore, it is not entered on the CTR.

(i) CTR exemptions. Certain types of financial institution customers are exempt from currency transaction reporting. They include a depository financial institution, to the extent of its domestic operations, a federal, state or local government agency or department, and any entity (other than a depository financial institution) whose common stock is listed on the New York, American, or Nasdaq stock exchanges (with some exceptions). A transaction account of a U.S. commercial enterprise also may be exempted if it has been maintained for at least 12 months and the business frequently engages in transactions in currency in excess of \$10,000. A "payroll customer's" transaction account also is exemptible if it has been maintained for at least 12

months, is owned by a U.S. commercial enterprise, and on a regular basis withdraws in excess of \$10,000 to pay its U.S. employees in currency. Financial institutions are required to file a Designation of Exempt Person form and undertake subsequent reviews and filings depending on the type of exempt entity involved.

(ii) Filing time frames and record retention requirements. A CTR must be filed within 15 days after the date of the transaction (25 days if filed magnetically or electronically). A copy of the CTR must be kept for 5 years.

(b) Report of International Transportation of Currency or Monetary Instruments ("CMIR"). A CMIR (FinCEN Form 105) must be filed with the Bureau of Customs and Border Protection by a person or entity (1) who physically transports, mails, or ships currency or other monetary instruments in an aggregate amount exceeding \$10,000 at one time either into or out of the United States, or (2) who receives in the United States currency or other monetary instruments in an aggregate amount exceeding \$10,000 at one time which have been transported, mailed, or shipped to the person from any place outside the United States. There are numerous exemptions from this reporting requirement, including depository financial institutions and securities brokers and dealers that mail or ship currency or monetary instruments through the postal service or by common carrier.

(c) Report of Foreign Bank and Financial Accounts ("FBAR"). A FBAR must be filed with the Department of the Treasury by each United States person (an individual, partnership, corporation, estate or trust) who has a financial interest in, or signature or other authority over, any financial accounts, including bank, securities, or other types of financial accounts in a foreign country, if the aggregate value of these financial accounts exceeds \$10,000 at any time during the calendar year. Employees of depository financial institutions and certain other U.S. corporations that maintain foreign financial accounts are exempt from the reporting, as long as they do not have a personal interest in the accounts.

(d) Extensions of Credit and Currency Transfers. Financial institutions are required to retain

records for five years on the following: (1) for each extension of credit exceeding \$10,000 (unless secured by real property), the name and address of the borrower, the amount of the loan, the nature or purpose of the loan, and the date of the loan, (2) for each instruction received regarding a transaction resulting (or intended to result and later cancelled if such a record is normally made) in the transfer of more than \$10,000 to or from a person, account, or place outside the United States, and (3) for each instruction given to another financial institution or person regarding a transaction resulting in the transfer of more than \$10,000 to a person, account or place outside the United States.

b) 1986 - Money Laundering Control Act ("MLCA").

(1) The MLCA, among other things, added a provision to the BSA prohibiting the "structuring" of transactions and established money laundering as a separate criminal offense.

(2) Structuring. The BSA imposes criminal liability on a person or financial institution that structures transactions to avoid their reporting. Structuring a transaction includes, for example, breaking down a single sum of currency exceeding \$10,000 into smaller sums at or below \$10,000. The transactions need not exceed the \$10,000 reporting threshold at any single financial institution on any single day in order to constitute structuring.

(3) Money laundering as a separate criminal offense. 18 U.S.C. §1956(a)(1) establishes money laundering as a federal offense that carries with it a fine of up to \$500,000 or twice the value of the property involved, whichever is greater, and/or imprisonment for up to 20 years. Under the statute, it is a crime to conduct (or attempt to conduct) a financial transaction with the proceeds of "specified unlawful activity," knowing that the property involved comes from some form of unlawful activity with the intent to promote the carrying on of "specified unlawful activity" (defined in the statute to include a multitude of offenses such as bank robbery, murder, mail fraud, and even certain environmental crimes), with the intent to engage in tax evasion or the filing of false tax documents, knowing that the transaction is designed to conceal or disguise the nature, location, source, ownership, or control of the proceeds, or knowing that the transaction is designed to avoid a transaction reporting requirement under state or federal law.

(4) Money laundering is not a continuing offense; each financial transaction constitutes a separate offense.

(5) For example, a drug dealer who takes \$1 million in cash from a drug sale and divides the money into smaller lots and deposits it in 10 different banks (or in 10 different branches of the same bank) on the same day has committed 10 distinct violations of the new statute. If he then withdraws some of the money and uses it to purchase a boat or condominium, he will have committed two more violations, one for the withdrawal and one for the purchase." S. Rep. No. 433, 99th Cong. 2d Sess., at 12-13 (1986) In addition, money laundering is a separate and distinct offense from the underlying criminal activity that resulted in the "dirty money" being "laundered."

c) 1988- Anti-Drug Abuse Act ("ADAA").

(1) The ADAA, among other anti-money laundering provisions, amended the BSA to require recordkeeping and reporting in connection with the purchase and sale of bank checks, cashier's checks, traveler's checks, and money orders for currency in amounts between \$3,000 and \$10,000, inclusive.

(2) Purchaser verification.

(a) Financial institutions must verify the identity of a person purchasing monetary instruments for currency in amounts between \$3,000 and \$10,000. Financial institutions may either verify that the purchaser of monetary instruments is a deposit account holder with identifying information on record with the institution, or an institution may verify the identity of the purchaser by viewing a form of identification that contains the customer's name and address and that the financial community accepts as a means of identification when cashing checks for noncustomers. The financial institution must obtain additional information for purchasers who do not have deposit accounts.

(3) Aggregation

(a) Multiple purchases during one business day totaling \$3,000 or more must be aggregated and treated as one purchase if the financial institution has knowledge that the purchases have occurred.

(4) Recordkeeping

(a) The method used to verify the identity of the purchaser must be recorded. Additional information, such as the date of purchase, the type of monetary instruments purchased, including their serial numbers, and the amount in dollars of each of the instruments purchased, also must be recorded. Records must be retained by the financial institution for five years

(5) Reporting

(a) The Secretary of the Treasury is authorized to request a financial institution's monetary instrument purchase records at any time.

d) 1992 - Annunzio-Wylie Anti-Money Laundering Act ("AWAMLA").

(1) The AWAMLA amended the BSA to require that financial institutions report "suspicious activity" and maintain records of certain funds transfers.

(2) Suspicious activity reports ("SARs").

(a) Financial institutions³ are required to file a SAR if (1) the transaction is conducted or attempted by, at or through the financial institution, (2) it involves funds or other assets of \$5,000 (in general, \$2,000 in the case of money services businesses), and (3) the financial institution knows, suspects, or has reason to suspect that:

(i) 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 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, or

(ii) the transaction is designed to evade any requirements of the BSA, or

(iii) the transaction has no business or apparent lawful purpose or is not the sort in which the particular customer would

³ Depository financial institutions also are subject to additional SAR filing requirements under regulations promulgated by the five federal bank regulatory agencies. For example, a bank must file a SAR if it has a substantial basis for identifying an insider in connection with a criminal activity, regardless of the dollar amount involved in the transaction.

normally be expected to engage, and the financial institution knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction, or

(iv) in the case of non-depository financial institutions, the transaction involves use of the financial institution to facilitate criminal activity.

(b) Timing

(i) A SAR must be filed within 30 calendar days after a financial institution detects the facts forming the basis for the filing. Except with respect to SARs filed by money services businesses, an additional 30 days may be tacked on for the identification of a suspect. In addition, ongoing suspicious activity should be reported at least every 90 days. Certain exigent situations also must be reported by telephone immediately.

(c) Confidentiality

(i) A financial institution, and its directors, officers, employees and agents, may not notify any person involved in a suspicious transaction that the transaction has been reported.

(d) Safe harbor

(i) A financial institution, and its directors, officers, employees and agents, that make a disclosure of any possible violation of law or regulation, "shall not be liable to any person under any law or regulation of the United States, any constitution, law, or regulation of any State or political subdivision of any State, or under any contract or other legally enforceable agreement (including any arbitration agreement), for such disclosure or for any failure to provide notice of such disclosure to the person who is the subject of such disclosure or any other person identified in the disclosure".

(e) Record retention

(i) Financial institutions are required to retain a copy of a SAR and supporting documentation for five years.

(3) Funds transfers

(a) Each financial institution involved in a funds transfer of \$3,000 or more is required to collect and retain certain information in connection with the transfer. There are various exceptions to the funds transfer requirements, where, for example, the originator and beneficiary are: a depository financial institution, a wholly owned domestic subsidiary of a depository financial institution chartered in the United States, a broker or dealer in securities, a wholly owned domestic subsidiary of a broker or dealer in securities, the United States, a state or local government, or a federal, state or local government agency or instrumentality.

(b) The information required to be collected and retained depends on the financial institution's role in the particular funds transfer (originator, intermediary, or beneficiary institution). The requirements also may vary depending on whether an established customer of a financial institution is involved and whether a payment order is made in person.

(c) Under what is known as the "Travel Rule," financial institutions are required to include certain information in the transmittal order, including the names and addresses of the transmitter and, to the extent known, the recipient.

e) 2001 - USA PATRIOT Act.

(1) Among other provisions, the USA PATRIOT Act required the Secretary of the Treasury and the federal financial regulators to promulgate regulations for a financial institution's identification of its customers prior to opening accounts. The Act also mandated that all financial institutions implement an anti-money laundering program.

(2) Customer identification programs ("CIPs")

(a) The USA PATRIOT Act required that financial institutions implement reasonable procedures for:

- (i) verifying the identity of any person seeking to open an account to the extent reasonable and practicable,
- (ii) maintaining records of the information used to verify a person's identity,

including name, address, and other identifying information, and

(iii) consulting lists of known or suspected terrorists or terrorist organizations provided to the financial institution by any government agency to determine whether a person seeking to open an account appears on any such list.⁶

(b) A financial institution's customer identification program must be "risk based," meaning that it must be tailored to address the risks presented by the institution's size, location, customer base, product offerings, and account opening procedures, for example. However, the applicable regulations require that financial institutions obtain certain minimum identification information, including a customer's name, address, date of birth (if applicable), and, subject to certain exceptions, a taxpayer identification number or government-issued document if the customer is not a "U.S. person." In addition, financial institutions must have procedures in place for the documentary or non-documentary verification of the identifying information provided by customers, and also must maintain records of the information obtained in connection with the verification procedures.

(3) Anti-money laundering programs.

(a) Prior to the USA PATRIOT Act, only depository financial institutions and casinos were required to establish an anti-money laundering program. The Act expanded this requirement to include all financial institutions⁷ and provided that, at a minimum, an anti-money laundering program must include the following four "touchstones":

- (i) the development of internal policies, procedures, and controls,
- (ii) the designation of a compliance officer,
- (iii) an ongoing employee training program, and
- (iv) an independent audit function to test programs.

⁶ At this time, no such list has been designated. But, refer to the discussion of OFAC SDN lists in Section III.L.

⁷ However, as of July 2006, only certain types of financial institutions are subject to final rules implementing the anti-money laundering program requirements established by the USA PATRIOT Act.

II. Who is affected by anti-money laundering regulations?

A. Financial institutions.

1. Financial institutions are on the front line of anti-money laundering regulations. Through enactment of various laws since 1970, financial institutions have been required to develop and implement programs that are reasonably designed to detect and deter money laundering and terrorist financing activities. Financial institutions are not expected to ascertain whether an underlying crime has actually been committed. That is the job of law enforcement; financial institutions are merely required to report suspicious activities.

2. The systems financial institutions are required to develop should be risk based; that is, the financial institutions are required to evaluate the risk within their institution's products, services customers, and geographic locations. Some factors will be weighted more heavily than others. In general, however, a large international financial institution with a multitude of products, particularly those that facilitate the movement of money across borders, will be expected to have a significantly more robust BSA program than a small community savings and loan with traditional mortgage and deposit products.

3. The BSA defines the term "financial institution" as follows:

- a) an insured bank (as defined in section 3(h) of the Federal Deposit Insurance Act (12 U.S.C. 1813 (h)));
 - b) a commercial bank or trust company;
 - c) a private banker;
 - d) an agency or branch of a foreign bank in the United States;
 - e) any credit union;
 - f) a thrift institution;
 - g) a broker or dealer registered with the Securities and Exchange Commission under the Securities Exchange Act of 1934 (15 U.S.C. 78a et seq.);
 - h) a broker or dealer in securities or commodities;
 - i) an investment banker or investment company;
 - j) a currency exchange;
 - k) an issuer, redeemer, or cashier of travelers' checks, checks, money orders, or similar instruments;
 - l) an operator of a credit card system;
 - m) an insurance company;
 - n) a dealer in precious metals, stones, or jewels;
 - o) a pawnbroker;
 - p) a loan or finance company;
 - q) a travel agency;
 - r) a licensed sender of money or any other person who engages as a business in the transmission of funds, including any person who engages as a business in an informal money transfer system or any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside of the conventional financial institutions system;
 - s) a telegraph company;
 - t) a business engaged in vehicle sales, including automobile, airplane, and boat sales;
 - u) persons involved in real estate closings and settlements;
 - v) the United States Postal Service;
 - w) an agency of the United States Government or of a State or local government carrying out a duty or power of a business described in this paragraph;
 - x) a casino, gambling casino, or gaming establishment with an annual gaming revenue of more than \$1,000,000 which—
 - (1) is licensed as a casino, gambling casino, or gaming establishment under the laws of any State or any political subdivision of any State; or
 - (2) is an Indian gaming operation conducted under or pursuant to the Indian Gaming Regulatory Act other than an operation which is limited to class I gaming (as defined in section 4(6) of such Act);
 - y) any business or agency which engages in any activity which the Secretary of the Treasury determines, by regulation, to be an activity which is similar to, related to, or a substitute for any activity in which any business described in this paragraph is authorized to engage; or
 - z) any other business designated by the Secretary whose cash transactions have a high degree of usefulness in criminal, tax, or regulatory matters.
- aa) Additional Definitions.— For purposes of the Bank Secrecy Act, the following definitions also apply:
- (1) Certain institutions included in definition.—The term "financial institution" (as defined in subsection (a)) includes the following:
 - (a) Any futures commission merchant, commodity trading advisor, or commodity pool operator registered, or required to register, under the Commodity Exchange Act.

4. Given the expansive definition of "financial institution," the potential reach of BSA recordkeeping and reporting requirements is extensive. However, final rules implementing the BSA requirements have not been issued for many of the entities covered by the Act. For example, although the Secretary of the Treasury is authorized to require that all domestic financial institutions perform currency transaction reporting under the BSA (31 U.S.C. §5313), to date the regulations implementing these reporting requirements apply only to depository financial institutions, brokers or dealers in securities, money services businesses, telegraph companies, persons subject to supervision by any state or federal bank regulatory authority, futures commission merchants, introducing brokers in commodities, casinos, and card clubs.

NOTE: The Internal Revenue Service has separate rules requiring the filing of reports regarding cash payments, which are discussed below at Section III.K.

B. Financial institutions' customers

1. The recordkeeping and reporting requirements established by the BSA impact a financial institution's policies and procedures as well as those of its customers.

NOTE: These impacts are discussed extensively in Section III, below.

C. Customers of Financial Institutions' Customers.

1. Because financial institutions must be increasingly vigilant in monitoring their customers' activities, by extension, customers of financial institutions need to be prepared to answer questions about the nature of their customers.

2. If a business customer of a financial institution is found to be involved in check cashing, for example, the financial institution may need to treat a customer as a money services business. Once a potential money services business is identified, a financial institution may need to request additional information from the customer concerning its compliance with federal and state registration requirements that need to be satisfied. Should the customer then refuse or fail to register as a money services business it may find that the financial institution is reluctant to maintain a relationship with the business. All businesses (and particularly money services businesses) should be prepared to provide this information to its financial institution when seeking to open an account or when requested to do so by its financial institution for purposes of maintaining an existing account relationship. Otherwise, the financial institution may feel uncomfortable about the relationship and request that the account be closed.

III. What are the potential impacts on customers?

A. General

1. As discussed, financial institutions have a legislative and regulatory mandate to monitor their customers' accounts for suspicious activities in order to detect and deter money laundering and terrorist financing.
2. Although generally speaking, federal financial regulators will not require an institution to close an account, financial institutions are required to take steps to determine for themselves whether to open or maintain an account for business. This will involve obtaining basic identifying information and conducting a basic risk assessment to determine the level of risk associated with the account and to solicit additional information, as deemed necessary. The extent to which a financial institution will seek additional information will be dictated by the financial institution's assessment of the level of risk posed by the individual customer. Not all businesses pose the same level of risk, and that not all businesses will always require additional due diligence. In some cases, the amount of additional customer due diligence performed by a financial institution will be negligible. In other situations, the additional due diligence performed will be extensive.
3. At the same time, financial institution customers have a natural and legitimate interest in maintaining the privacy of their financial information. Frequently, customers are not aware that this desire for secrecy may be viewed as a possible "red flag" necessitating further investigation by their financial institution and/or the filing of a SAR.

B. Red Flag Warnings

1. Businesses that are reluctant to provide such information will find it harder to maintain or open accounts with financial institutions in future, as the institutions become more familiar with the risks of noncompliance with regulatory mandates for an effective BSA/AML program.
2. Some red flags identified by the regulators that may be noted by your financial institution include the following:
 - a) Customers who provide insufficient or suspicious information about their identity, corporate ownership, business activities or expected transaction activity.
 - b) A customer's background differs from that which would be expected on the basis of his or her business activities.
 - c) A customer who makes frequent or large transactions and has no record of past or present employment experience.
 - d) Customers who are reluctant to provide information, particularly if the customer is a company and the information sought is about controlling parties or beneficial owners.

- e) Customers who try to avoid reporting or recordkeeping requirement (i.e., "structuring").
- f) Unexplained funds transfers, particularly those sent in large, round dollar amounts or which occur to or from an offshore corporate haven or high-risk geographic location without an apparent business reason or when the activity is inconsistent with the customer's business or history.
- g) Activities that are inconsistent with the stated purpose or anticipated activities given when opening the account.
- h) Unusual patterns of activity, particularly those involving currency or currency substitutes (money orders, stored value cards) that are atypical or inconsistent with past practices.

C. Private Banking

1. The Federal Reserve has long recognized that private banking is vulnerable to money laundering activities. Consequently, it is not surprising that private banking activities have come within the scope of the BSA and regulations. Under the USA Patriot Act, the federal banking regulators were required to establish regulations that provide for due diligence for private banking accounts for non-U.S. persons, and enhanced scrutiny of "senior foreign political figures."
2. Broadly speaking, private banking is the provision of a wide variety of financial services targeted to high net worth individuals and their related businesses, typically through a relationship manager who develops and maintains strong ties to the customer and provides him or her with a high degree of personalized service.
3. Frequently, private banking involves money management services, including:
 - a) investment portfolio management,
 - b) financial planning,
 - c) custodial services,
 - d) funds transfer,
 - e) lending,
 - f) overdraft privileges,
 - g) letter-of-credit financing and
 - h) bill payment.
4. Private banking is very competitive among financial institutions, and almost always involves a high degree of confidentiality. Although usually customers have legitimate reasons for desiring confidentiality, these attributes make private banking susceptible to the elements of money laundering: placement, layering and integration.

5. Under the BSA, covered financial institutions are required to develop processes and systems for monitoring the risks associated with private banking accounts maintained for non-U.S. persons. A "covered financial institution" includes:
 - a) Insured depository financial institutions
 - b) Insured savings associations
 - c) Insured credit unions
 - d) Agencies and branches of foreign depository financial institutions
 - e) Securities broker-dealers
 - f) Futures commission merchants
 - g) Introducing brokers
 - h) Mutual funds
6. However, money services business ("MSBs"), casinos, operators of credit card systems and foreign branches of U.S. depository financial institutions are not subject to this rule.
7. A "private banking account", is defined as an account (or any combination of accounts) maintained at a financial institution that satisfies all three of the following criteria:
 - a) Requires a minimum aggregate deposit of funds or other assets of not less than \$1,000,000.
 - b) Is established on behalf of or for the benefit of one or more non-U.S. persons who are direct or beneficial owners of the account, and
 - c) Is assigned to, or is administered by, in whole or in part, an officer, employee, or agent of a financial institution acting as a liaison between a financial institution covered by the regulation and the direct or beneficial owner of the account.
8. Many financial institutions offer services that are generically termed private banking, but do not require a minimum deposit of at least \$1,000,000. Although these relationships are not subject to the expanded requirements under the BSA for "private banking accounts", they nevertheless will be subject to a greater level of due diligence under the financial institution's risk-based BSA/AML compliance program.
9. For private banking accounts that fall within the definition, the financial institution is responsible to have a process whereby the financial institution:
 - a) Determines identity of nominal and beneficial owner of any private banking account
 - b) Determines if owner is a senior foreign political figure (also termed a "politically exposed person" or "PEP").

- c) Determines source(s) of funds deposited into a private banking account, purpose and expected use of the account.
- d) Reviews account activity to ensure that it is consistent with the information obtained about the client's source of funds, and with the stated purpose and expected use of the account, and
- e) Files Suspicious Activity Report (SAR), as appropriate, to report any known or suspected money laundering or suspicious activity conducted to, from, or through a private banking account.

D. Money Services Businesses

1. What is a Money Services Business ("MSB")?

a) In general. According to the Financial Crimes Enforcement Network ("FinCEN"), "MSBs provide valuable financial services, especially to those who may not have ready access to the banking sector. The MSB industry is quite diverse, ranging from large Fortune 500 companies with global presence to small "mom-and-pop" convenience stores in ethnic neighborhoods where English may rarely be spoken. Moreover, given the types of the products and services provided and the distribution channels, some participants in this industry sector may be at greater risk for misuse by terrorist financiers, money launderers, and other criminals. Consequently, [FinCEN] believe[s] that it is vital to identify and reduce the number of unregistered MSBs in order to better focus resources to encourage increased compliance with the BSA's programmatic, recordkeeping, and reporting requirements."

b) Definition.

(1) An MSB is each agent, agency, branch, or office within the United States of any person doing business, whether or not on a regular basis or as an organized business concern, in one or more of the following capacities:

- (a) Currency dealers or exchangers
- (b) Check cashers
- (c) Issuers of traveler's checks, money orders, or stored value
- (d) Sellers or redeemers of traveler's checks, money orders, or stored value
- (e) Money transmitters
- (f) The United States Postal Service (except with respect to the sale of postage or philatelic products)

(2) A business in one of the first four categories that engages in transactions "in an amount greater than

\$1,000 in currency or monetary or other instruments for any person on any day in one or more transactions" is considered to be an MSB (although there is no dollar threshold for money transmitters). 31 C.F.R. §103.11(uu). FinCEN has stated, however, that "if an entity crosses the \$1,000 MSB definitional threshold on a one-time basis, that one-time action, if not repeated, does not cause the entity to become an MSB."

c) Exclusions.

(1) Depository financial institutions, savings and loans, credit unions, and persons registered with, and regulated or examined by, the Securities and Exchange Commission or the Commodity Futures Trading Commission, are not MSBs.

d) Registration.

(1) MSBs (irrespective of whether they are required to be licensed by a State) must register with the Department of the Treasury (31 C.F.R. §103.41), except for:

- (a) The United States Postal Service
- (b) A branch office of an MSB
- (c) Agencies of the United States, of any State, or of any political subdivision of a State
- (d) An issuer, seller, or redeemer of stored value
- (e) A person that is an MSB solely because it acts as an agent for another MSB. For example, a grocery store that acts as an agent for an issuer of money orders and performs no other services that would cause it to be a money services business is not required to register. However, registration would be required if the grocery store, in addition to acting as an agent of an issuer of money orders, also cashed checks or exchanged currencies (other than as an agent for another business) in an amount greater than \$1,000 in currency or monetary or other instruments for any person on any day, in one or more transactions.

(2) An MSB that is required to register with FinCEN has 180 days in which to register from the time that it begins conducting business. Ignorance of the law is no defense for an MSB not registering—simply operating an MSB that is required to register but has failed to do so is sufficient to trigger severe penalties for the MSB under the USA PATRIOT Act. A list of registered MSBs is posted

on FinCEN's website. As of October 2004, only one out of ten of all MSBs had registered with FinCEN as required by federal law. (Statement of Julie L. Williams, Acting Comptroller of the Currency, before the Committee on Banking, Housing, and Urban Affairs United States Senate, April 26, 2005.) FinCEN's new August 2006 list, which was current as of August 3, 2006, contains data on 26,951 registered MSBs.

e) MSBs and BSA recordkeeping and reporting requirements.

(1) In addition to the requirement to register with FinCEN, MSBs, with limited exceptions, also are subject to the recordkeeping and reporting requirements of the Bank Secrecy Act. For example, an MSB must have an anti-money laundering program, and it is subject to large currency transaction reporting and may be subject to suspicious activity reporting requirements, among other requirements.

f) MSBs as depository financial institution customers: what MSBs can expect.

(1) Interagency Guidance

(a) The FFIEC issued an "Interagency Interpretive Guidance on Providing Banking Services to Money Services Businesses Operating in the United States" on April 26, 2005 (the "Guidance"). The Guidance was meant to reassure depository financial institutions that they are not expected to be the de facto regulators of MSBs and will not be held responsible for their customers' compliance with the BSA and other applicable federal and state laws and regulations.

(b) Nevertheless, the Guidance clarified certain minimum due diligence expectations for depository financial institutions when opening or maintaining accounts for MSBs.

(2) Minimum due diligence.

(a) An MSB can expect that a depository financial institution will undertake the following minimum due diligence steps when opening or maintaining its account:

(i) Apply its Customer Identification Program (commonly referred to as a "CIP")

(ii) Confirm the customer's FinCEN registration, if required

(iii) Confirm the customer's state licensing status, if applicable

(iv) Confirm the customer's agent status, if applicable

(v) Conduct a risk assessment to determine the level of risk associated with each account of the customer and whether further due diligence is required

(3) Risk assessment.

(a) Not all MSBs pose the same level of risk for money laundering and other illegal activities. For example, a local grocery store that cashes paychecks for neighborhood customers poses less risk than a currency exchange that cashes checks for customers spread over a large metropolitan area. The level of a depository financial institution's scrutiny of an MSB should reflect the level of risk that it presents. This means that a depository financial institution may need to obtain additional information from an MSB that falls into a higher risk category.

(b) Basic considerations.

(i) When performing this basic risk assessment, depository financial institutions will consider, at a minimum:

(a) the types of products and services offered by an MSB

(b) the locations and markets served by the MSB

(c) the types of banking account services needed by the MSB

(d) the purpose of each depository financial institution account

(4) "Risk indicators."

(a) The FFIEC Guidance lists two sets of "risk indicators" that depository financial institutions can use as checklists: one set represents a low level of risk, and the other represents a higher level of risk. An example of a low risk indicator would be that the MSB primarily markets to customers that conduct routine transactions with moderate frequency in low amounts. A high risk indicator may be that the MSB has failed to obtain proper state licensing, or it allows its customers to conduct higher transactional

amounts with moderate to high frequency. The final determination of the level of risk posed by an MSB is always a judgment call to be made by the depository financial institution.

(5) Significance of being a high risk MSB.

(a) Once a depository financial institution has identified an MSB as a high risk customer, the FFIEC Guidance suggests seven extra due diligence steps that a depository financial institution may need to take. These include:

- (i) making an on-site visit to the MSB
- (ii) reviewing the MSB's own anti-money laundering program
- (iii) reviewing the MSB's employee screening practices
- (iv) reviewing lists of the MSB's agents and locations in and outside of the United States that receive services through the MSB's depository financial institution account
- (v) reviewing the MSB's procedures for its operations
- (vi) reviewing results of the MSB's independent testing of its anti-money laundering program
- (vii) reviewing written agent management and termination practices for the money services business

(b) Some or all of these additional steps should be conducted based on the "level of perceived risk, and the size and sophistication" of the particular MSB, which the Guidance suggests may change over the course of the MSB's relationship with the depository financial institution.

(6) FinCEN registration and state licensing failures

(a) One of the BSA compliance challenges confronting depository financial institutions today is the extent to which they need to inquire about a customer's activities in order to determine whether the customer must be registered with FinCEN and/or licensed by a state authority. MSBs registered with FinCEN may or may not need to be licensed in the state where they are conducting business. Likewise, a non-financial

institution that requires licensure under state law may not be an MSB subject to registration under federal laws and regulations. This can make for complicated account opening and monitoring procedures.

(b) Most depository financial institutions will make certain inquiries at account opening and conduct ongoing account monitoring to uncover activities such as check cashing that may require registration and licensure.

(c) One thing is clear, however, and that is that if a depository financial institution determines that its customer should be registered with FinCEN or licensed by the state, a failure on the part of the customer to be registered or licensed will result in the depository financial institution's filing of a suspicious activity report on the customer under 31 C.F.R. §103.18!

E. Politically Exposed Persons ("PEPs")

1. With respect to PEPs, covered institutions are required to monitor the accounts to guard against accepting the proceeds of official foreign corruption. "Proceeds of foreign corruption" means any assets or property that is acquired by, through, or on behalf of a PEP through misappropriation, theft, or embezzlement of public funds, the unlawful conversion of property of a foreign government, or through acts of bribery or extortion, and includes any other property into which any such assets have been transformed or converted. (31 CFR 103.178(c)(2)).

a) A senior foreign political figure, or PEP, includes the following:

(1) A current or former:

- (a) Senior official in the executive, legislative, administrative, military, or judicial branches of a foreign government (whether elected or not).
- (b) Senior official of a major foreign political party.
- (c) Senior executive of a foreign-government-owned commercial enterprise.

(2) A corporation, business, or other entity that has been formed by, or for the benefit of, any such individual.

(3) An immediate family member (including spouses, parents, siblings, children, and a spouse's parents and siblings) of any such individual.

(4) A person who is widely and publicly known (or is actually known by the relevant financial institution) to be a close associate of such individual.

2. Financial institutions are expected to identify PEPs by inquiring about present and past employment, reviewing public databases that are reasonably available, and reviewing government lists, newspapers and public reports regarding foreign figures and their associates.

F. Customers Presenting Special Concerns

1. Certain customers, by their nature, present additional risks to financial institutions for money laundering. These include the following:

- a) Nonresident Aliens and Foreign Individuals
- b) Politically Exposed Persons
- c) Embassy and Foreign Consulate Accounts
- d) Non-Depository Financial Institutions
- e) Professional Service Providers
- f) Non-Governmental Organizations and Charities
- g) Certain Business Entities, such as shell corporations, international business corporations (i.e., companies that are formed outside a person's country of residence) and private investment companies, especially those opened in offshore financial centers.
- h) Cash-Intensive Businesses, such as
 - (1) Convenience stores,
 - (2) Restaurants,
 - (3) Retail stores,
 - (4) Liquor stores,
 - (5) Cigarette distributors,
 - (6) Privately owned automated teller machines (ATMs),
 - (7) Vending machine operators and
 - (8) Parking garages.

G. Trade Finance

1. Trade finance typically involves short-term financing to facilitate the import and export of goods. Companies on both sides of the trade desire financial institutions' involvement in trade finance in order to minimize payment risk. However, because trade finance activities involve multiple parties on both

sides of the transaction, the process of due diligence becomes more difficult. Also, since trade finance can be more document-based than other banking activities, it can be susceptible to documentary fraud, which can be linked to money laundering, terrorist financing, or the circumvention of OFAC sanctions or other prohibitions.

2. Trade in weapons or nuclear equipment are obviously high risk for terrorist activity, but financial institutions also need to be concerned about goods that may be over- or under-valued in an effort to evade AML or customs regulations.

Example: An importer pays a large sum of money from the proceeds of an illegal activity for goods that are essentially worthless and are subsequently discarded.

Example: Trade documents, such as invoices, are fraudulently altered to hide the scheme. Variations on this theme include double invoicing, partial shipment of goods, and the use of fictitious goods. Illegal proceeds transferred in such transactions thereby appear sanitized and enter the realm of legitimate commerce.

Example: Third-party nominees, such as shell companies, are substituted to disguise an individual's or company's role in a trade finance agreement. This substitution results in a lack of transparency, effectively hiding the identity of the purchasing party, thus increasing the risk of money laundering activity.

3. Financial institutions involved in trade finance activities are expected to have an understanding of the customer's underlying business and locations served. This may require background checks or investigations, particularly in higher risk jurisdictions and to carefully review documentation, not only for compliance with the terms of the letter of credit, but also for anomalies or red flags that could indicate unusual or suspicious activity. In some circumstances, stopping the trade may be required to avoid a potential violation of an OFAC sanction.

4. In addition to OFAC filtering, the financial institution is likely to scrutinize:

- a) Items shipped that are inconsistent with the nature of the customer's business (e.g., a steel company that starts dealing in paper products, or an information technology company that starts dealing in bulk pharmaceuticals).
- b) Customers conducting business in high-risk jurisdictions.
- c) Customers shipping items through high-risk jurisdictions, including transit through non-cooperative countries.
- d) Customers involved in potentially high-risk activities (e.g., dealers in weapons, nuclear materials, chemicals, precious gems; or certain natural resources such as metals, ore, and crude oil).

- e) Obvious over- or under-pricing of goods and services (e.g., importer pays \$400 an item for one shipment and \$750 for an identical item in the next shipment; exporter charges one customer \$100 per item and another customer \$400 for an identical item in the same week).
- f) Excessively amended letters of credit without reasonable justification.
- g) Transactions evidently designed to evade legal restrictions, including evasion of necessary government licensing requirements.

H. Enhanced Due Diligence

1. Depending on the institution and the sophistication of its BSA/AML program, you may find that your financial institution is no longer willing to do business with you, or will only do business on certain conditions. Typically, these involve enhanced due diligence, by which the institution will seek to understand or obtain the following information:

Type of Customer	Additional Scrutiny May Involve
Nonresident Aliens	The accountholder's home country The types of products and services used. Forms of identification. Sources of wealth and funds. Unusual account activity.
Politically exposed persons	Identity of the accountholder and beneficial owner. Asking directly about possible PEP status. Identity of the accountholder's country of residence. Employment or other sources of funds. Checking references, as appropriate, to determine whether the individual is or has been a PEP. Identifying the source of wealth. Obtaining information on immediate family members or close associates having transaction authority over the account. Determining the purpose of the account and the expected volume and nature of account activity. Reviewing public sources of information.
Offshore corporations	Determining the beneficial ownership of the corporation Understanding interlocking relationships between affiliated corporations If corporation is organized in tax haven jurisdiction, will need to understand sources of wealth and income, and intended purpose of account If shares are held in bearer form, requiring amendments to charter to make registered form; alternatively, the financial institution will seek to hold shares in trust.

Type of Customer	Additional Scrutiny May Involve
NGOs and charitable organizations	Purpose and objectives of their stated activities. The geographic locations served (including headquarters and operational areas). Organizational structure. Donor and volunteer base. Funding and disbursement criteria (including basic beneficiary information). Recordkeeping requirements. Its affiliation with other NGOs, governments, or groups. Internal controls and audits. Information regarding principals, directors or officers. Obtaining and reviewing the financial statements and audits. Verifying the source and use of funds. Evaluating large contributors or grantors of the NGO. Conducting reference checks.
Cash intensive businesses	Understand customer's business operations, such as intended use of the account; including anticipated transaction volume, products, and services used; Geographic locations involved in the business.
Privately owned ATMs	Payment system utilized, including sponsoring institution Corporate documentation, licenses, permits, contracts and references to verify an independent sales organization's ("ISO's") legitimacy. Controls over the currency servicing arrangements Understanding currency generation of the associated business. Locations of privately owned ATMs ISO's target geographic market. Expected account activity, including expected currency withdrawals.

I. Reporting of Cash Payments Over \$10,000 to a Trade or Business

1. What is this requirement? Who must comply?

- a) Any person in a trade or business who receives more than \$10,000 in cash in a single transaction or in related transactions must file with the Internal Revenue Service ("IRS") Form 8300. The IRS and the Department of Treasury both have similar requirements regarding the filing of Form 8300. The IRS requirements can be found at 26 USCS 6050I, and at 31 USC 5331 for the Department of Treasury, which was added by section 365 of the USA PATRIOT Act. Both agencies have also promulgated regulations that provide further guidance. The IRS has provided additional guidance through Publication 1544. Generally, if you comply with the IRS requirements then you also are complying with the Department of Treasury regulations.
- b) The report is designed to create a record of cash transactions that can be used by law enforcement to track down and arrest drug dealers, terrorist financiers, and other money launderers. These types of reports are critical to law enforcements efforts and allow the tracking of large

transactions using cash or certain types of monetary instruments. Some of the key definitions associated with the filing of Form 8300 include:

2. The definition of person is very broad and includes individuals, companies, partnerships, associations, trusts, and estates.

a) Depository financial institutions and broker/dealers do not have to comply with this requirement because they are obligated to file Currency Transactions Reports.

b) Cash is defined as coin and currency (both US and foreign). It also includes other items not normally thought of as "cash." For example, cashier's checks, bank drafts, treasurer's checks, and money orders all are considered cash. Further, a qualifying monetary instrument must have a face amount of \$10,000 or less, and the trade or business must receive the item in a designated reporting transaction or any transaction in which you know the payer is trying to avoid the reporting requirement. Cash does not include personal checks drawn on an individuals account.

c) A designated reporting transaction is defined to include the retail sale of a consumer durable (e.g. automobile or boat), a collectible (e.g. art, rug, metal, gem, etc.), or travel and entertainment.

d) As you can see, these regulations are fact specific and require an analysis of the type of business involved, the type and amount of the monetary instrument, and type of transaction. Lastly, the IRS regulation requires notice be sent to the subject of the Form 8300 report. This notice must include a contact person at the trade or business, and the total amount of the cash that was reported on the Form 8300. This notice must be sent to the subject by January 31 of the year following the calendar year for which the report was filed.

e) Additionally, some businesses subject to these regulations must also comply with the suspicious activity reporting obligations found in the Bank Secrecy Act. While the reports may appear to be duplicative, the Department of Treasury has made it clear that the two regulatory schemes are different and must be complied with separately (see 71 FR 26215 (May 4, 2006)). Further, the filing of a Form 8300 and the subsequent notice that must be sent to the customer must not alert the customer that a suspicious activity report was or will be filed. Suspicious activity reports are required to be kept confidential.

J. Office Of Foreign Assets Control

1. What is this requirement? Who must comply?

a) The Office of Foreign Assets Control, or OFAC, administers and enforces the economic sanctions authorized by the Congress or the President. These sanctions and embargo programs are designed to utilize the US's economic power to

further its foreign policy and national security interests by targeting foreign countries, terrorists, international narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction. The regulations apply to all United States persons, certain foreign persons living in the United States, and for certain sanctions programs, foreign subsidiaries of United States persons.

b) OFAC administers two general types of programs. The first are economic sanctions against particular countries. These are commonly referred to as sanctions programs and include countries such as Cuba, Iran, North Korea, and Sudan, as well as programs targeted at terrorists and weapons of mass destruction. Each sanctions program is different since they are designed to achieve a specific foreign policy objective that varies from program to program.

c) The second type of program is the Specially Designated Nationals list, or SDN. While the country sanctions may apply to all transactions associated with the government of Cuba, the SDN list specifically identifies an entity that US persons may not "do business with." SDNs typically include terrorist groups, Columbian drug lords, charities that provide funding to terrorists, and other persons that the US government wishes to specifically place economic sanctions upon.

d) The OFAC SDN list is updated regularly as a result of law enforcement investigations or Presidential actions. For example, shortly after the attacks of 9/11 the President, utilizing his statutory authority, issued an executive order seizing the property of the suspected terrorists. Upon issuance of this executive order, all US persons were expected to comply with the requirements of the executive order.

e) OFAC and BSA are different legal obligations. They are based on different statutes and serve different public policy purposes. Most importantly, these laws apply to different constituencies - OFAC applies to almost every US person, while BSA only applies to certain financial institutions. However, there is overlap between the two requirements and are often times considered together. One reason for this treatment is that the OFAC SDN list contains names of terrorists and drug dealers. A solid OFAC compliance program will buttress your BSA compliance efforts.

2. How to Comply?

a) Each of the twenty-some sanctions programs and several thousand SDNs vary in the extent and scope of the prohibited transactions. Generally, businesses must determine how it will build a compliance program. For example, are the company's transactions geographically narrow or do they involve several states or even international matters? Will the company purchase technology that ensures all transactions are scanned against the SDN list? What are the expectations of the company's primary regulator? Lastly, will the company analysis

each and every sanctions program in order to determine if it applies to the company, or will it take a more generic approach whereby it will limit business with anyone on the SDN list or in any sanctioned country.

b) Generally, the OFAC regulations do not specifically require the checking of the OFAC SDN list or country sanctions list. But, if a prohibited transaction occurs with entities on either list, then you will probably violated OFAC regulations and likely incur both a fine and potential reputational harm as well. OFAC fines are published on the OFAC website.

c) Each business needs to understand its customers and the likelihood of performing transactions with prohibited entities. For example, a convenience store in Iowa is likely not implementing a robust OFAC compliance program, as it is not doing business with anyone on the lists. On the other hand, a major league baseball team wishing to sign a new prospect out of Cuba will need to thoroughly understand the OFAC sanctions programs.

d) Once the company has determined its OFAC risks, it should then implement a compliance program. A leading practice is to identify a compliance officer that will be responsible for establishing and managing the program on a day-to-day basis. Corporate wide policies and procedures regarding controls should be written. Business leaders should be directly assigned responsibilities. Employees should receive regular training about OFAC and the company's policies, with increased training for those employees that are integral to your compliance efforts. Lastly, the OFAC compliance program should be periodically evaluated to ensure it is being followed, as well as identify any aspects that could be enhanced.

3. What Next?

a) Now that the company has determined its OFAC risk and created a compliance program, the next step is to compare your transactions against the SDN list and the list of embargoed or blocked countries. Technology solutions can provide significant value to this process. Regardless of how the comparison takes place, there will be a sizable number of potential matches. This is a result of the common names contained in the SDN list. Each potential match should be reviewed to determine if your customer matches the prohibited name (a "hit") or if the match is a considered not a match (a "false positive").

b) The company should develop a consistent, documented, and repeatable process to clear its potential match.

c) If an exact name match is located, you should contact your legal counsel in order to determine the next steps. If a prohibited transaction is identified, OFAC requires the reporting of this information within 10 days and annually each September 30th. The prohibited transaction likely will need to be

"blocked." Again, counsel should be engaged in order to navigate these complex laws.

d) The OFAC requirements are an important part of the United States' foreign policy and national security goals. Compliance programs should be designed to ensure prohibited transactions do not occur or are reported promptly if they should.

IV. Money Laundering & Bank Secrecy in the EU⁸

A. Money Laundering: the European perspective

1. In the European Union, the "why" and "how" of money laundering are essentially the same as in the U.S. (query: are crooks the same the world around?). Broadly speaking, it covers the handling of the proceeds of criminal activity and assisting or facilitating others to do so.
2. Given that the EU is composed of 25 sovereign countries, there is added focus on the cross-border nature of money laundering: "money laundering shall be regarded as such even where the activities...were carried out in the territory of...a third country". Third EU Money Laundering Directive
3. How extensive is money laundering? The IMF estimated in 1996 that money laundering could amount to between 2% and 5% of the world's GDP.
4. The Financial Action Task Force (FATF)⁹ is an international body of 31 governments and 2 regional governing authorities, based in Paris, whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing. The FATF issues legal and policy-based recommendations on fighting money laundering and terrorist financing, most recently updated in June 2003.
5. The FATF also issues a 'name and shame' list of "non-cooperative countries and territories". Twenty-three countries were initially on the list but the only country now listed is Myanmar. The following countries were recently removed from the NCCT list: Nigeria (removed June 2006), Cook Islands (removed October 2005), Indonesia (removed October 2005) and the Philippines (removed October 2005).

⁸ The 25 EU Member States are: Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, Netherlands, and United Kingdom. Romania and Bulgaria are scheduled to join the EU on January 1, 2007.

⁹ FATF members are: Argentina, Australia, Austria, Belgium, Brazil, Canada, Denmark, Finland, France, Germany, Greece, Hong Kong, Iceland, Ireland, Italy, Japan, Luxembourg, Mexico, Netherlands, New Zealand, Norway, Portugal, Russian Federation, Singapore, South Africa, Spain, Sweden, Switzerland, Turkey, United Kingdom, United States...AND the European Commission and the Gulf Cooperation Council.

B. AML regulation in the EU

1. Significant EU money laundering legislation.

- a) First EU Directive on money laundering was adopted in 1991 (91/308/EEC), then implemented into national legislation. It applied to financial institutions (defined to include insurance companies) and credit institutions and to EU branches of foreign financial institutions and credit institutions.
- b) First Directive was limited to the laundering of the proceeds of illegal drugs. It required (a) the identification of customers, evidence of which had to be retained for at least five years after the customer relationship ended, (b) the reporting of known or suspected money laundering transactions to national authorities and (c) the establishment of adequate control procedures and training.
- c) A second, amending Directive was adopted in 2001 (2001/97/EC) that expanded the scope beyond drugs money to the proceeds of any serious criminal activity including fraud. It extended the coverage of AML responsibilities to auditors, external accountants, tax advisors, external lawyers, notaries, firms giving financial advice, real estate agents and dealers in high value goods such as precious stones and works of art where payment is made in cash of a value of EUR 15,000 or more. Six EU countries failed to pass implementing legislation.
- d) AML and anti-terrorism legislation come together in the Third EU Money Laundering Directive (2005/60/EC), adopted in October 2005, which replaces the first and second directives. Significantly it adopts a risk-based approach to customer due diligence (explained below) in line with the FATF Recommendations.
- e) NOTE: Third Directive is to be adopted into national law by October 2007.

C. Who is affected by anti-money laundering regulations?

1. In the EU, AML regulations apply (subject to more stringent variations in local law) to:

- a) financial institutions (see the definition below) and EU branches of foreign financial institutions
- b) credit institutions (which are defined as deposit-taking and credit-granting institutions) and EU branches of foreign credit institutions
- c) auditors
- d) external accountants
- e) tax advisors
- f) lawyers in private practice and notaries
- g) firms giving financial advice

h) real estate agents

i) dealers in high value goods such as precious stones and works of art where payment is made in cash of a value of EUR 15,000 or more

j) trust and company service providers

k) and any natural or legal person trading in goods paid for in cash above EUR 15,000

l) casinos.

D. EU Definition of a "financial institution":

1. Institutions that engage in:

a) lending

b) financial leasing

c) money transmission services

d) issuing and administering means of payment (e.g., credit cards, traveller's cheques and bankers' drafts)

e) guarantees and commitments

f) trading for its own account or for the account of customers in (a) money market instruments, (b) foreign exchange, (c) financial futures and options, (d) exchange and interest rate instruments and (e) transferable securities

g) participation in securities issues and the provision of services related to such issues

h) advice to undertakings on capital structure, industrial strategy and related questions and advice as well as services relating to mergers and the purchase of undertakings

i) money brokering

j) portfolio management and advice

k) safekeeping and administration of securities

l) safe custody services

m) and also insurance companies authorized in accordance with EU Directive 2002/83/EC and EU branches of foreign insurance companies and certain insurance intermediaries

n) and also investment firms as defined in EU Directive 2004/39/EC and EU branches of foreign investment firms

o) and also collective investment schemes (i.e., European mutual funds) marketing their shares.

E. Specific AML and Know Your Customer (KYC) Requirements

1. In the EU, the Third Directive requires Member States to apply AML laws and regulations to the proceeds of any "serious

crime", which now includes offences punishable by six months or more in prison.

2. As implemented in the United Kingdom: Proceeds of Crime Act 2002 and Money Laundering Regulations 2003. Current money laundering offences are (a) assisting a money launderer (14 years in jail plus a fine), (b) acquiring, possessing or using the proceeds of crime (14 years in jail plus a fine), concealing or transferring illegal funds (14 years in jail plus a fine), (d) failure to report a suspicious transaction (5 years in jail plus a fine) and (e) notifying a customer that they are being investigated or have been reported (5 years in jail plus a fine).

a) In 2004 a lawyer in private practice became the first British lawyer convicted of failing to report suspicion of money laundering after his client deposited cash representing 2/3rds of the price of a new house.

F. Customer identification (KYC, also referred to as "customer due diligence" or CDD)

1. In line with the FATF Recommendations, the Third EU Directive gives guidelines to Member States that permit a risk-based approach to KYC "depending on the type of customer, business relationship or transaction".
2. KYC must include identifying the customer and verifying the customer's identity on the basis of documents, data or information from an independent and reliable source. Where the beneficial owner is shielded by a legal structure such as a company or trust, the beneficial owner must be identified and the ownership and control of the legal structure must be understood.
3. KYC must also include obtaining information on the purpose and intended nature of the business relationship.
4. The business relationship must be monitored on an ongoing basis to ensure that transactions are consistent with the customer's identity and the customer's business and risk profile. Where necessary, the source of funds must be identified.
5. All information held must be kept up to date.
6. Exceptions for "simplified customer due diligence": where the customer is itself an institution covered by the Third Directive or is located in a third country with "requirements equivalent to" the Directive, the KYC requirements do not apply.
7. Another exception: Member States may choose not to apply KYC requirements to listed companies whose securities are traded on regulated markets.
8. Another exception: Member States may choose not to apply KYC requirements to domestic government authorities.
9. Another exception: Member States may choose not to apply KYC requirements to life insurance policies with annual premiums below EUR 1,000.

10. Additional requirements for "enhanced customer due diligence": where the customer is not physically present for identification purposes, enhanced identification procedures are required.

11. Additional requirements for "enhanced customer due diligence": where the customer is a "politically exposed person" (defined below), senior management approval is required to establish a business relationship and the source of wealth and source of funds must be established.

G. Politically Exposed Persons.

1. More narrowly than U.S. law, the Third Directive defines politically exposed persons as "natural persons who are or have been entrusted with prominent public functions and immediate family members, or persons known to be close associates, of such persons".
2. Does a PEP ever stop being a PEP? The European Commission is debating this question, and is considering the position that a person no longer entrusted with prominent public functions for at least one year is no longer a PEP.
3. Further clarifications of the definition are also being considered.

H. Record Retention.

1. The record retention requirement for KYC and transaction-specific records is still five years from the end of the relationship or transaction. As with all EU Directives, Member States can impose longer requirements.
2. The United Kingdom has adopted the five year requirement. A summary of the U.K.'s record retention requirements is attached in the supplemental materials.

I. Reporting obligations and the prohibition of disclosure.

1. Each Member State is required by the Third Directive to establish a financial intelligence unit to receive, analyze and forward to the competent authorities information concerning potential money laundering or potential terrorist financing.
2. Institutions and persons covered by the Third Directive may not carry out transactions they know or suspect to be related to money laundering or terrorist financing until a report has been filed and any other locally required procedures have been completed.
3. No institution or person covered by the Third Directive may disclose to the customer concerned that a report has been filed or that an investigation is or may be carried out.

J. Suspicious Activity Reports (SARs): some UK issues.

1. The Serious Organised Crime Agency (SOCA) is the U.K.'s designated financial crimes intelligence unit. Total direct staff of 80.

2. Nearly 200,000 SARs were filed in 2005 (the U.K.'s population is 1/5th that of the U.S.). Banks and building societies filed 71%, accountants 7.5%, lawyers 5% and money transmission agents 5%.

3. Where permission to conclude a proposed transaction was required, consent was given in 92% of cases and the average response time was 3 days. For a customer awaiting a transfer of funds, three days can be a very long time to wait.

4. SARs can now be filed on-line. The paper forms are not simple to complete (samples are attached).

5. A March 2006 U.K. Government report found too much "defensive reporting of little value".

6. The U.K. regulations also require the appointment of a Money Laundering Reporting Officer, who must be a senior employee based in the U.K., must have sufficient resources including time and support staff, must be free to act on his own authority and must be approved by the regulator (the Financial Services Authority). The MLRO is to "consider" SARs before they are filed.

7. In cross-border transactions, a reporting obligation is likely to arise in multiple countries.

K. Training Obligations

1. The Third Directive requires that "relevant staff" be kept aware of the legal requirements surrounding money laundering and terrorist financing through training.

2. In the UK, all staff who handle or who are managerially responsible for transactions that may involve money laundering must receive training at least every 2 years.

L. International Trade Finance

1. The FATF recently issued a report on Trade Based Money Laundering (23 June 2006). This is "the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origins".

2. The report is attached in the supplemental materials.

3. Trade-based money laundering "represents an increasingly important money laundering and terrorist financing vulnerability".

4. Most common methods are the over- and under-invoicing of goods and services, multiple invoicing of goods and services, over- and under-shipment of goods and services and falsely described goods and services.

5. Red Flag Warnings.

a) The shipment does not make economic sense

b) The goods are trans-shipped through one or more jurisdictions for no apparent economic reason.

c) The size of the shipment appears inconsistent with the scale of the exporter or importer's regular business activities.

M. Information Sharing: Bank Secrecy and the EU Savings Tax Directive

1. Europe's recent battles over bank secrecy confirm there are strong feelings on both sides, while the FATF expresses concern that bank secrecy could inhibit the implementation of AML efforts.

2. After several years of difficult discussion, the EU adopted in 2003 the so-called Savings Tax Directive, 2003/48/ EC. The Directive took effect July 1, 2005 and requires banks in most EU countries to send customer names and information on saving income to the authorities in the customer's home country.

3. The discussions took years because Switzerland (not an EU Member State) and Luxembourg (a founding EU member) did not want to give up their cherished bank secrecy laws. When I worked in Luxembourg in the late 1990s, bank secrecy was considered a matter of public policy that could not be waived, even by a willing customer.

4. The compromise: Austria, Belgium and Luxembourg agreed for a "transitional period" to impose a withholding tax against income earned by EU residents, and to send 75% of that tax to the customers' home state, but not to identify the customers by name to their domestic tax authorities. Switzerland will do the same. The withholding rate is 15% for the first three years.

V. Supplemental Materials

FFIEC, Bank Secrecy Act/Anti-Money Laundering Examination Manual, 2006 (accessible at http://www.ffiec.gov/bsa_aml_infobase/default.htm)

Office of Foreign Assets Control (OFAC): <http://www.treas.gov/offices/enforcement/ofac/>

Financial Crimes Enforcement Network (FinCEN): <http://www.fincen.gov/>

3rd EU Money Laundering Directive, 2005/60/EC (copy attached)

FATF web site: www.fatf-gafi.org.

FATF "Trade Based Money Laundering", 23 June 2006 (copy attached).

Serious Organised Crime Agency, www.soca.gov.uk.

Sample Suspicious Activity Report (forms attached)

Savings Tax Directive, 2003/48/ EC (copy attached)

U.K.'s record retention requirements (copy attached)

Association of Corporate Counsel

Program 810: Bank Secrecy Act and Anti-Money Laundering Issues for All Corporations

Presented by:

Bruce Jay Baker

Eileen Lyon

Brian Mannion

Michael R. Nelson

ACC Annual Meeting

Hyatt Grand Manchester

San Diego, California

October 25, 2006

ANTI-MONEY LAUNDERING REGULATION IN THE UNITED STATES.....

What is money laundering? Why it is done?

How it is done?

- Placement
- Layering
- Integration

Who regulates money laundering and how?

- Agencies responsible for combating money laundering and terrorist financing.

Significant US money laundering legislation

- 1 0 - Bank Secrecy Act (31 USC 311 et seq., 12 USC §1 2 b, and §§1 1-1 and 31 USC §§ 311- 332) (“BSA”).....
- 1 6 - Money Laundering Control Act (“MLCA”).....
- 1 - Anti-Drug Abuse Act (“ADAA”).....
 - Aggregation.....
 - Recordkeeping.....
 - Reporting.....
- 1 2 - Annunzio-Wylie Anti-Money Laundering Act (“AWAMLA”).....
 - Suspicious activity reports (“SARs”).....
 - Timing.....
 - Confidentiality.....
 - Safe harbor.....
 - Record retention.....
 - Funds transfers.....
- 2001 - USA PATRIOT Act.....
 - Customer identification programs.....
 - Anti-money laundering programs.....

Who is affected by anti-money laundering regulations?

- Financial institutions.....
- Financial institutions’ customers.....
- Customers of Financial Institutions’ Customers.....

What are the potential impacts on customers?

- Red Flag Warnings
- Private Banking
- Money Services Businesses.....
 - What is a Money Services Business (“MSB”)?
 - Definition.....
 - Exclusions.....
 - Registration.....
 - MSBs and BSA recordkeeping and reporting requirements.....
 - MSBs as bank customers: what MSBs can expect
 - Significance of being a high risk MSB.....
 - FinCEN registration and state licensing failures
- Politically Exposed Persons (“PEPs”).....
- Customers Presenting Special Concerns.....
- Trade Finance
- Enhanced Due Diligence

Reporting of Cash Payments Over \$10,000 to a Trade or Business.....

- What is this requirement? Who must comply?

- Office Of Foreign Assets Control.....
- What is this requirement? Who must comply?.....
- How to Comply.....
- What Next.....

MONEY LAUNDERING & BANK SECRECY IN THE EU

Money Laundering: the European perspective

- AML regulation in the EU
- Significant EU money laundering legislation.....

Who is affected by anti-money laundering regulations?

Definition of a “financial institution”:

Specific AML and Know Your Customer (KYC) Requirements.....

Customer identification (KYC, also referred to as “customer due diligence” or CDD)

Politically Exposed Persons.....

Record Retention.....

Reporting obligations and the prohibition of disclosure.....

Suspicious Activity Reports (SARs): some UK issues.....

Training Obligations.....

- International Trade Finance.....
- Red Flag Warnings.....

Information Sharing: Bank Secrecy and the EU Savings Tax Directive.....

SUPPLEMENTAL MATERIALS.....

Anti-Money Laundering Regulation in the United States

What is money laundering? Why it is done?

The colloquial meaning of the term "money laundering" is the process of turning ill-gotten gains, "dirty" money, into "clean money" so that the funds appear to be the proceeds of legal activities. In essence, it is a means of hiding the illegal source of funds. It also serves to

- Facilitate tax evasion
- Convert a large sum of currency into more manageable assets
- Distance illegal proceeds from the crime for purposes of avoiding prosecution and seizure

How it is done?

The Federal Financial Institutions Examination Council (the "FFIEC"), comprised of the five federal banking agencies, breaks money laundering down into three steps, all of which can occur simultaneously: placement, layering, and integration.

Placement

The placement phase involves introducing unlawful proceeds into the financial system without attracting the attention of financial institutions or law enforcement. For example

- Dividing a large sum of money into smaller sums for deposit into one or more bank accounts so as to evade a bank's currency transaction reporting requirements (also known as "structuring")
- Commingling of currency derived from legal activity with currency derived from illegal activity

Layering

Layering involves moving funds around the financial system in an attempt to create confusion and complicate the paper trail. For example

- Exchanging monetary instruments, such as money orders, for larger or smaller amounts
- Wiring money to and from several accounts in one or more financial institutions

Integration

Final phase of money laundering, and the ultimate goal according to the FFIEC, is integration of the illegal funds "to create the appearance of legality." Additional transactions are engaged in at this stage to "further shield the criminal from a recorded connection to the funds by providing a plausible explanation for the source of the funds. For example, the purchase and resale of real estate, investment securities, foreign trusts, or other assets."

Who regulates money laundering and how?

Agencies responsible for combating money laundering and terrorist financing.

The U.S. General Accounting Office report entitled Combating Money Laundering: Opportunities Exist to Improve the National Strategy (GAO-03-13) includes the following summary of the roles and responsibilities of various federal agencies in the fight against money laundering and terrorist financing:

Agencies under the Departments of the Treasury, Justice, and Homeland Security [(DHS)] are to coordinate with each other and with financial regulators in combating money laundering.

Within Treasury, the Financial Crimes Enforcement Network (FinCEN) was established in 1990 to support law enforcement agencies by collecting, analyzing, and coordinating financial intelligence information to combat money laundering.

In addition to FinCEN, Treasury components actively involved in anti-money laundering and antiterrorist financing efforts include the Executive Office for Terrorist Financing and Financial Crimes, the Office of International Affairs, and the Internal Revenue Service and its Criminal Investigation unit (IRS-CI).¹

Department of Justice components involved in efforts to combat money laundering and terrorist financing include the Criminal Division's Asset Forfeiture and Money Laundering Section (AFMLS) and Counterterrorism Section, the Federal Bureau of Investigation (FBI), the Drug Enforcement Administration (DEA), and the Executive Office for U.S. Attorneys (EOUSA) and U.S. Attorneys Offices.²

With the creation of DHS in March 2003, anti-money laundering activities of the Customs Service were transferred from Treasury to DHS's Bureau of Immigration and Customs Enforcement (ICE).

The financial regulators who oversee financial institutions' anti-money laundering efforts include the depository institution financial regulators that constitute the FFIEC (Federal Reserve Board (FRB), FDIC, Office of the Comptroller of the Currency (OCC), Office of Thrift Supervision (OTS), and National Credit Union Administration (NCUA)), as well as the Securities and Exchange Commission (SEC), which regulates the securities markets, and the Commodity Futures Trading Commission (CFTC), which regulates commodity futures and options markets.

Significant US money laundering legislation.

1970 - Bank Secrecy Act (31 USC 311 et seq., 12 USC § 12 b, and §§ 1-1 and 31 USC §§ 311-332) ("BSA").

In order to aid in the identification of the source, volume, and movement of currency and other monetary instruments, the Act established recordkeeping and reporting requirements for

¹ Among other duties, Treasury's Executive Office for Terrorist Financing and Financial Crimes is charged with developing and implementing the NMLS (National Money Laundering Strategy) and U.S. government strategies to combat terrorist financing. These duties were previously conducted by Treasury's Office of Enforcement, which was disbanded in March 2003.

² Justice's Asset Forfeiture and Money Laundering Section (AFMLS) is the department's focal point for NMLS issues

individuals and financial institutions. The principal BSA reporting and recordkeeping requirements created were the following:

Currency Transaction Report ("CTR"). Financial institutions are required to file a CTR with the U.S. Department of the Treasury for each cash transaction (deposit, withdrawal, exchange or other payment or transfer) involving more than \$10,000.

Aggregation of currency transactions. Multiple currency transactions must be treated as a single transaction if the financial institution has knowledge that they are by or on behalf of the same person and result in either cash in or cash out totaling more than \$10,000 during any one business day. According to the FFIEC, "[b]anks are strongly encouraged to develop systems necessary to aggregate currency transactions throughout the bank."

For example, a bank should be able to aggregate the transactions conducted by one individual over the course of one business day conducted at all of its US branches. If the aggregate of the transactions is greater than \$10,000, a CTR must be filed.

In addition, transactions are not to be offset against one another: If there are both cash in and cash out transactions that are reportable, the amounts should be considered separately and not aggregated. However, they may be reported on a single CTR.

Examples. The following examples appear in the instructions section of the CTR (FinCEN Form 10):

- A person deposits \$11,000 in currency to his savings account and withdraws \$12,000 in currency from his checking account. The CTR should be completed as follows: Cash In \$11,000, Cash Out \$12,000. This is because there are two reportable transactions. However, one CTR may be filed to reflect both.
- A person deposits \$6,000 in currency to his savings account and withdraws \$,000 in currency from his checking account. Further, he presents \$,000 in currency to be exchanged for the equivalent in French Francs. The CTR should be completed as follows: Cash In \$11,000 and no entry for Cash Out. This is because in determining whether the transactions are reportable, the currency exchange is aggregated with each of the Cash In and Cash Out amounts. The result is a reportable \$11,000 Cash In transaction. The total Cash Out amount is \$,000, which does not meet the reporting threshold. Therefore, it is not entered on the CTR.

CTR exemptions. Certain types of financial institution customers are exempt from currency transaction reporting. They include a bank, to the extent of its domestic operations, a federal, state or local government agency or department, and any entity (other than a bank) whose common stock is listed on the New York, American, or Nasdaq stock exchanges (with some exceptions). A transaction account of a U.S. commercial enterprise also may be exempted if it has been maintained for at least 12 months and the business frequently engages in transactions in currency in excess of \$10,000. A "payroll customer's" transaction account also is exemptible if it has been maintained for at least 12 months, is owned by a U.S. commercial enterprise, and on a regular basis withdraws in excess of \$10,000 to pay its U.S. employees in currency. Financial institutions are required to file a Designation of Exempt Person form and undertake subsequent reviews and filings depending on the type of exempt entity involved.

Filing time frames and record retention requirements. A CTR must be filed within 1 days after the date of the transaction (2 days if filed magnetically or electronically). A copy of the CTR must be kept for years.

Report of International Transportation of Currency or Monetary Instruments ("CMIR"). A CMIR (FinCEN Form10) must be filed with the Bureau of Customs and Border Protection by a person or entity (1) who physically transports, mails, or ships currency or other monetary instruments in an aggregate amount exceeding \$10,000 at one time either into or out of the United States, or (2) who receives in the United States currency or other monetary instruments in an aggregate amount exceeding \$10,000 at one time which have been transported, mailed, or shipped to the person from any place outside the United States. There are numerous exemptions from this reporting requirement, including banks and securities brokers and dealers that mail or ship currency or monetary instruments through the postal service or by common carrier.

Report of Foreign Bank and Financial Accounts ("FBAR"). A FBAR must be filed with the Department of the Treasury by each United States person (an individual, partnership, corporation, estate or trust) who has a financial interest in, or signature or other authority over, any financial accounts, including bank, securities, or other types of financial accounts in a foreign country, if the aggregate value of these financial accounts exceeds \$10,000 at any time during the calendar year. Employees of banks and certain other U.S. corporations that maintain foreign financial accounts are exempt from the reporting, as long as they do not have a personal interest in the accounts.

Extensions of Credit and Currency Transfers????

1 6 - Money Laundering Control Act ("MLCA").

The MLCA, among other things, added a provision to the BSA prohibiting the "structuring" of transactions and established money laundering as a separate criminal offense.

Structuring. The BSA imposes criminal liability on a person or financial institution that structures transactions to avoid their reporting. Structuring a transaction includes, for example, breaking down a single sum of currency exceeding \$10,000 into smaller sums at or below \$10,000. The transactions need not exceed the \$10,000 reporting threshold at any single financial institution on any single day in order to constitute structuring.

Money laundering as a separate criminal offense. 1 U.S.C. §1 6(a)(1) establishes money laundering as a federal offense that carries with it a fine of up to \$ 00,000 or twice the value of the property involved, whichever is greater, and/or imprisonment for up to 20 years. Under the statute, it is a crime to conduct (or attempt to conduct) a financial transaction with the proceeds of "specified unlawful activity," knowing that the property involved comes from some form of unlawful activity with the intent to promote the carrying on of "specified unlawful activity" (defined in the statute to include a multitude of offenses such as bank robbery, murder, mail fraud, and even certain environmental crimes), with the intent to engage in tax evasion or the filing of false tax documents, knowing that the transaction is designed to conceal or disguise the nature, location, source, ownership, or control of the proceeds, or knowing that the transaction is designed to avoid a transaction reporting requirement under state or federal law.

Money laundering is not a continuing offense; each financial transaction constitutes a separate offense. "For example, a drug dealer who takes \$1 million in cash from a drug sale and divides the money into smaller lots and deposits it in 10 different banks (or in 10 different branches of the same bank) on the same day has committed 10 distinct violations of the new statute. If he then withdraws some of the money and uses it to purchase a boat or condominium, he will have committed two more violations, one for the withdrawal and one for the purchase." S. Rep. No. 33, th Cong. 2d Sess., at 12-13 (1 6) In addition, money laundering is a separate and distinct offense from the underlying criminal activity that resulted in the "dirty money" being "laundered."

1 - Anti-Drug Abuse Act ("ADAA").

The ADAA, among other anti-money laundering provisions, amended the BSA to require recordkeeping and reporting in connection with the purchase and sale of bank checks, cashier's checks, traveler's checks, and money orders for currency in amounts between \$3,000 and \$10,000, inclusive.

Purchaser verification. Financial institutions must verify the identity of a person purchasing monetary instruments for currency in amounts between \$3,000 and \$10,000. Financial institutions may either verify that the purchaser of monetary instruments is a deposit account holder with identifying information on record with the institution, or an institution may verify the identity of the purchaser by viewing a form of identification that contains the customer's name and address and that the financial community accepts as a means of identification when cashing checks for noncustomers. The financial institution must obtain additional information for purchasers who do not have deposit accounts.

Aggregation.

Multiple purchases during one business day totaling \$3,000 or more must be aggregated and treated as one purchase if the financial institution has knowledge that the purchases have occurred.

Recordkeeping.

The method used to verify the identity of the purchaser must be recorded. Additional information, such as the date of purchase, the type of monetary instruments purchased, including their serial numbers, and the amount in dollars of each of the instruments purchased, also must be recorded. Records must be retained by the financial institution for five years.

Reporting.

The Secretary of the Treasury is authorized to request a financial institution's monetary instrument purchase records at any time.

1 2 - Annunzio-Wylie Anti-Money Laundering Act ("AWAML").

The AWAML amended the BSA to require that financial institutions report "suspicious activity" and maintain records of certain funds transfers.

Suspicious activity reports ("SARs").

Financial institutions³ are required to file a SAR if (1) the transaction is conducted or attempted by, at or through the financial institution, (2) it involves funds or other assets of \$,000 (in general, \$2,000 in the case of money services businesses), and (3) the financial institution knows, suspects, or has reason to suspect that

- 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 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, or

- the transaction is designed to evade any requirements of the BSA, or
- 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 financial institution knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction, or
- in the case of financial institutions other than banks, the transaction involves use of the financial institution to facilitate criminal activity.

Timing.

A SAR must be filed within 30 calendar days after a financial institution detects the facts forming the basis for the filing. Except with respect to SARs filed by money services businesses, an additional 30 days may be tacked on for the identification of a suspect. In addition, ongoing suspicious activity should be reported at least every 0 days. Certain exigent situations also must be reported by telephone immediately.

Confidentiality.

A financial institution, and its directors, officers, employees and agents may not notify any person involved in a suspicious transaction that the transaction has been reported.

Safe harbor.

A financial institution, and its directors, officers, employees and agents, that make a disclosure of any possible violation of law or regulation, "shall not be liable to any person under any law or regulation of the United States, any constitution, law, or regulation of any State or political subdivision of any State, or under any contract or other legally enforceable agreement (including any arbitration agreement), for such disclosure or for any failure to provide notice of such disclosure to the person who is the subject of such disclosure or any other person identified in the disclosure".

Record retention.

Financial institutions are required to retain a copy of a SAR and supporting documentation for five years.

Funds transfers.

Each financial institution involved in a funds transfer of \$3,000 or more is required to collect and retain certain information in connection with the transfer. There are various exceptions to the funds transfer requirements, where, for example, the originator and beneficiary are: a bank, a wholly owned domestic subsidiary of a bank chartered in the United States, a broker or dealer in securities, a wholly owned domestic subsidiary of a broker or dealer in securities, the United States, a state or local government, or a federal, state or local government agency or instrumentality.

The information required to be collected and retained depends on the financial institution's role in the particular funds transfer (originator, intermediary, or beneficiary institution). The

³ Financial institutions also are subject to additional SAR filing requirements under regulations promulgated by the five federal banking supervisory agencies. For example, a bank must file a SAR if it has a substantial basis for identifying an insider in connection with a criminal activity, regardless of the dollar amount involved in the transaction.

requirements also may vary depending on whether an established customer of a financial institution is involved and whether a payment order is made in person.

Under what is known as the "Travel Rule," financial institutions are required to include certain information in the transmittal order, including the names and addresses of the transmitter and, to the extent known, the recipient.

2001 - USA PATRIOT Act.

Among other provisions, the USA PATRIOT Act required the Secretary of the Treasury and the federal financial regulators to promulgate regulations for a financial institution's identification of its customers prior to opening accounts. The Act also mandated that all financial institutions implement an anti-money laundering program.

Customer identification programs.

The USA PATRIOT Act required that financial institutions implement reasonable procedures for

- verifying the identity of any person seeking to open an account to the extent reasonable and practicable,
- maintaining records of the information used to verify a person's identity, including name, address, and other identifying information, and
- consulting lists of known or suspected terrorists or terrorist organizations provided to the financial institution by any government agency to determine whether a person seeking to open an account appears on any such list.

A financial institution's customer identification program must be "risk based," meaning that it must be tailored to address the risks presented by the institution's size, location, customer base, product offerings, and account opening procedures, for example. However, the applicable regulations require that financial institutions obtain certain minimum identification information, including a customer's name, address, date of birth (if applicable), and, subject to certain exceptions, a taxpayer identification number or government-issued document if the customer is not a "U.S. person." In addition, financial institutions must have procedures in place for the documentary or non-documentary verification of the identifying information provided by customers, and also must maintain records of the information obtained in connection with the verification procedures.

Anti-money laundering programs.

Prior to the USA PATRIOT Act, only banking organizations and casinos were required to establish an anti-money laundering program. The Act expanded this requirement to include all financial institutions⁴ and provided that, at a minimum, an anti-money laundering program must include the following four "touchstones":

- the development of internal policies, procedures, and controls,
- the designation of a compliance officer,
- an ongoing employee training program, and
- an independent audit function to test programs.

⁴ However, as of July 2006, only certain types of financial institutions are subject to final rules implementing the anti-money laundering program requirements established by the USA PATRIOT Act.

Who is affected by anti-money laundering regulations?

Financial institutions.

Financial institutions are on the front line of anti-money laundering regulations. Through enactment of various laws since 1970, financial institutions have been required to develop and implement programs that are reasonably designed to detect and deter money laundering and terrorist financing activities. Financial institutions are not expected to ascertain whether an underlying crime has actually been committed. That is the job of law enforcement; financial institutions are merely required to report suspicious activities.

The systems financial institutions are required to develop should be risk based; that is, the financial institutions are required to evaluate the risk within their institution's products, services customers, and geographic locations. Some factors will be weighted more heavily than others. In general, however, a large international bank with a multitude of products, particularly those that facilitate the movement of money across borders, will be expected to have a significantly more robust BSA program than a small community savings and loan with traditional mortgage and deposit products.

The BSA defines the term "financial institution" as follows:

- (A) an insured bank (as defined in section 3(h) of the Federal Deposit Insurance Act (12 U.S.C. 1813(h)));
- (B) a commercial bank or trust company;
- (C) a private banker;
- (D) an agency or branch of a foreign bank in the United States;
- (E) any credit union;
- (F) a thrift institution;
- (G) a broker or dealer registered with the Securities and Exchange Commission under the Securities Exchange Act of 1934 (15 U.S.C. 77a et seq.);
- (H) a broker or dealer in securities or commodities;
- (I) an investment banker or investment company;
- (J) a currency exchange;
- (K) an issuer, redeemer, or cashier of travelers' checks, checks, money orders, or similar instruments;
- (L) an operator of a credit card system;
- (M) an insurance company;
- (N) a dealer in precious metals, stones, or jewels;
- (O) a pawnbroker;

(P) a loan or finance company;

(Q) a travel agency;

(R) a licensed sender of money or any other person who engages as a business in the transmission of funds, including any person who engages as a business in an informal money transfer system or any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside of the conventional financial institutions system;

(S) a telegraph company;

(T) a business engaged in vehicle sales, including automobile, airplane, and boat sales;

(U) persons involved in real estate closings and settlements;

(V) the United States Postal Service;

(W) an agency of the United States Government or of a State or local government carrying out a duty or power of a business described in this paragraph;

(X) a casino, gambling casino, or gaming establishment with an annual gaming revenue of more than \$1,000,000 which—

(i) is licensed as a casino, gambling casino, or gaming establishment under the laws of any State or any political subdivision of any State; or

(ii) is an Indian gaming operation conducted under or pursuant to the Indian Gaming Regulatory Act other than an operation which is limited to class I gaming (as defined in section (6) of such Act);

(Y) any business or agency which engages in any activity which the Secretary of the Treasury determines, by regulation, to be an activity which is similar to, related to, or a substitute for any activity in which any business described in this paragraph is authorized to engage; or

(Z) any other business designated by the Secretary whose cash transactions have a high degree of usefulness in criminal, tax, or regulatory matters.

(C) **Additional Definitions.**— For purposes of this subchapter, the following definitions shall apply:

(1) **Certain institutions included in definition.**—The term “financial institution” (as defined in subsection (a)) includes the following:

(A) Any futures commission merchant, commodity trading advisor, or commodity pool operator registered, or required to register, under the Commodity Exchange Act.

Given the expansive definition of “financial institution,” the potential reach of BSA recordkeeping and reporting requirements is extensive. However, final rules implementing the BSA requirements have not been issued for many of the entities covered by the Act. For example, although the Secretary of the Treasury is authorized to require that all domestic

financial institutions perform currency transaction reporting under the BSA (31 U.S.C. § 313), to date the regulations implementing these reporting requirements apply only to banks, brokers or dealers in securities, money services businesses, telegraph companies, persons subject to supervision by any state or federal bank supervisory authority, futures commission merchants, introducing brokers in commodities, casinos, and card clubs.

Financial institutions' customers

The recordkeeping and reporting requirements established by the BSA impact a financial institution's policies and procedures as well as those of its customers.

Customers of Financial Institutions' Customers.

Because financial institutions must be increasingly vigilant in monitoring their customers' activities, by extension customers of financial institutions need to be prepared to answer questions about the nature of their customers.

If a business customer of a bank is found to be involved in check cashing, for example, the financial institution may need to treat a customer as a money services business. Once a potential money services business is identified, a financial institution may need to request additional information from the customer concerning its compliance with federal and state registration requirements that need to be satisfied. Should the customer then refuse or fail to register as a money services business it may find that the financial institution is reluctant to maintain a relationship with the business. All businesses (and particularly money services businesses) should be prepared to provide this information to its banking organization when seeking to open an account or when requested to do so by its banking organization for purposes of maintaining an existing account relationship. Otherwise, the bank may feel uncomfortable about the relationship and request that the account be closed.

What are the potential impacts on customers?

As discussed, financial institutions have a legislative and regulatory mandate to monitor their customers' accounts for suspicious activities in order to detect and deter money laundering and terrorist financing.

Although generally speaking, banking regulators will not require an institution to close an account, banking organizations are required to take steps to determine for themselves whether to open or maintain an account for business. This will involve obtaining basic identifying information and conducting a basic risk assessment to determine the level of risk associated with the account and to solicit additional information, as deemed necessary. The extent to which a banking organization will seek additional information will be dictated by the banking organization's assessment of the level of risk posed by the individual customer. Not all businesses pose the same level of risk, and that not all businesses will always require additional due diligence. In some cases, the amount of additional customer due diligence performed by a banking organization will be negligible. In other situations, the additional due diligence performed will be extensive.

At the same time, bank customers have a natural and legitimate interest in maintaining the privacy of their financial information. Frequently, customers are not aware that this desire for secrecy may be viewed as a possible “red flag” necessitating further investigation by their financial institution and/or the filing of a SAR.

Businesses that are reluctant to provide such information will find it harder to maintain or open bank accounts in future, as the institutions become more familiar with the risks of noncompliance with regulatory mandates for an effective BSA/AML program.

Red Flag Warnings

Some red flags identified by the regulators that have been adopted by your financial institution include the following:

- Customers who provide insufficient or suspicious information about their identity, corporate ownership, business activities or expected transaction activity.
- A customer's background differs from that which would be expected on the basis of his or her business activities.
- A customer who makes frequent or large transactions and has no record of past or present employment experience.
- Customers who are reluctant to provide information, particularly if the customer is a company and the information sought is about controlling parties or beneficial owners.
- Customers who try to avoid reporting or recordkeeping requirement (i.e., "structuring").
- Unexplained funds transfers, particularly those sent in large, round dollar amounts or which occur to or from an offshore corporate haven or high-risk geographic location without an apparent business reason or when the activity is inconsistent with the customer's business or history.
- Activities that are inconsistent with the stated purpose or anticipated activities given when opening the account.
- Unusual patterns of activity, particularly those involving currency or currency substitutes (money orders, stored value cards) that are atypical or inconsistent with past practices.

Private Banking

The Federal Reserve has long recognized that private banking is vulnerable to money laundering activities. Consequently, it is not surprising that private banking activities have come within the scope of the BSA and regulations. Under the USA Patriot Act, the Banking agencies were required to establish regulations that provide for due diligence for private banking accounts for non-U.S. persons, and enhanced scrutiny of "senior foreign political figures."

Broadly speaking, private banking is the provision of a wide variety of financial services targeted to high net worth individuals and their related businesses, typically through a relationship manager who develops and maintains strong ties to the customer and provides him or her with a high degree of personalized service.

Frequently, private banking involves money management services, including:

- investment portfolio management,
- financial planning,
- custodial services,
- funds transfer,
- lending,

- overdraft privileges,
- letter-of-credit financing and
- bill payment.

Private banking is very competitive among financial institutions, and almost always involves a high degree of confidentiality. Although usually customers have legitimate reasons for desiring confidentiality, these attributes make private banking susceptible to the elements of money laundering: placement, layering and integration.

Under the BSA, covered financial institutions are required to develop processes and systems for monitoring the risks associated with private banking accounts maintained for non-U.S. persons. A "covered financial institution" is:

- Insured banks
- Insured savings associations
- Insured credit unions
- Agencies and branches of foreign banks
- Securities broker-dealers
- Futures commission merchants
- Introducing brokers
- Mutual funds

However, MSBs, casinos, operators of credit card systems and foreign branches of U.S. banks are not subject to this rule.

A "private banking account", is defined as an account (or any combination of accounts) maintained at a bank that satisfies all three of the following criteria:

- Requires a minimum aggregate deposit of funds or other assets of not less than \$1,000,000.
- Is established on behalf of or for the benefit of one or more non-U.S. persons who are direct or beneficial owners of the account, and
- Is assigned to, or is administered by, in whole or in part, an officer, employee, or agent of a bank acting as a liaison between a financial institution covered by the regulation and the direct or beneficial owner of the account.

Many financial institutions offer services that are generically termed private banking, but do not require a minimum deposit of at least \$1,000,000. Although these relationships are not subject to the expanded requirements under the BSA for "private banking accounts", they nevertheless will be subject to a greater level of due diligence under the bank's risk-based BSA/AML compliance program.

For private banking accounts that fall within the definition, the bank is responsible to have a process whereby the bank:

- Determines identity of nominal and beneficial owner of any private banking account
- Determines if owner is a senior foreign political figure (also termed a "politically exposed person" or "PEP").

- Determines source(s) of funds deposited into a private banking account, purpose and expected use of the account.
- Reviews account activity to ensure that it is consistent with the information obtained about the client's source of funds, and with the stated purpose and expected use of the account, and
- Files Suspicious Activity Report (SAR), as appropriate, to report any known or suspected money laundering or suspicious activity conducted to, from, or through a private banking account.

Money Services Businesses

What is a Money Services Business ("MSB")?

In general. According to the Financial Crimes Enforcement Network ("FinCEN"), "MSBs provide valuable financial services, especially to those who may not have ready access to the banking sector. The MSB industry is quite diverse, ranging from large Fortune 500 companies with global presence to small "mom-and-pop" convenience stores in ethnic neighborhoods where English may rarely be spoken. Moreover, given the types of the products and services provided and the distribution channels, some participants in this industry sector may be at greater risk for misuse by terrorist financiers, money launderers, and other criminals. Consequently, [FinCEN] believe[s] that it is vital to identify and reduce the number of unregistered MSBs in order to better focus resources to encourage increased compliance with the BSA's programmatic, recordkeeping, and reporting requirements."

Definition.

An MSB is each agent, agency, branch, or office within the United States of any person doing business, whether or not on a regular basis or as an organized business concern, in one or more of the following capacities:

- Currency dealers or exchangers
- Check cashers
- Issuers of traveler's checks, money orders, or stored value
- Sellers or redeemers of traveler's checks, money orders, or stored value
- Money transmitters
- The United States Postal Service (except with respect to the sale of postage or philatelic products)

A business in one of the first four categories that engages in transactions "in an amount greater than \$1,000 in currency or monetary or other instruments for any person on any day in one or more transactions" is considered to be an MSB (although there is no dollar threshold for money transmitters). 31 C.F.R. §103.11(uu). FinCEN has stated, however, that "if an entity crosses the \$1,000 MSB definitional threshold on a one-time basis, that one-time action, if not repeated, does not cause the entity to become an MSB."

Exclusions.

Banks, savings and loans, credit unions, and persons registered with, and regulated or examined by, the Securities and Exchange Commission or the Commodity Futures Trading Commission, are not MSBs.

Registration.

MSBs (irrespective of whether they are required to be licensed by a State) must register with the Department of the Treasury (31 C.F.R. §103. 1), except for:

- The United States Postal Service
- A branch office of an MSB
- Agencies of the United States, of any State, or of any political subdivision of a State
- An issuer, seller, or redeemer of stored value
- A person that is an MSB solely because it acts as an agent for another MSB.

For example, a grocery store that acts as an agent for an issuer of money orders and performs no other services that would cause it to be a money services business is not required to register. However, registration would be required if the grocery store, in addition to acting as an agent of an issuer of money orders, also cashed checks or exchanged currencies (other than as an agent for another business) in an amount greater than \$1,000 in currency or monetary or other instruments for any person on any day, in one or more transactions.

An MSB that is required to register with FinCEN has 10 days in which to register from the time that it begins conducting business. Ignorance of the law is no defense for an MSB not registering—simply operating an MSB that is required to register but has failed to do so is sufficient to trigger severe penalties for the MSB under the USA PATRIOT Act. A list of registered MSBs is posted on FinCEN's website. As of October 2006, only one out of ten of all MSBs had registered with FinCEN as required by federal law. (Statement of Julie L. Williams, Acting Comptroller of the Currency, before the Committee on Banking, Housing, and Urban Affairs United States Senate, April 26, 2006.) FinCEN's new August 2006 list, which was current as of August 3, 2006, contains data on 26,111 registered MSBs.

MSBs and BSA recordkeeping and reporting requirements.

In addition to the requirement to register with FinCEN, MSBs, with limited exceptions, also are subject to the recordkeeping and reporting requirements of the Bank Secrecy Act. For example, an MSB must have an anti-money laundering program, and it is subject to large currency transaction reporting and suspicious activity reporting requirements, among other requirements.

MSBs as bank customers: what MSBs can expect.

Background.

The Federal Financial Institutions Examination Council ("FFIEC") (which is comprised of one representative respectively from the Board of Governors of the Federal Reserve System, the

Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and Office of Thrift Supervision) issued an "Interagency Interpretive Guidance on Providing Banking Services to Money Services Businesses Operating in the United States" on April 26, 200 (the "Guidance"). The Guidance was meant to reassure banks that they are not expected to be the de facto regulators of MSBs and will not be held responsible for their customers' compliance with the BSA and other applicable federal and state laws and regulations. Nevertheless, the Guidance clarified certain minimum due diligence expectations for banks when opening or maintaining accounts for MSBs.

Minimum due diligence.

An MSB can expect that a financial institution will undertake the following minimum due diligence steps when opening or maintaining its account:

Apply its Customer Identification Program (commonly referred to as a "CIP")

- Confirm the customer's FinCEN registration, if required
- Confirm the customer's state licensing status, if applicable
- Confirm the customer's agent status, if applicable
- Conduct a risk assessment to determine the level of risk associated with each account of the customer and whether further due diligence is required

Risk assessment.

Not all MSBs pose the same level of risk for money laundering and other illegal activities. For example, a local grocery store that cashes paychecks for neighborhood customers poses less risk than a currency exchange that cashes checks for customers spread over a large metropolitan area. The level of a financial institution's scrutiny of an MSB should reflect the level of risk that it presents. This means that a financial institution may need to obtain additional information from an MSB that falls into a higher risk category.

Basic considerations.

When performing this basic risk assessment, financial institutions will consider, at a minimum:

- the types of products and services offered by an MSB
- the locations and markets served by the MSB
- the types of banking account services needed by the MSB
- the purpose of each bank account

"Risk indicators."

The FFIEC Guidance lists two sets of "risk indicators" that financial institutions can use as checklists: one set represents a low level of risk, and the other represents a higher level of risk. An example of a low risk indicator would be that the MSB primarily markets to customers that conduct routine transactions with moderate frequency in low amounts. A high risk indicator may be that the MSB has failed to obtain proper state licensing, or it allows its customers to conduct higher transactional amounts with moderate to high frequency. The final determination of the level of risk posed by an MSB is always a judgment call to be made by the financial institution.

Significance of being a high risk MSB.

Once a financial institution has identified an MSB as a high risk customer, the FFIEC Guidance suggests seven extra due diligence steps that a financial institution may need to take. These include:

- making an on-site visit to the MSB
- reviewing the MSB's own anti-money laundering program
- reviewing the MSB's employee screening practices
- reviewing lists of the MSB's agents and locations in and outside of the United States that receive services through the MSB's bank account
- reviewing the MSB's procedures for its operations
- reviewing results of the MSB's independent testing of its anti-money laundering program
- reviewing written agent management and termination practices for the money services business

Some or all of these additional steps should be conducted based on the "level of perceived risk, and the size and sophistication" of the particular MSB, which the Guidance suggests may change over the course of the MSB's relationship with the financial institution.

FinCEN registration and state licensing failures

One of the BSA compliance challenges confronting financial institutions today is the extent to which they need to inquire about a customer's activities in order to determine whether the customer must be registered with FinCEN and/or licensed by a state authority. MSBs registered with FinCEN may or may not need to be licensed in the state where they are conducting business. Likewise, a non-financial institution that requires licensure under state law may not be an MSB subject to registration under federal laws and regulations. This can make for complicated account opening and monitoring procedures. Most financial institutions will make certain inquiries at account opening and conduct ongoing account monitoring to uncover activities such as check cashing that may require registration and licensure. One thing is clear, however, and that is that if a financial institution determines that its customer should be registered with FinCEN or licensed by the state, a failure on the part of the customer to be registered or licensed will result in the financial institution's filing of a suspicious activity report on the customer under 31 C.F.R. §103.1 !

Politically Exposed Persons ("PEPs")

With respect to PEPs, covered institutions are required to monitor the accounts to guard against accepting the proceeds of official foreign corruption. "Proceeds of foreign corruption" means any assets or property that is acquired by, through, or on behalf of a PEP through misappropriation, theft, or embezzlement of public funds, the unlawful conversion of property of a foreign government, or through acts of bribery or extortion, and includes any other property into which any such assets have been transformed or converted. (31 CFR 103.1 (c)(2)).

- A senior foreign political figure, or PEP, includes the following:
- A current or former:

- Senior official in the executive, legislative, administrative, military, or judicial branches of a foreign government (whether elected or not).
- Senior official of a major foreign political party.
- Senior executive of a foreign-government-owned commercial enterprise.
- A corporation, business, or other entity that has been formed by, or for the benefit of, any such individual.
- An immediate family member (including spouses, parents, siblings, children, and a spouse's parents and siblings) of any such individual.
- A person who is widely and publicly known (or is actually known by the relevant bank) to be a close associate of such individual.

Financial institutions are expected to identify PEPs by inquiring about present and past employment, reviewing public databases that are reasonably available, and reviewing government lists, newspapers and public reports regarding foreign figures and their associates.

Customers Presenting Special Concerns

Certain customers, by their nature, present additional risks to banks and financial institutions for money laundering. These include the following:

- Nonresident Aliens and Foreign Individuals
- Politically Exposed Persons
- Embassy and Foreign Consulate Accounts
- Non-Bank Financial Institutions
- Professional Service Providers
- Non-Governmental Organizations and Charities
- Certain Business Entities, such as shell corporations, international business corporations (i.e., companies that are formed outside a person's country of residence) and private investment companies, especially those opened in offshore financial centers.
- Cash-Intensive Businesses, such as
 - Convenience stores,
 - Restaurants,
 - Retail stores,
 - Liquor stores,
 - Cigarette distributors,
 - Privately owned automated teller machines (ATMs),
 - Vending machine operators and
 - Parking garages.

Trade Finance

Trade finance typically involves short-term financing to facilitate the import and export of goods. Companies on both sides of the trade desire financial institutions' involvement in trade

finance in order to minimize payment risk. However, because trade finance activities involve multiple parties on both sides of the transaction, the process of due diligence becomes more difficult. Also, since trade finance can be more document-based than other banking activities, it can be susceptible to documentary fraud, which can be linked to money laundering, terrorist financing, or the circumvention of OFAC sanctions or other prohibitions.

Trade in weapons or nuclear equipment are obviously high risk for terrorist activity, but financial institutions also need to be concerned about goods that may be over- or under-valued in an effort to evade AML or customs regulations.

Example: An importer pays a large sum of money from the proceeds of an illegal activity for goods that are essentially worthless and are subsequently discarded.

Example: Trade documents, such as invoices, are fraudulently altered to hide the scheme. Variations on this theme include double invoicing, partial shipment of goods, and the use of fictitious goods. Illegal proceeds transferred in such transactions thereby appear sanitized and enter the realm of legitimate commerce.

Example: Third-party nominees, such as shell companies, are substituted to disguise an individual's or company's role in a trade finance agreement. This substitution results in a lack of transparency, effectively hiding the identity of the purchasing party, thus increasing the risk of money laundering activity.

Financial institutions involved in trade finance activities are expected to have an understanding of the customer's underlying business and locations served. This may require background checks or investigations, particularly in higher risk jurisdictions and to carefully review documentation, not only for compliance with the terms of the letter of credit, but also for anomalies or red flags that could indicate unusual or suspicious activity. In some circumstances, stopping the trade may be required to avoid a potential violation of an OFAC sanction.

In addition to OFAC filtering, the bank is likely to scrutinize:

- Items shipped that are inconsistent with the nature of the customer's business (e.g., a steel company that starts dealing in paper products, or an information technology company that starts dealing in bulk pharmaceuticals).
- Customers conducting business in high-risk jurisdictions.
- Customers shipping items through high-risk jurisdictions, including transit through non-cooperative countries.
- Customers involved in potentially high-risk activities (e.g., dealers in weapons, nuclear materials, chemicals, precious gems; or certain natural resources such as metals, ore, and crude oil).
- Obvious over- or under-pricing of goods and services (e.g., importer pays \$ 00 an item for one shipment and \$ 0 for an identical item in the next shipment; exporter charges one customer \$100 per item and another customer \$ 00 for an identical item in the same week).
- Excessively amended letters of credit without reasonable justification.
- Transactions evidently designed to evade legal restrictions, including evasion of necessary government licensing requirements.

Enhanced Due Diligence

Depending on the institution and the sophistication of its BSA/AML program, you may find that your bank is no longer willing to do business with you, or will only do business on certain conditions. Typically, these involve enhanced due diligence, by which the institution will seek to understand or obtain the following information:

Type of Customer	Additional Scrutiny May Involve
Nonresident Aliens	<p>The accountholder's home country</p> <p>The types of products and services used.</p> <p>Forms of identification.</p> <p>Sources of wealth and funds.</p> <p>Unusual account activity.</p>
Politically exposed persons	<p>Identity of the accountholder and beneficial owner.</p> <p>Asking directly about possible PEP status.</p> <p>Identity of the accountholder's country of residence.</p> <p>Employment or other sources of funds.</p> <p>Checking references, as appropriate, to determine whether the individual is or has been a PEP.</p> <p>Identifying the source of wealth.</p> <p>Obtaining information on immediate family members or close associates having transaction authority over the account.</p> <p>Determining the purpose of the account and the expected volume and nature of account activity.</p> <p>Reviewing public sources of information.</p>

Type of Customer

Offshore corporations

NGOs and charitable organizations

Additional Scrutiny May Involve

Determining the beneficial ownership of the corporation

Understanding interlocking relationships between affiliated corporations

If corporation is organized in tax haven jurisdiction, will need to understand sources of wealth and income, and intended purpose of account

If shares are held in bearer form, requiring amendments to charter to make registered form; alternatively, the bank will seek to hold shares in trust.

Purpose and objectives of their stated activities.

The geographic locations served (including headquarters and operational areas).

Organizational structure.

Donor and volunteer base.

Funding and disbursement criteria (including basic beneficiary information).

Recordkeeping requirements.

Its affiliation with other NGOs, governments, or groups.

Internal controls and audits.

Information regarding principals, directors or officers.

Obtaining and reviewing the financial statements and audits.

Verifying the source and use of funds.

Evaluating large contributors or grantors of the NGO.

Conducting reference checks.

Type of Customer	Additional Scrutiny May Involve
Cash intensive businesses	Understand customer's business operations, such as intended use of the account; including anticipated transaction volume, products, and services used;
	Geographic locations involved in the business.
Privately owned ATMs	Payment system utilized, including sponsoring institution
	Corporate documentation, licenses, permits, contracts and references to verify an independent sales organization's ("ISO's") legitimacy.
	Controls over the currency servicing arrangements
	Understanding currency generation of the associated business.
	Locations of privately owned ATMs
	ISO's target geographic market.
	Expected account activity, including expected currency withdrawals.

- Cash is defined as coin and currency (both US and foreign). It also includes other items not normally thought of as "cash." For example, cashier's checks, bank drafts, treasurer's checks, and money orders all are considered cash. Further, a qualifying monetary instrument must have a face amount of \$10,000 or less, and the trade or business must receive the item in a designated reporting transaction or any transaction in which you know the payer is trying to avoid the reporting requirement. Cash does not include personal checks drawn on an individuals account.
- A designated reporting transaction is defined to include the retail sale of a consumer durable (e.g. automobile or boat), a collectible (e.g. art, rug, metal, gem, etc.), or travel and entertainment.

As you can see, these regulations are fact specific and require an analysis of the type of business involved, the type and amount of the monetary instrument, and type of transaction. Lastly, the IRS regulation requires notice be sent to the subject of the Form 300 report. This notice must include a contact person at the trade or business, and the total amount of the cash that was reported on the Form 300. This notice must be sent to the subject by January 31 of the year following the calendar year for which the report was filed.

Additionally, some businesses subject to these regulations must also comply with the suspicious activity reporting obligations found in the Bank Secrecy Act. While the reports may appear to be duplicative, the Department of Treasury has made it clear that the two regulatory schemes are different and must be complied with separately (see 1 FR 2621 (May , 2006)). Further, the filing of a Form 300 and the subsequent notice that must be sent to the customer must not alert the customer that a suspicious activity report was or will be filed. Suspicious activity reports are required to be kept confidential.

Office Of Foreign Assets Control

What is this requirement? Who must comply?

The Office of Foreign Assets Control, or OFAC, administers and enforces the economic sanctions authorized by the Congress or the President. These sanctions and embargo programs are designed to utilize the US's economic power to further its foreign policy and national security interests by targeting foreign countries, terrorists, international narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction. The regulations apply to all United States persons, certain foreign persons living in the United States, and for certain sanctions programs, foreign subsidiaries of United States persons.

OFAC administers two general types of programs. The first are economic sanctions against particular countries. These are commonly referred to as sanctions programs and include countries such as Cuba, Iran, North Korea, and Sudan, as well as programs targeted at terrorists and weapons of mass destruction. Each sanctions program is different since they are designed to achieve a specific foreign policy objective that varies from program to program.

The second type of program is the Specially Designated Nationals list, or SDN. While the country sanctions may apply to all transactions associated with the government of Cuba, the SDN list specifically identifies an entity that US persons may not "do business with." SDNs typically include terrorist groups, Columbian drug lords, charities that provide funding to terrorists, and other persons that the US government wishes to specifically place economic sanctions upon.

Reporting of Cash Payments Over \$10,000 to a Trade or Business

What is this requirement? Who must comply?

Any person in a trade or business who receives more than \$10,000 in cash in a single transaction or in related transactions must file with the Internal Revenue Service ("IRS") Form 300. The IRS and the Department of Treasury both have similar requirements regarding the filing of Form 300. The IRS requirements can be found at 26 USCS 60 01, and at 31 USC 331 for the Department of Treasury, which was added by section 36 of the USA PATRIOT Act. Both agencies have also promulgated regulations that provide further guidance. The IRS has provided additional guidance through Publication 1 . Generally, if you comply with the IRS requirements then you also are complying with the Department of Treasury regulations.

The report is designed to create a record of cash transactions that can be used by law enforcement to track down and arrest drug dealers, terrorist financiers, and other money launderers. These types of reports are critical to law enforcements efforts and allow the tracking of large transactions using cash or certain types of monetary instruments. Some of the key definitions associated with the filing of Form 300 include:

- The definition of person is very broad and includes individuals, companies, partnerships, associations, trusts, and estates.
- Banks and broker/dealers do not have to comply with this requirement because they are obligated to file Currency Transactions Reports.

The OFAC SDN list is updated regularly as a result of law enforcement investigations or Presidential actions. For example, shortly after the attacks of /11 the President, utilizing his statutory authority, issued an executive order seizing the property of the suspected terrorists. Upon issuance of this executive order, all US persons were expected to comply with the requirements of the executive order.

- OFAC and BSA are different legal obligations. They are based on different statutes and serve different public policy purposes. Most importantly, these laws apply to different constituencies – OFAC applies to almost every US person, while BSA only applies to certain financial institutions. However, there is overlap between the two requirements and are often times considered together. One reason for this treatment is that the OFAC SDN list contains names of terrorists and drug dealers. These are the types of entities that your BSA program is supposed to identify and report to the government. A solid OFAC compliance program will buttress your BSA compliance efforts.

How to Comply

Each of the twenty-some sanctions programs and several thousand SDNs vary in the extent and scope of the prohibited transactions. Generally, businesses must determine how it will build a compliance program. For example, are the company's transactions geographically narrow or do they involve several states or even international matters? Will the company purchase technology that ensures all transactions are scanned against the SDN list? What are the expectations of the company's primary regulator? Lastly, will the company analysis each and every sanctions program in order to determine if it applies to the company, or will it take a more generic approach whereby it will limit business with anyone on the SDN list or in any sanctioned country.

- Generally, the OFAC regulations do not specifically require the checking of the OFAC SDN list or country sanctions list. But, if a prohibited transaction occurs with entities on either list, then you will probably violated OFAC regulations and likely incur both a fine and potential reputational harm as well. OFAC fines are published on the OFAC website.
- Each business needs to understand its customers and the likelihood of performing transactions with prohibited entities. For example, a convenience store in Iowa is likely not implementing a robust OFAC compliance program, as it is not doing business with anyone on the lists. On the other hand, a major league baseball team wishing to sign a new prospect out of Cuba will need to thoroughly understand the OFAC sanctions programs.

Once the company has determined its OFAC risks, it should then implement a compliance program. A leading practice is to identify a compliance officer that will be responsible for establishing and managing the program on a day-to-day basis. Corporate wide policies and procedures regarding controls should be written. Business leaders should be directly assigned responsibilities. Employees should receive regular training about OFAC and the company's policies, with increased training for those employees that are integral to your compliance efforts. Lastly, the OFAC compliance program should be periodically evaluated to ensure it is being followed, as well as identify any aspects that could be enhanced.

What Next

Now that the company has determined its OFAC risk and created a compliance program, the next step is to compare your transactions against the SDN list and the list of embargoed or blocked countries. Technology solutions can provide significant value to this process.

Regardless of how the comparison takes place, there will be a sizable number of potential matches. This is a result of the common names contained in the SDN list. Each potential match should be reviewed to determine if your customer matches the prohibited name (a "hit") or if the match is a considered not a match (a "false positive").

- The company should develop a consistent, documented, and repeatable process to clear its potential match.
- If an exact name match is located, you should contact your legal counsel in order to determine the next steps. If a prohibited transaction is identified, OFAC requires the reporting of this information within 10 days and annually each September 30th. The prohibited transaction likely will need to be "blocked." Again, counsel should be engaged in order to navigate these complex laws.

The OFAC requirements are an important part of the United States' foreign policy and national security goals. Compliance programs should be designed to ensure prohibited transactions do not occur or are reported promptly if they should.

Money Laundering & Bank Secrecy in the EU5

Money Laundering: the European perspective

In the European Union, the "why" and "how" of money laundering are essentially the same as in the U.S. (query: are crooks the same the world around?). Broadly speaking, it covers the handling of the proceeds of criminal activity and assisting or facilitating others to do so.

Given that the EU is composed of 25 sovereign countries, there is added focus on the cross-border nature of money laundering: "money laundering shall be regarded as such even where the activities...were carried out in the territory of...a third country". Third EU Money Laundering Directive

How extensive is money laundering? The IMF estimated in 1996 that money laundering could amount to between 2% and 5% of the world's GDP.

The Financial Action Task Force (FATF)⁶ is an international body of 31 governments and 2 regional governing authorities, based in Paris, whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing. The FATF issues legal and policy-based recommendations on fighting money laundering and terrorist financing, most recently updated in June 2003.

The FATF also issues a 'name and shame' list of "non-cooperative countries and territories". Twenty-three countries were initially on the list but the only country now listed is Myanmar. The following countries were recently removed from the NCCT list: Nigeria (removed June 2006), Cook Islands (removed October 2000), Indonesia (removed October 2000) and the Philippines (removed October 2000).

AML regulation in the EU

Significant EU money laundering legislation.

First EU Directive on money laundering was adopted in 1991 (1/30/EEC), then implemented into national legislation. It applied to financial institutions (defined to include insurance companies) and credit institutions and to EU branches of foreign financial institutions and credit institutions.

First Directive was limited to the laundering of the proceeds of illegal drugs. It required (a) the identification of customers, evidence of which had to be retained for at least five years after the customer relationship ended, (b) the reporting of known or suspected money laundering transactions to national authorities and (c) the establishment of adequate control procedures and training.

A second, amending Directive was adopted in 2001 (2001/90/EC) that expanded the scope beyond drugs money to the proceeds of any serious criminal activity including fraud. It

⁵ The 25 EU Member States are: Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, Netherlands, and United Kingdom. Romania and Bulgaria are scheduled to join the EU on January 1, 2007.

⁶ FATF members are: Argentina, Australia, Austria, Belgium, Brazil, Canada, Denmark, Finland, France, Germany, Greece, Hong Kong, Iceland, Ireland, Italy, Japan, Luxembourg, Mexico, Netherlands, New Zealand, Norway, Portugal, Russian Federation, Singapore, South Africa, Spain, Sweden, Switzerland, Turkey, United Kingdom, United States...AND the European Commission and the Gulf Cooperation Council.

extended the coverage of AML responsibilities to auditors, external accountants, tax advisors, external lawyers, notaries, firms giving financial advice, real estate agents and dealers in high value goods such as precious stones and works of art where payment is made in cash of a value of EUR 1,000 or more. Six EU countries failed to pass implementing legislation.

AML and anti-terrorism legislation come together in the Third EU Money Laundering Directive (2003/60/EC), adopted in October 2003, which replaces the first and second directives. Significantly it adopts a risk-based approach to customer due diligence (explained below) in line with the FATF Recommendations.

NOTE: Third Directive is to be adopted into national law by October 2005.

Who is affected by anti-money laundering regulations?

In the EU, AML regulations apply (subject to more stringent variations in local law) to:

- financial institutions (see the definition below) and EU branches of foreign financial institutions
- credit institutions (which are defined as deposit-taking and credit-granting institutions) and EU branches of foreign credit institutions
- auditors
- external accountants
- tax advisors
- lawyers in private practice and notaries
- firms giving financial advice
- real estate agents
- dealers in high value goods such as precious stones and works of art where payment is made in cash of a value of EUR 1,000 or more
- trust and company service providers
- and any natural or legal person trading in goods paid for in cash above EUR 1,000
- casinos.

Definition of a "financial institution":

Institutions that engage in:

- lending
- financial leasing
- money transmission services
- issuing and administering means of payment (e.g., credit cards, traveller's cheques and bankers' drafts)
- guarantees and commitments
- trading for its own account or for the account of customers in (a) money market instruments, (b) foreign exchange, (c) financial futures and options, (d) exchange and interest rate instruments and (e) transferable securities

- participation in securities issues and the provision of services related to such issues
- advice to undertakings on capital structure, industrial strategy and related questions and advice as well as services relating to mergers and the purchase of undertakings
- money broking
- portfolio management and advice
- safekeeping and administration of securities
- safe custody services
- and also insurance companies authorized in accordance with EU Directive 2002/3/EC and EU branches of foreign insurance companies and certain insurance intermediaries
- and also investment firms as defined in EU Directive 2004/39/EC and EU branches of foreign investment firms
- and also collective investment schemes (i.e., European mutual funds) marketing their shares.

Specific AML and Know Your Customer (KYC) Requirements

In the EU, the Third Directive requires Member States to apply AML laws and regulations to the proceeds of any "serious crime", which now includes offences punishable by six months or more in prison.

As implemented in the United Kingdom: Proceeds of Crime Act 2002 and Money Laundering Regulations 2003. Current money laundering offences are (a) assisting a money launderer (1 years in jail plus a fine), (b) acquiring, possessing or using the proceeds of crime (1 years in jail plus a fine), concealing or transferring illegal funds (1 years in jail plus a fine), (d) failure to report a suspicious transaction (years in jail plus a fine) and (e) notifying a customer that they are being investigated or have been reported (years in jail plus a fine).

In 200 a lawyer in private practice became the first British lawyer convicted of failing to report suspicion of money laundering after his client deposited cash representing 2/3rds of the price of a new house.

Customer identification (KYC, also referred to as "customer due diligence" or CDD)

In line with the FATF Recommendations, the Third EU Directive gives guidelines to Member States that permit a risk-based approach to KYC "depending on the type of customer, business relationship or transaction".

KYC must include identifying the customer and verifying the customer's identity on the basis of documents, data or information from an independent and reliable source. Where the beneficial owner is shielded by a legal structure such as a company or trust, the beneficial owner must be identified and the ownership and control of the legal structure must be understood.

KYC must also include obtaining information on the purpose and intended nature of the business relationship.

The business relationship must be monitored on an ongoing basis to ensure that transactions are consistent with the customer's identity and the customer's business and risk profile. Where necessary, the source of funds must be identified.

All information held must be kept up to date.

Exceptions for "simplified customer due diligence": where the customer is itself an institution covered by the Third Directive or is located in a third country with "requirements equivalent to" the Directive, the KYC requirements do not apply.

Another exception: Member States may choose not to apply KYC requirements to listed companies whose securities are traded on regulated markets.

Another exception: Member States may choose not to apply KYC requirements to domestic government authorities.

Another exception: Member States may choose not to apply KYC requirements to life insurance policies with annual premiums below EUR 1,000.

Additional requirements for "enhanced customer due diligence": where the customer is not physically present for identification purposes, enhanced identification procedures are required.

Additional requirements for "enhanced customer due diligence": where the customer is a "politically exposed person" (defined below), senior management approval is required to establish a business relationship and the source of wealth and source of funds must be established.

Politically Exposed Persons.

More narrowly than U.S. law, the Third Directive defines politically exposed persons as "natural persons who are or have been entrusted with prominent public functions and immediate family members, or persons known to be close associates, of such persons".

Does a PEP ever stop being a PEP? The European Commission is debating this question, and is considering the position that a person no longer entrusted with prominent public functions for at least one year is no longer a PEP.

Further clarifications of the definition are also being considered.

Record Retention.

The record retention requirement for KYC and transaction-specific records is still five years from the end of the relationship or transaction. As with all EU Directives, Member States can impose longer requirements.

The United Kingdom has adopted the five year requirement. A summary of the U.K.'s record retention requirements is attached in the supplemental materials.

Reporting obligations and the prohibition of disclosure.

Each Member State is required by the Third Directive to establish a financial intelligence unit to receive, analyze and forward to the competent authorities information concerning potential money laundering or potential terrorist financing.

Institutions and persons covered by the Third Directive may not carry out transactions they know or suspect to be related to money laundering or terrorist financing until a report has been filed and any other locally required procedures have been completed.

No institution or person covered by the Third Directive may disclose to the customer concerned that a report has been filed or that an investigation is or may be carried out.

Suspicious Activity Reports (SARs): some UK issues.

The Serious Organised Crime Agency (SOCA) is the U.K.'s designated financial crimes intelligence unit. Total direct staff of 0.

Nearly 200,000 SARs were filed in 200 (the U.K.'s population is 1/ th that of the U.S.). Banks and building societies filed 1%, accountants . %, lawyers % and money transmission agents %.

Where permission to conclude a proposed transaction was required, consent was given in 2% of cases and the average response time was 3 days. For a customer awaiting a transfer of funds, three days can be a very long time to wait.

SARs can now be filed on-line. The paper forms are not simple to complete (samples to be attached).

A March 2006 U.K. Government report found too much "defensive reporting of little value".

The U.K. regulations also require the appointment of a Money Laundering reporting Officer, who must be a senior employee based in the U.K., must have sufficient resources including time and support staff, must be free to act on his own authority and must be approved by the regulator (the Financial Services Authority). The MLRO is to "consider" SARs before they are filed.

In cross-border transactions, a reporting obligation is likely to arise in multiple countries.

Training Obligations

The Third Directive requires that "relevant staff" be kept aware of the legal requirements surrounding money laundering and terrorist financing through training.

In the UK, all staff who handle or who are managerially responsible for transactions that may involve money laundering must receive training at least every 2 years.

International Trade Finance

The FATF recently issued a report on Trade Based Money Laundering (23 June 2006). This is "the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origins".

The report is attached in the supplemental materials

Trade-based money laundering "represents an increasingly important money laundering and terrorist financing vulnerability".

Most common methods are the over- and under-invoicing of goods and services, multiple invoicing of goods and services, over- and under-shipment of goods and services and falsely described goods and services.

Red Flag Warnings.

- The shipment does not make economic sense
- The goods are trans-shipped through one or more jurisdictions for no apparent economic reason.

- The size of the shipment appears inconsistent with the scale of the exporter or importer's regular business activities.

Information Sharing: Bank Secrecy and the EU Savings Tax Directive

Europe's recent battles over bank secrecy confirm there are strong feelings on both sides, while the FATF expresses concern that bank secrecy could inhibit the implementation of AML efforts.

After several years of difficult discussion, the EU adopted in 2003 the so-called Savings Tax Directive, 2003/ / EC. The Directive took effect July 1, 200 and requires banks in most EU countries to send customer names and information on saving income to the authorities in the customer's home country.

The discussions took years because Switzerland (not an EU Member State) and Luxembourg (a founding EU member) did not want to give up their cherished bank secrecy laws. When I worked in Luxembourg in the late 1 0s, bank secrecy was considered a mater of public policy that could not be waived, even by a willing customer.

The compromise: Austria, Belgium and Luxembourg agreed for a "transitional period" to impose a withholding tax against income earned by EU residents, and to send % of that tax to the customers' home state, but not to identify the customers by name to their domestic tax authorities. Switzerland will do the same. The withholding rate is 1 % for the first three years.

Supplemental Materials

FFIEC, Bank Secrecy Act/Anti-Money Laundering Examination Manual, 2006 (accessible at http://www.ffiec.gov/bsa_aml_infobase/default.htm)

Office of Foreign Assets Control (OFAC): <http://www.treas.gov/offices/enforcement/ofac/>

Financial Crimes Enforcement Network (FinCEN): <http://www.fincen.gov/>

3rd EU Money Laundering Directive, 2001/60/EC (copy to be attached)

FATF web site: www.fatf-gafi.org

FATF "Trade Based Money Laundering", 23 June 2006 (copy to be attached).

Serious Organised Crime Agency, www.soca.gov.uk

Sample Suspicious Activity Report (form to be attached)

Savings Tax Directive, 2003/1005/EC (copy to be attached)

U.K.'s record retention requirements (copy to be attached)

25.11.2005

EN

Official Journal of the European Union

L 309/15

DIRECTIVE 2005/60/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 26 October 2005

on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 47(2), first and third sentences, and Article 95 thereof,

Having regard to the proposal from the Commission,

Having regard to the opinion of the European Economic and Social Committee (1),

Having regard to the opinion of the European Central Bank (2),

Acting in accordance with the procedure laid down in Article 251 of the Treaty (3),

Whereas:

- (1) Massive flows of dirty money can damage the stability and reputation of the financial sector and threaten the single market, and terrorism shakes the very foundations of our society. In addition to the criminal law approach, a preventive effort via the financial system can produce results.
- (2) The soundness, integrity and stability of credit and financial institutions and confidence in the financial system as a whole could be seriously jeopardised by the efforts of criminals and their associates either to disguise the origin of criminal proceeds or to channel lawful or unlawful money for terrorist purposes. In order to avoid Member States' adopting measures to protect their financial systems which could be inconsistent with the functioning of the internal market and with the prescriptions of the rule of law and Community public policy, Community action in this area is necessary.
- (3) In order to facilitate their criminal activities, money launderers and terrorist financiers could try to take advantage of the freedom of capital movements and the freedom to supply financial services which the integrated financial area entails, if certain coordinating measures are not adopted at Community level.

(1) Opinion delivered on 11 May 2005 (not yet published in the Official Journal).

(2) OJ C 40, 17.2.2005, p. 9.

(3) Opinion of the European Parliament of 26 May 2005 (not yet published in the Official Journal) and Council Decision of 19 September 2005.

(4) In order to respond to these concerns in the field of money laundering, Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering (4) was adopted. It required Member States to prohibit money laundering and to oblige the financial sector, comprising credit institutions and a wide range of other financial institutions, to identify their customers, keep appropriate records, establish internal procedures to train staff and guard against money laundering and to report any indications of money laundering to the competent authorities.

(5) Money laundering and terrorist financing are frequently carried out in an international context. Measures adopted solely at national or even Community level, without taking account of international coordination and cooperation, would have very limited effects. The measures adopted by the Community in this field should therefore be consistent with other action undertaken in other international fora. The Community action should continue to take particular account of the Recommendations of the Financial Action Task Force (hereinafter referred to as the FATF), which constitutes the foremost international body active in the fight against money laundering and terrorist financing. Since the FATF Recommendations were substantially revised and expanded in 2003, this Directive should be in line with that new international standard.

(6) The General Agreement on Trade in Services (GATS) allows Members to adopt measures necessary to protect public morals and prevent fraud and adopt measures for prudential reasons, including for ensuring the stability and integrity of the financial system.

(7) Although initially limited to drugs offences, there has been a trend in recent years towards a much wider definition of money laundering based on a broader range of predicate offences. A wider range of predicate offences facilitates the reporting of suspicious transactions and international cooperation in this area. Therefore, the definition of serious crime should be brought into line with the definition of serious crime in Council Framework Decision 2001/500/JHA of 26 June 2001 on money laundering, the identification, tracing, freezing, seizing and confiscation of instrumentalities and the proceeds of crime (5).

(4) OJ L 166, 28.6.1991, p. 77. Directive as amended by Directive 2001/97/EC of the European Parliament and of the Council (OJ L 344, 28.12.2001, p. 76).

(5) OJ L 182, 5.7.2001, p. 1.

- (8) Furthermore, the misuse of the financial system to channel criminal or even clean money to terrorist purposes poses a clear risk to the integrity, proper functioning, reputation and stability of the financial system. Accordingly, the preventive measures of this Directive should cover not only the manipulation of money derived from crime but also the collection of money or property for terrorist purposes.
- (9) Directive 91/308/EEC, though imposing a customer identification obligation, contained relatively little detail on the relevant procedures. In view of the crucial importance of this aspect of the prevention of money laundering and terrorist financing, it is appropriate, in accordance with the new international standards, to introduce more specific and detailed provisions relating to the identification of the customer and of any beneficial owner and the verification of their identity. To that end a precise definition of 'beneficial owner' is essential. Where the individual beneficiaries of a legal entity or arrangement such as a foundation or trust are yet to be determined, and it is therefore impossible to identify an individual as the beneficial owner, it would suffice to identify the class of persons intended to be the beneficiaries of the foundation or trust. This requirement should not include the identification of the individuals within that class of persons.
- (10) The institutions and persons covered by this Directive should, in conformity with this Directive, identify and verify the identity of the beneficial owner. To fulfil this requirement, it should be left to those institutions and persons whether they make use of public records of beneficial owners, ask their clients for relevant data or obtain the information otherwise, taking into account the fact that the extent of such customer due diligence measures relates to the risk of money laundering and terrorist financing, which depends on the type of customer, business relationship, product or transaction.
- (11) Credit agreements in which the credit account serves exclusively to settle the loan and the repayment of the loan is effected from an account which was opened in the name of the customer with a credit institution covered by this Directive pursuant to Article 8(1)(a) to (c) should generally be considered as an example of types of less risky transactions.
- (12) To the extent that the providers of the property of a legal entity or arrangement have significant control over the use of the property they should be identified as a beneficial owner.
- (13) Trust relationships are widely used in commercial products as an internationally recognised feature of the comprehensively supervised wholesale financial markets. An obligation to identify the beneficial owner does not arise from the fact alone that there is a trust relationship in this particular case.
- (14) This Directive should also apply to those activities of the institutions and persons covered hereunder which are performed on the Internet.
- (15) As the tightening of controls in the financial sector has prompted money launderers and terrorist financiers to seek alternative methods for concealing the origin of the proceeds of crime and as such channels can be used for terrorist financing, the anti-money laundering and anti-terrorist financing obligations should cover life insurance intermediaries and trust and company service providers.
- (16) Entities already falling under the legal responsibility of an insurance undertaking, and therefore falling within the scope of this Directive, should not be included within the category of insurance intermediary.
- (17) Acting as a company director or secretary does not of itself make someone a trust and company service provider. For that reason, the definition covers only those persons that act as a company director or secretary for a third party and by way of business.
- (18) The use of large cash payments has repeatedly proven to be very vulnerable to money laundering and terrorist financing. Therefore, in those Member States that allow cash payments above the established threshold, all natural or legal persons trading in goods by way of business should be covered by this Directive when accepting such cash payments. Dealers in high-value goods, such as precious stones or metals, or works of art, and auctioneers are in any event covered by this Directive to the extent that payments to them are made in cash in an amount of EUR 15 000 or more. To ensure effective monitoring of compliance with this Directive by that potentially wide group of institutions and persons, Member States may focus their monitoring activities in particular on those natural and legal persons trading in goods that are exposed to a relatively high risk of money laundering or terrorist financing, in accordance with the principle of risk-based supervision. In view of the different situations in the various Member States, Member States may decide to adopt stricter provisions, in order to properly address the risk involved with large cash payments.

- (19) Directive 91/308/EEC brought notaries and other independent legal professionals within the scope of the Community anti-money laundering regime; this coverage should be maintained unchanged in this Directive; these legal professionals, as defined by the Member States, are subject to the provisions of this Directive when participating in financial or corporate transactions, including providing tax advice, where there is the greatest risk of the services of those legal professionals being misused for the purpose of laundering the proceeds of criminal activity or for the purpose of terrorist financing.
- (20) Where independent members of professions providing legal advice which are legally recognised and controlled, such as lawyers, are ascertaining the legal position of a client or representing a client in legal proceedings, it would not be appropriate under this Directive to put those legal professionals in respect of these activities under an obligation to report suspicions of money laundering or terrorist financing. There must be exemptions from any obligation to report information obtained either before, during or after judicial proceedings, or in the course of ascertaining the legal position for a client. Thus, legal advice shall remain subject to the obligation of professional secrecy unless the legal counsellor is taking part in money laundering or terrorist financing, the legal advice is provided for money laundering or terrorist financing purposes or the lawyer knows that the client is seeking legal advice for money laundering or terrorist financing purposes.
- (21) Directly comparable services need to be treated in the same manner when provided by any of the professionals covered by this Directive. In order to ensure the respect of the rights laid down in the European Convention for the Protection of Human Rights and Fundamental Freedoms and the Treaty on European Union, in the case of auditors, external accountants and tax advisors, who, in some Member States, may defend or represent a client in the context of judicial proceedings or ascertain a client's legal position, the information they obtain in the performance of those tasks should not be subject to the reporting obligations in accordance with this Directive.
- (22) It should be recognised that the risk of money laundering and terrorist financing is not the same in every case. In line with a risk-based approach, the principle should be introduced into Community legislation that simplified customer due diligence is allowed in appropriate cases.
- (23) The derogation concerning the identification of beneficial owners of pooled accounts held by notaries or other independent legal professionals should be without prejudice to the obligations that those notaries or other independent legal professionals have pursuant to this Directive. Those obligations include the need for such notaries or other independent legal professionals themselves to identify the beneficial owners of the pooled accounts held by them.
- (24) Equally, Community legislation should recognise that certain situations present a greater risk of money laundering or terrorist financing. Although the identity and business profile of all customers should be established, there are cases where particularly rigorous customer identification and verification procedures are required.
- (25) This is particularly true of business relationships with individuals holding, or having held, important public positions, particularly those from countries where corruption is widespread. Such relationships may expose the financial sector in particular to significant reputational and/or legal risks. The international effort to combat corruption also justifies the need to pay special attention to such cases and to apply the complete normal customer due diligence measures in respect of domestic politically exposed persons or enhanced customer due diligence measures in respect of politically exposed persons residing in another Member State or in a third country.
- (26) Obtaining approval from senior management for establishing business relationships should not imply obtaining approval from the board of directors but from the immediate higher level of the hierarchy of the person seeking such approval.
- (27) In order to avoid repeated customer identification procedures, leading to delays and inefficiency in business, it is appropriate, subject to suitable safeguards, to allow customers to be introduced whose identification has been carried out elsewhere. Where an institution or person covered by this Directive relies on a third party, the ultimate responsibility for the customer due diligence procedure remains with the institution or person to whom the customer is introduced. The third party, or introducer, also retains his own responsibility for all the requirements in this Directive, including the requirement to report suspicious transactions and maintain records, to the extent that he has a relationship with the customer that is covered by this Directive.

L 309/18	EN	Official Journal of the European Union	25.11.2005	25.11.2005	EN	Official Journal of the European Union	L 309/19
(28) In the case of agency or outsourcing relationships on a contractual basis between institutions or persons covered by this Directive and external natural or legal persons not covered hereby, any anti-money laundering and anti-terrorist financing obligations for those agents or outsourcing service providers as part of the institutions or persons covered by this Directive, may only arise from contract and not from this Directive. The responsibility for complying with this Directive should remain with the institution or person covered hereby.		the anti-money laundering and anti-terrorist financing system. Member States should be aware of this problem and should do whatever they can to protect employees from such threats or hostile action.		(37) This Directive establishes detailed rules for customer due diligence, including enhanced customer due diligence for high-risk customers or business relationships, such as appropriate procedures to determine whether a person is a politically exposed person, and certain additional, more detailed requirements, such as the existence of compliance management procedures and policies. All these requirements are to be met by each of the institutions and persons covered by this Directive, while Member States are expected to tailor the detailed implementation of those provisions to the particularities of the various professions and to the differences in scale and size of the institutions and persons covered by this Directive.		complex money laundering or terrorist financing operations, sanctions should also be adjusted in line with the activity carried on by legal persons.	
(29) Suspicious transactions should be reported to the financial intelligence unit (FIU), which serves as a national centre for receiving, analysing and disseminating to the competent authorities suspicious transaction reports and other information regarding potential money laundering or terrorist financing. This should not compel Member States to change their existing reporting systems where the reporting is done through a public prosecutor or other law enforcement authorities, as long as the information is forwarded promptly and unfiltered to FIUs, allowing them to conduct their business properly, including international cooperation with other FIUs.		(33) Disclosure of information as referred to in Article 28 should be in accordance with the rules on transfer of personal data to third countries as laid down in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1). Moreover, Article 28 cannot interfere with national data protection and professional secrecy legislation.		(38) In order to ensure that the institutions and others subject to Community legislation in this field remain committed, feedback should, where practicable, be made available to them on the usefulness and follow-up of the reports they present. To make this possible, and to be able to review the effectiveness of their systems to combat money laundering and terrorist financing Member States should keep and improve the relevant statistics.		(42) Natural persons exercising any of the activities referred to in Article 2(1)(3)(a) and (b) within the structure of a legal person, but on an independent basis, should be independently responsible for compliance with the provisions of this Directive, with the exception of Article 35.	
(30) By way of derogation from the general prohibition on executing suspicious transactions, the institutions and persons covered by this Directive may execute suspicious transactions before informing the competent authorities, where refraining from the execution thereof is impossible or likely to frustrate efforts to pursue the beneficiaries of a suspected money laundering or terrorist financing operation. This, however, should be without prejudice to the international obligations accepted by the Member States to freeze without delay funds or other assets of terrorists, terrorist organisations or those who finance terrorism, in accordance with the relevant United Nations Security Council resolutions.		(34) Persons who merely convert paper documents into electronic data and are acting under a contract with a credit institution or a financial institution do not fall within the scope of this Directive, nor does any natural or legal person that provides credit or financial institutions solely with a message or other support systems for transmitting funds or with clearing and settlement systems.		(39) When registering or licensing a currency exchange office, a trust and company service provider or a casino nationally, competent authorities should ensure that the persons who effectively direct or will direct the business of such entities and the beneficial owners of such entities are fit and proper persons. The criteria for determining whether or not a person is fit and proper should be established in conformity with national law. As a minimum, such criteria should reflect the need to protect such entities from being misused by their managers or beneficial owners for criminal purposes.		(43) Clarification of the technical aspects of the rules laid down in this Directive may be necessary to ensure an effective and sufficiently consistent implementation of this Directive, taking into account the different financial instruments, professions and risks in the different Member States and the technical developments in the fight against money laundering and terrorist financing. The Commission should accordingly be empowered to adopt implementing measures, such as certain criteria for identifying low and high risk situations in which simplified due diligence could suffice or enhanced due diligence would be appropriate, provided that they do not modify the essential elements of this Directive and provided that the Commission acts in accordance with the principles set out herein, after consulting the Committee on the Prevention of Money Laundering and Terrorist Financing.	
(31) Where a Member State decides to make use of the exemptions provided for in Article 23(2), it may allow or require the self-regulatory body representing the persons referred to therein not to transmit to the FIU any information obtained from those persons in the circumstances referred to in that Article.		(35) Money laundering and terrorist financing are international problems and the effort to combat them should be global. Where Community credit and financial institutions have branches and subsidiaries located in third countries where the legislation in this area is deficient, they should, in order to avoid the application of very different standards within an institution or group of institutions, apply the Community standard or notify the competent authorities of the home Member State if this application is impossible.		(40) Taking into account the international character of money laundering and terrorist financing, coordination and cooperation between FIUs as referred to in Council Decision 2000/642/JHA of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information (2), including the establishment of an EU FIU-net, should be encouraged to the greatest possible extent. To that end, the Commission should lend such assistance as may be needed to facilitate such coordination, including financial assistance.		(44) The measures necessary for the implementation of this Directive should be adopted in accordance with Council Decision 1999/468/EC of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission (3). To that end a new Committee on the Prevention of Money Laundering and Terrorist Financing, replacing the Money Laundering Contact Committee set up by Directive 91/308/EEC, should be established.	
(32) There has been a number of cases of employees who report their suspicions of money laundering being subjected to threats or hostile action. Although this Directive cannot interfere with Member States' judicial procedures, this is a crucial issue for the effectiveness of		(36) It is important that credit and financial institutions should be able to respond rapidly to requests for information on whether they maintain business relationships with named persons. For the purpose of identifying such business relationships in order to be able to provide that information quickly, credit and financial institutions should have effective systems in place which are commensurate with the size and nature of their business. In particular it would be appropriate for credit institutions and larger financial institutions to have electronic systems at their disposal. This provision is of particular importance in the context of procedures leading to measures such as the freezing or seizing of assets (including terrorist assets), pursuant to applicable national or Community legislation with a view to combating terrorism.		(41) The importance of combating money laundering and terrorist financing should lead Member States to lay down effective, proportionate and dissuasive penalties in national law for failure to respect the national provisions adopted pursuant to this Directive. Provision should be made for penalties in respect of natural and legal persons. Since legal persons are often involved in		(45) In view of the very substantial amendments that would need to be made to Directive 91/308/EEC, it should be repealed for reasons of clarity.	
		(1) OJ L 281, 23.11.1995, p. 31. Directive as amended by Regulation (EC) No 1882/2003 (OJ L 284, 31.10.2003, p. 1).		(2) OJ L 271, 24.10.2000, p. 4.		(3) OJ L 184, 17.7.1999, p. 23.	

(47) In exercising its implementing powers in accordance with this Directive, the Commission should respect the following principles: the need for high levels of transparency and consultation with institutions and persons covered by this Directive and with the European Parliament and the Council; the need to ensure that competent authorities will be able to ensure compliance with the rules consistently; the balance of costs and benefits to institutions and persons covered by this Directive on a long-term basis in any implementing measures; the need to respect the necessary flexibility in the application of the implementing measures in accordance with a risk-sensitive approach; the need to ensure coherence with other Community legislation in this area; the need to protect the Community, its Member States and their citizens from the consequences of money laundering and terrorist financing.

(48) This Directive respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union. Nothing in this Directive should be interpreted or implemented in a manner that is inconsistent with the European Convention on Human Rights.

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I

SUBJECT MATTER, SCOPE AND DEFINITIONS

Article 1

1. Member States shall ensure that money laundering and terrorist financing are prohibited.

2. For the purposes of this Directive, the following conduct, when committed intentionally, shall be regarded as money laundering:

(a) the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such activity to evade the legal consequences of his action;

(b) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is

derived from criminal activity or from an act of participation in such activity;

(c) the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such activity;

(d) participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions mentioned in the foregoing points.

3. Money laundering shall be regarded as such even where the activities which generated the property to be laundered were carried out in the territory of another Member State or in that of a third country.

4. For the purposes of this Directive, 'terrorist financing' means the provision or collection of funds, by any means, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the offences within the meaning of Articles 1 to 4 of Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism⁽¹⁾.

5. Knowledge, intent or purpose required as an element of the activities mentioned in paragraphs 2 and 4 may be inferred from objective factual circumstances.

Article 2

1. This Directive shall apply to:

(1) credit institutions;

(2) financial institutions;

(3) the following legal or natural persons acting in the exercise of their professional activities:

(a) auditors, external accountants and tax advisors;

(b) notaries and other independent legal professionals, when they participate, whether by acting on behalf of and for their client in any financial or real estate transaction, or by assisting in the planning or execution of transactions for their client concerning the:

(i) buying and selling of real property or business entities;

(ii) managing of client money, securities or other assets;

⁽¹⁾ OJ L 164, 22.6.2002, p. 3.

(iii) opening or management of bank, savings or securities accounts;

(iv) organisation of contributions necessary for the creation, operation or management of companies;

(v) creation, operation or management of trusts, companies or similar structures;

(c) trust or company service providers not already covered under points (a) or (b);

(d) real estate agents;

(e) other natural or legal persons trading in goods, only to the extent that payments are made in cash in an amount of EUR 15 000 or more, whether the transaction is executed in a single operation or in several operations which appear to be linked;

(f) casinos.

2. Member States may decide that legal and natural persons who engage in a financial activity on an occasional or very limited basis and where there is little risk of money laundering or terrorist financing occurring do not fall within the scope of Article 3(1) or (2).

Article 3

For the purposes of this Directive the following definitions shall apply:

(1) 'credit institution' means a credit institution, as defined in the first subparagraph of Article 1(1) of Directive 2000/12/EC of the European Parliament and of the Council of 20 March 2000 relating to the taking up and pursuit of the business of credit institutions⁽¹⁾, including branches within the meaning of Article 1(3) of that Directive located in the Community of credit institutions having their head offices inside or outside the Community;

(2) 'financial institution' means:

(a) an undertaking other than a credit institution which carries out one or more of the operations included in points 2 to 12 and 14 of Annex I to Directive 2000/12/EC, including the activities of currency exchange offices (bureaux de change) and of money transmission or remittance offices;

(b) an insurance company duly authorised in accordance with Directive 2002/83/EC of the European Parliament and of the Council of 5 November 2002 concerning life assurance⁽²⁾, insofar as it carries out activities covered by that Directive;

(c) an investment firm as defined in point 1 of Article 4(1) of Directive 2004/39/EC of the European Parliament

⁽¹⁾ OJ L 126, 26.5.2000, p. 1. Directive as last amended by Directive 2005/1/EC (OJ L 79, 24.3.2005, p. 9).

⁽²⁾ OJ L 345, 19.12.2002, p. 1. Directive as last amended by Directive 2005/1/EC.

and of the Council of 21 April 2004 on markets in financial instruments⁽³⁾;

(d) a collective investment undertaking marketing its units or shares;

(e) an insurance intermediary as defined in Article 2(5) of Directive 2002/92/EC of the European Parliament and of the Council of 9 December 2002 on insurance mediation⁽⁴⁾, with the exception of intermediaries as mentioned in Article 2(7) of that Directive, when they act in respect of life insurance and other investment related services;

(f) branches, when located in the Community, of financial institutions as referred to in points (a) to (e), whose head offices are inside or outside the Community;

(3) 'property' means assets of every kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments in any form including electronic or digital, evidencing title to or an interest in such assets;

(4) 'criminal activity' means any kind of criminal involvement in the commission of a serious crime;

(5) 'serious crimes' means, at least:

(a) acts as defined in Articles 1 to 4 of Framework Decision 2002/475/JHA;

(b) any of the offences defined in Article 3(1)(a) of the 1988 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances;

(c) the activities of criminal organisations as defined in Article 1 of Council Joint Action 98/733/JHA of 21 December 1998 on making it a criminal offence to participate in a criminal organisation in the Member States of the European Union⁽⁵⁾;

(d) fraud, at least serious, as defined in Article 1(1) and Article 2 of the Convention on the Protection of the European Communities' Financial Interests⁽⁶⁾;

(e) corruption;

(f) all offences which are punishable by deprivation of liberty or a detention order for a maximum of more than one year or, as regards those States which have a minimum threshold for offences in their legal system, all offences punishable by deprivation of liberty or a detention order for a minimum of more than six months;

⁽¹⁾ OJ L 145, 30.4.2004, p. 1.

⁽²⁾ OJ L 9, 15.1.2003, p. 3.

⁽³⁾ OJ L 351, 29.12.1998, p. 1.

⁽⁴⁾ OJ C 316, 27.11.1995, p. 49.

- (6) 'beneficial owner' means the natural person(s) who ultimately owns or controls the customer and/or the natural person on whose behalf a transaction or activity is being conducted. The beneficial owner shall at least include:
- (a) in the case of corporate entities:
- (i) the natural person(s) who ultimately owns or controls a legal entity through direct or indirect ownership or control over a sufficient percentage of the shares or voting rights in that legal entity, including through bearer share holdings, other than a company listed on a regulated market that is subject to disclosure requirements consistent with Community legislation or subject to equivalent international standards;
- (ii) the natural person(s) who otherwise exercises control over the management of a legal entity;
- (b) in the case of legal entities, such as foundations, and legal arrangements, such as trusts, which administer and distribute funds:
- (i) where the future beneficiaries have already been determined, the natural person(s) who is the beneficiary of 25 % or more of the property of a legal arrangement or entity;
- (ii) where the individuals that benefit from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates;
- (iii) the natural person(s) who exercises control over 25 % or more of the property of a legal arrangement or entity;
- (7) 'trust and company service providers' means any natural or legal person which by way of business provides any of the following services to third parties:
- (a) forming companies or other legal persons;
- (b) acting as or arranging for another person to act as a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
- (c) providing a registered office, business address, correspondence or administrative address and other related services for a company, a partnership or any other legal person or arrangement;
- (d) acting as or arranging for another person to act as a trustee of an express trust or a similar legal arrangement;
- (e) acting as or arranging for another person to act as a nominee shareholder for another person other than a company listed on a regulated market that is subject to disclosure requirements in conformity with Community legislation or subject to equivalent international standards;
- (8) 'politically exposed persons' means natural persons who are or have been entrusted with prominent public functions and immediate family members, or persons known to be close associates, of such persons;
- (9) 'business relationship' means a business, professional or commercial relationship which is connected with the professional activities of the institutions and persons covered by this Directive and which is expected, at the time when the contact is established, to have an element of duration;
- (10) 'shell bank' means a credit institution, or an institution engaged in equivalent activities, incorporated in a jurisdiction in which it has no physical presence, involving meaningful mind and management, and which is unaffiliated with a regulated financial group.

Article 4

1. Member States shall ensure that the provisions of this Directive are extended in whole or in part to professions and to categories of undertakings, other than the institutions and persons referred to in Article 2(1), which engage in activities which are particularly likely to be used for money laundering or terrorist financing purposes.

2. Where a Member State decides to extend the provisions of this Directive to professions and to categories of undertakings other than those referred to in Article 2(1), it shall inform the Commission thereof.

Article 5

The Member States may adopt or retain in force stricter provisions in the field covered by this Directive to prevent money laundering and terrorist financing.

CHAPTER II

CUSTOMER DUE DILIGENCE

SECTION 1

General provisions

Article 6

Member States shall prohibit their credit and financial institutions from keeping anonymous accounts or anonymous passbooks. By way of derogation from Article 9(6), Member States shall in all cases require that the owners and beneficiaries of existing anonymous accounts or anonymous passbooks be made the subject of customer due diligence measures as soon as possible and in any event before such accounts or passbooks are used in any way.

Article 7

The institutions and persons covered by this Directive shall apply customer due diligence measures in the following cases:

- (a) when establishing a business relationship;
- (b) when carrying out occasional transactions amounting to EUR 15 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;
- (c) when there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold;
- (d) when there are doubts about the veracity or adequacy of previously obtained customer identification data.

Article 8

1. Customer due diligence measures shall comprise:

- (a) identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;
- (b) identifying, where applicable, the beneficial owner and taking risk-based and adequate measures to verify his identity so that the institution or person covered by this Directive is satisfied that it knows who the beneficial owner is, including, as regards legal persons, trusts and similar legal arrangements, taking risk-based and adequate measures to understand the ownership and control structure of the customer;
- (c) obtaining information on the purpose and intended nature of the business relationship;
- (d) conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transac-

tions being conducted are consistent with the institution's or person's knowledge of the customer, the business and risk profile, including, where necessary, the source of funds and ensuring that the documents, data or information held are kept up-to-date.

2. The institutions and persons covered by this Directive shall apply each of the customer due diligence requirements set out in paragraph 1, but may determine the extent of such measures on a risk-sensitive basis depending on the type of customer, business relationship, product or transaction. The institutions and persons covered by this Directive shall be able to demonstrate to the competent authorities mentioned in Article 37, including self-regulatory bodies, that the extent of the measures is appropriate in view of the risks of money laundering and terrorist financing.

Article 9

1. Member States shall require that the verification of the identity of the customer and the beneficial owner takes place before the establishment of a business relationship or the carrying-out of the transaction.

2. By way of derogation from paragraph 1, Member States may allow the verification of the identity of the customer and the beneficial owner to be completed during the establishment of a business relationship if this is necessary not to interrupt the normal conduct of business and where there is little risk of money laundering or terrorist financing occurring. In such situations these procedures shall be completed as soon as practicable after the initial contact.

3. By way of derogation from paragraphs 1 and 2, Member States may, in relation to life insurance business, allow the verification of the identity of the beneficiary under the policy to take place after the business relationship has been established. In that case, verification shall take place at or before the time of payout or at or before the time the beneficiary intends to exercise rights vested under the policy.

4. By way of derogation from paragraphs 1 and 2, Member States may allow the opening of a bank account provided that there are adequate safeguards in place to ensure that transactions are not carried out by the customer or on its behalf until full compliance with the aforementioned provisions is obtained.

5. Member States shall require that, where the institution or person concerned is unable to comply with points (a), (b) and (c) of Article 8(1), it may not carry out a transaction through a bank account, establish a business relationship or carry out the transaction, or shall terminate the business relationship, and shall consider making a report to the financial intelligence unit (FIU) in accordance with Article 22 in relation to the customer.

Member States shall not be obliged to apply the previous subparagraph in situations when notaries, independent legal professionals, auditors, external accountants and tax advisors are in the course of ascertaining the legal position for their client or performing their task of defending or representing that client in, or concerning judicial proceedings, including advice on instituting or avoiding proceedings.

6. Member States shall require that institutions and persons covered by this Directive apply the customer due diligence procedures not only to all new customers but also at appropriate times to existing customers on a risk-sensitive basis.

Article 10

1. Member States shall require that all casino customers be identified and their identity verified if they purchase or exchange gambling chips with a value of EUR 2 000 or more.

2. Casinos subject to State supervision shall be deemed in any event to have satisfied the customer due diligence requirements if they register, identify and verify the identity of their customers immediately on or before entry, regardless of the amount of gambling chips purchased.

SECTION 2

Simplified customer due diligence

Article 11

1. By way of derogation from Articles 7(a), (b) and (d), 8 and 9(1), the institutions and persons covered by this Directive shall not be subject to the requirements provided for in those Articles where the customer is a credit or financial institution covered by this Directive, or a credit or financial institution situated in a third country which imposes requirements equivalent to those laid down in this Directive and supervised for compliance with those requirements.

2. By way of derogation from Articles 7(a), (b) and (d), 8 and 9(1) Member States may allow the institutions and persons covered by this Directive not to apply customer due diligence in respect of:

(a) listed companies whose securities are admitted to trading on a regulated market within the meaning of Directive

2004/39/EC in one or more Member States and listed companies from third countries which are subject to disclosure requirements consistent with Community legislation;

(b) beneficial owners of pooled accounts held by notaries and other independent legal professionals from the Member States, or from third countries provided that they are subject to requirements to combat money laundering or terrorist financing consistent with international standards and are supervised for compliance with those requirements and provided that the information on the identity of the beneficial owner is available, on request, to the institutions that act as depository institutions for the pooled accounts;

(c) domestic public authorities,

or in respect of any other customer representing a low risk of money laundering or terrorist financing which meets the technical criteria established in accordance with Article 40(1)(b).

3. In the cases mentioned in paragraphs 1 and 2, institutions and persons covered by this Directive shall in any case gather sufficient information to establish if the customer qualifies for an exemption as mentioned in these paragraphs.

4. The Member States shall inform each other and the Commission of cases where they consider that a third country meets the conditions laid down in paragraphs 1 or 2 or in other situations which meet the technical criteria established in accordance with Article 40(1)(b).

5. By way of derogation from Articles 7(a), (b) and (d), 8 and 9(1), Member States may allow the institutions and persons covered by this Directive not to apply customer due diligence in respect of:

(a) life insurance policies where the annual premium is no more than EUR 1 000 or the single premium is no more than EUR 2 500;

(b) insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral;

(c) a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme;

(d) electronic money, as defined in Article 1(3)(b) of Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions⁽⁷⁾, where, if the device cannot be recharged, the maximum amount stored in the device is no more than EUR 150, or where, if the device can be recharged, a limit of EUR 2 500 is imposed on the total amount transacted in a calendar year, except when an amount of EUR 1 000 or more is redeemed in that same calendar year by the bearer as referred to in Article 3 of Directive 2000/46/EC,

or in respect of any other product or transaction representing a low risk of money laundering or terrorist financing which meets the technical criteria established in accordance with Article 40(1)(b).

Article 12

Where the Commission adopts a decision pursuant to Article 40(4), the Member States shall prohibit the institutions and persons covered by this Directive from applying simplified due diligence to credit and financial institutions or listed companies from the third country concerned or other entities following from situations which meet the technical criteria established in accordance with Article 40(1)(b).

SECTION 3

Enhanced customer due diligence

Article 13

1. Member States shall require the institutions and persons covered by this Directive to apply, on a risk-sensitive basis, enhanced customer due diligence measures, in addition to the measures referred to in Articles 7, 8 and 9(6), in situations which by their nature can present a higher risk of money laundering or terrorist financing, and at least in the situations set out in paragraphs 2, 3, 4 and in other situations representing a high risk of money laundering or terrorist financing which meet the technical criteria established in accordance with Article 40(1)(c).

2. Where the customer has not been physically present for identification purposes, Member States shall require those institutions and persons to take specific and adequate measures to compensate for the higher risk, for example by applying one or more of the following measures:

(7) OJ L 275, 27.10.2000, p. 39.

(a) ensuring that the customer's identity is established by additional documents, data or information;

(b) supplementary measures to verify or certify the documents supplied, or requiring confirmatory certification by a credit or financial institution covered by this Directive;

(c) ensuring that the first payment of the operations is carried out through an account opened in the customer's name with a credit institution.

3. In respect of cross-frontier correspondent banking relationships with respondent institutions from third countries, Member States shall require their credit institutions to:

(a) gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision;

(b) assess the respondent institution's anti-money laundering and anti-terrorist financing controls;

(c) obtain approval from senior management before establishing new correspondent banking relationships;

(d) document the respective responsibilities of each institution;

(e) with respect to payable-through accounts, be satisfied that the respondent credit institution has verified the identity of and performed ongoing due diligence on the customers having direct access to accounts of the correspondent and that it is able to provide relevant customer due diligence data to the correspondent institution, upon request.

4. In respect of transactions or business relationships with politically exposed persons residing in another Member State or in a third country, Member States shall require those institutions and persons covered by this Directive to:

(a) have appropriate risk-based procedures to determine whether the customer is a politically exposed person;

(b) have senior management approval for establishing business relationships with such customers;

(c) take adequate measures to establish the source of wealth and source of funds that are involved in the business relationship or transaction;

(d) conduct enhanced ongoing monitoring of the business relationship.

5. Member States shall prohibit credit institutions from entering into or continuing a correspondent banking relationship with a shell bank and shall require that credit institutions take appropriate measures to ensure that they do not engage in or continue correspondent banking relationships with a bank that is known to permit its accounts to be used by a shell bank.

6. Member States shall ensure that the institutions and persons covered by this Directive pay special attention to any money laundering or terrorist financing threat that may arise from products or transactions that might favour anonymity, and take measures, if needed, to prevent their use for money laundering or terrorist financing purposes.

SECTION 4

Performance by third parties

Article 14

Member States may permit the institutions and persons covered by this Directive to rely on third parties to meet the requirements laid down in Article 8(1)(a) to (c). However, the ultimate responsibility for meeting those requirements shall remain with the institution or person covered by this Directive which relies on the third party.

Article 15

1. Where a Member State permits credit and financial institutions referred to in Article 2(1)(1) or (2) situated in its territory to be relied on as a third party domestically, that Member State shall in any case permit institutions and persons referred to in Article 2(1) situated in its territory to recognise and accept, in accordance with the provisions laid down in Article 14, the outcome of the customer due diligence requirements laid down in Article 8(1)(a) to (c), carried out in accordance with this Directive by an institution referred to in Article 2(1)(1) or (2) in another Member State, with the exception of currency exchange offices and money transmission or remittance offices, and meeting the requirements laid down in Articles 16 and 18, even if the documents or data on which these requirements have been based are different to those required in the Member State to which the customer is being referred.

2. Where a Member State permits currency exchange offices and money transmission or remittance offices referred to in Article 3(2)(a) situated in its territory to be relied on as a third party domestically, that Member State shall in any case permit them to recognise and accept, in accordance with Article 14,

the outcome of the customer due diligence requirements laid down in Article 8(1)(a) to (c), carried out in accordance with this Directive by the same category of institution in another Member State and meeting the requirements laid down in Articles 16 and 18, even if the documents or data on which these requirements have been based are different to those required in the Member State to which the customer is being referred.

3. Where a Member State permits persons referred to in Article 2(1)(3)(a) to (c) situated in its territory to be relied on as a third party domestically, that Member State shall in any case permit them to recognise and accept, in accordance with Article 14, the outcome of the customer due diligence requirements laid down in Article 8(1)(a) to (c), carried out in accordance with this Directive by a person referred to in Article 2(1)(3)(a) to (c) in another Member State and meeting the requirements laid down in Articles 16 and 18, even if the documents or data on which these requirements have been based are different to those required in the Member State to which the customer is being referred.

Article 16

1. For the purposes of this Section, 'third parties' shall mean institutions and persons who are listed in Article 2, or equivalent institutions and persons situated in a third country, who meet the following requirements:

(a) they are subject to mandatory professional registration, recognised by law;

(b) they apply customer due diligence requirements and record keeping requirements as laid down or equivalent to those laid down in this Directive and their compliance with the requirements of this Directive is supervised in accordance with Section 2 of Chapter V, or they are situated in a third country which imposes equivalent requirements to those laid down in this Directive.

2. Member States shall inform each other and the Commission of cases where they consider that a third country meets the conditions laid down in paragraph 1(b).

Article 17

Where the Commission adopts a decision pursuant to Article 40(4), Member States shall prohibit the institutions and persons covered by this Directive from relying on third parties from the third country concerned to meet the requirements laid down in Article 8(1)(a) to (c).

Article 18

1. Third parties shall make information requested in accordance with the requirements laid down in Article 8(1)(a) to (c) immediately available to the institution or person covered by this Directive to which the customer is being referred.

2. Relevant copies of identification and verification data and other relevant documentation on the identity of the customer or the beneficial owner shall immediately be forwarded, on request, by the third party to the institution or person covered by this Directive to which the customer is being referred.

Article 19

This Section shall not apply to outsourcing or agency relationships where, on the basis of a contractual arrangement, the outsourcing service provider or agent is to be regarded as part of the institution or person covered by this Directive.

CHAPTER III

REPORTING OBLIGATIONS

SECTION 1

General provisions

Article 20

Member States shall require that the institutions and persons covered by this Directive pay special attention to any activity which they regard as particularly likely, by its nature, to be related to money laundering or terrorist financing and in particular complex or unusually large transactions and all unusual patterns of transactions which have no apparent economic or visible lawful purpose.

Article 21

1. Each Member State shall establish a FIU in order effectively to combat money laundering and terrorist financing.

2. That FIU shall be established as a central national unit. It shall be responsible for receiving (and to the extent permitted, requesting), analysing and disseminating to the competent authorities, disclosures of information which concern potential money laundering, potential terrorist financing or are required by national legislation or regulation. It shall be provided with adequate resources in order to fulfil its tasks.

3. Member States shall ensure that the FIU has access, directly or indirectly, on a timely basis, to the financial, administrative and law enforcement information that it requires to properly fulfil its tasks.

Article 22

1. Member States shall require the institutions and persons covered by this Directive, and where applicable their directors and employees, to cooperate fully:

(a) by promptly informing the FIU, on their own initiative, where the institution or person covered by this Directive knows, suspects or has reasonable grounds to suspect that money laundering or terrorist financing is being or has been committed or attempted;

(b) by promptly furnishing the FIU, at its request, with all necessary information, in accordance with the procedures established by the applicable legislation.

2. The information referred to in paragraph 1 shall be forwarded to the FIU of the Member State in whose territory the institution or person forwarding the information is situated. The person or persons designated in accordance with the procedures provided for in Article 34 shall normally forward the information.

Article 23

1. By way of derogation from Article 22(1), Member States may, in the case of the persons referred to in Article 2(1)(3)(a) and (b), designate an appropriate self-regulatory body of the profession concerned as the authority to be informed in the first instance in place of the FIU. Without prejudice to paragraph 2, the designated self-regulatory body shall in such cases forward the information to the FIU promptly and unfiltered.

2. Member States shall not be obliged to apply the obligations laid down in Article 22(1) to notaries, independent legal professionals, auditors, external accountants and tax advisors with regard to information they receive from or obtain on one of their clients, in the course of ascertaining the legal position for their client or performing their task of defending or representing that client in, or concerning judicial proceedings, including advice on instituting or avoiding proceedings, whether such information is received or obtained before, during or after such proceedings.

Article 24

1. Member States shall require the institutions and persons covered by this Directive to refrain from carrying out transactions which they know or suspect to be related to money laundering or terrorist financing until they have completed the necessary action in accordance with Article 22(1)(a). In conformity with the legislation of the Member States, instructions may be given not to carry out the transaction.

2. Where such a transaction is suspected of giving rise to money laundering or terrorist financing and where to refrain in such manner is impossible or is likely to frustrate efforts to pursue the beneficiaries of a suspected money laundering or terrorist financing operation, the institutions and persons concerned shall inform the FIU immediately afterwards.

Article 25

1. Member States shall ensure that if, in the course of inspections carried out in the institutions and persons covered by this Directive by the competent authorities referred to in Article 37, or in any other way, those authorities discover facts that could be related to money laundering or terrorist financing, they shall promptly inform the FIU.

2. Member States shall ensure that supervisory bodies empowered by law or regulation to oversee the stock, foreign exchange and financial derivatives markets inform the FIU if they discover facts that could be related to money laundering or terrorist financing.

Article 26

The disclosure in good faith as foreseen in Articles 22(1) and 23 by an institution or person covered by this Directive or by an employee or director of such an institution or person of the information referred to in Articles 22 and 23 shall not constitute a breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, and shall not involve the institution or person or its directors or employees in liability of any kind.

Article 27

Member States shall take all appropriate measures in order to protect employees of the institutions or persons covered by this Directive who report suspicions of money laundering or terrorist financing either internally or to the FIU from being exposed to threats or hostile action.

SECTION 2

Prohibition of disclosure

Article 28

1. The institutions and persons covered by this Directive and their directors and employees shall not disclose to the customer concerned or to other third persons the fact that information has been transmitted in accordance with Articles 22 and 23 or that a money laundering or terrorist financing investigation is being or may be carried out.

2. The prohibition laid down in paragraph 1 shall not include disclosure to the competent authorities referred to in

Article 37, including the self-regulatory bodies, or disclosure for law enforcement purposes.

3. The prohibition laid down in paragraph 1 shall not prevent disclosure between institutions from Member States, or from third countries provided that they meet the conditions laid down in Article 11(1), belonging to the same group as defined by Article 2(12) of Directive 2002/87/EC of the European Parliament and of the Council of 16 December 2002 on the supplementary supervision of credit institutions, insurance undertakings and investment firms in a financial conglomerate⁽¹⁾.

4. The prohibition laid down in paragraph 1 shall not prevent disclosure between persons referred to in Article 2(1)(3)(a) and (b) from Member States, or from third countries which impose requirements equivalent to those laid down in this Directive, who perform their professional activities, whether as employees or not, within the same legal person or a network. For the purposes of this Article, a 'network' means the larger structure to which the person belongs and which shares common ownership, management or compliance control.

5. For institutions or persons referred to in Article 2(1)(1), (2) and (3)(a) and (b) in cases related to the same customer and the same transaction involving two or more institutions or persons, the prohibition laid down in paragraph 1 shall not prevent disclosure between the relevant institutions or persons provided that they are situated in a Member State, or in a third country which imposes requirements equivalent to those laid down in this Directive, and that they are from the same professional category and are subject to equivalent obligations as regards professional secrecy and personal data protection. The information exchanged shall be used exclusively for the purposes of the prevention of money laundering and terrorist financing.

6. Where the persons referred to in Article 2(1)(3)(a) and (b) seek to dissuade a client from engaging in illegal activity, this shall not constitute a disclosure within the meaning of the paragraph 1.

7. The Member States shall inform each other and the Commission of cases where they consider that a third country meets the conditions laid down in paragraphs 3, 4 or 5.

Article 29

Where the Commission adopts a decision pursuant to Article 40(4), the Member States shall prohibit the disclosure between institutions and persons covered by this Directive and institutions and persons from the third country concerned.

⁽¹⁾ OJ L 35, 11.2.2003, p. 1.

CHAPTER IV

Article 32

RECORD KEEPING AND STATISTICAL DATA

Article 30

Member States shall require the institutions and persons covered by this Directive to keep the following documents and information for use in any investigation into, or analysis of, possible money laundering or terrorist financing by the FIU or by other competent authorities in accordance with national law:

- in the case of the customer due diligence, a copy or the references of the evidence required, for a period of at least five years after the business relationship with their customer has ended;
- in the case of business relationships and transactions, the supporting evidence and records, consisting of the original documents or copies admissible in court proceedings under the applicable national legislation for a period of at least five years following the carrying-out of the transactions or the end of the business relationship.

Article 31

1. Member States shall require the credit and financial institutions covered by this Directive to apply, where applicable, in their branches and majority-owned subsidiaries located in third countries measures at least equivalent to those laid down in this Directive with regard to customer due diligence and record keeping.

Where the legislation of the third country does not permit application of such equivalent measures, the Member States shall require the credit and financial institutions concerned to inform the competent authorities of the relevant home Member State accordingly.

2. Member States and the Commission shall inform each other of cases where the legislation of the third country does not permit application of the measures required under the first subparagraph of paragraph 1 and coordinated action could be taken to pursue a solution.

3. Member States shall require that, where the legislation of the third country does not permit application of the measures required under the first subparagraph of paragraph 1, credit or financial institutions take additional measures to effectively handle the risk of money laundering or terrorist financing.

Member States shall require that their credit and financial institutions have systems in place that enable them to respond fully and rapidly to enquiries from the FIU, or from other authorities, in accordance with their national law, as to whether they maintain or have maintained during the previous five years a business relationship with specified natural or legal persons and on the nature of that relationship.

Article 33

1. Member States shall ensure that they are able to review the effectiveness of their systems to combat money laundering or terrorist financing by maintaining comprehensive statistics on matters relevant to the effectiveness of such systems.

2. Such statistics shall as a minimum cover the number of suspicious transaction reports made to the FIU, the follow-up given to these reports and indicate on an annual basis the number of cases investigated, the number of persons prosecuted, the number of persons convicted for money laundering or terrorist financing offences and how much property has been frozen, seized or confiscated.

3. Member States shall ensure that a consolidated review of these statistical reports is published.

CHAPTER V

ENFORCEMENT MEASURES

SECTION 1

Internal procedures, training and feedback

Article 34

1. Member States shall require that the institutions and persons covered by this Directive establish adequate and appropriate policies and procedures of customer due diligence, reporting, record keeping, internal control, risk assessment, risk management, compliance management and communication in order to forestall and prevent operations related to money laundering or terrorist financing.

2. Member States shall require that credit and financial institutions covered by this Directive communicate relevant policies and procedures where applicable to branches and majority-owned subsidiaries in third countries.

Article 35

1. Member States shall require that the institutions and persons covered by this Directive take appropriate measures so that their relevant employees are aware of the provisions in force on the basis of this Directive.

These measures shall include participation of their relevant employees in special ongoing training programmes to help them recognise operations which may be related to money laundering or terrorist financing and to instruct them as to how to proceed in such cases.

Where a natural person falling within any of the categories listed in Article 2(1)(3) performs his professional activities as an employee of a legal person, the obligations in this Section shall apply to that legal person rather than to the natural person.

2. Member States shall ensure that the institutions and persons covered by this Directive have access to up-to-date information on the practices of money launderers and terrorist financiers and on indications leading to the recognition of suspicious transactions.

3. Member States shall ensure that, wherever practicable, timely feedback on the effectiveness of and follow-up to reports of suspected money laundering or terrorist financing is provided.

SECTION 2

Supervision

Article 36

1. Member States shall provide that currency exchange offices and trust and company service providers shall be licensed or registered and casinos be licensed in order to operate their business legally. Without prejudice to future Community legislation, Member States shall provide that money transmission or remittance offices shall be licensed or registered in order to operate their business legally.

2. Member States shall require competent authorities to refuse licensing or registration of the entities referred to in paragraph 1 if they are not satisfied that the persons who effectively direct or will direct the business of such entities or the beneficial owners of such entities are fit and proper persons.

Article 37

1. Member States shall require the competent authorities at least to effectively monitor and to take the necessary measures

with a view to ensuring compliance with the requirements of this Directive by all the institutions and persons covered by this Directive.

2. Member States shall ensure that the competent authorities have adequate powers, including the power to compel the production of any information that is relevant to monitoring compliance and perform checks, and have adequate resources to perform their functions.

3. In the case of credit and financial institutions and casinos, competent authorities shall have enhanced supervisory powers, notably the possibility to conduct on-site inspections.

4. In the case of the natural and legal persons referred to in Article 2(1)(3)(a) to (e), Member States may allow the functions referred to in paragraph 1 to be performed on a risk-sensitive basis.

5. In the case of the persons referred to in Article 2(1)(3)(a) and (b), Member States may allow the functions referred to in paragraph 1 to be performed by self-regulatory bodies, provided that they comply with paragraph 2.

SECTION 3

Cooperation

Article 38

The Commission shall lend such assistance as may be needed to facilitate coordination, including the exchange of information between FIUs within the Community.

SECTION 4

Penalties

Article 39

1. Member States shall ensure that natural and legal persons covered by this Directive can be held liable for infringements of the national provisions adopted pursuant to this Directive. The penalties must be effective, proportionate and dissuasive.

2. Without prejudice to the right of Member States to impose criminal penalties, Member States shall ensure, in conformity with their national law, that the appropriate administrative measures can be taken or administrative sanctions can be imposed against credit and financial institutions for infringements of the national provisions adopted pursuant to this Directive. Member States shall ensure that these measures or sanctions are effective, proportionate and dissuasive.

3. In the case of legal persons, Member States shall ensure that at least they can be held liable for infringements referred to in paragraph 1 which are committed for their benefit by any person, acting either individually or as part of an organ of the legal person, who has a leading position within the legal person, based on:

(a) a power of representation of the legal person;

(b) an authority to take decisions on behalf of the legal person, or

(c) an authority to exercise control within the legal person.

4. In addition to the cases already provided for in paragraph 3, Member States shall ensure that legal persons can be held liable where the lack of supervision or control by a person referred to in paragraph 3 has made possible the commission of the infringements referred to in paragraph 1 for the benefit of a legal person by a person under its authority.

CHAPTER VI

IMPLEMENTING MEASURES

Article 40

1. In order to take account of technical developments in the fight against money laundering or terrorist financing and to ensure uniform implementation of this Directive, the Commission may, in accordance with the procedure referred to in Article 41(2), adopt the following implementing measures:

(a) clarification of the technical aspects of the definitions in Article 3(2)(a) and (d), (6), (7), (8), (9) and (10);

(b) establishment of technical criteria for assessing whether situations represent a low risk of money laundering or terrorist financing as referred to in Article 11(2) and (5);

(c) establishment of technical criteria for assessing whether situations represent a high risk of money laundering or terrorist financing as referred to in Article 13;

(d) establishment of technical criteria for assessing whether, in accordance with Article 2(2), it is justified not to apply this Directive to certain legal or natural persons carrying out a financial activity on an occasional or very limited basis.

2. In any event, the Commission shall adopt the first implementing measures to give effect to paragraphs 1(b) and 1(d) by 15 June 2006.

3. The Commission shall, in accordance with the procedure referred to in Article 41(2), adapt the amounts referred to in Articles 2(1)(3)(e), 7(b), 10(1) and 11(5)(a) and (d) taking into

account Community legislation, economic developments and changes in international standards.

4. Where the Commission finds that a third country does not meet the conditions laid down in Article 11(1) or (2), Article 28(3), (4) or (5), or in the measures established in accordance with paragraph 1(b) of this Article or in Article 16(1)(b), or that the legislation of that third country does not permit application of the measures required under the first subparagraph of Article 31(1), it shall adopt a decision so stating in accordance with the procedure referred to in Article 41(2).

Article 41

1. The Commission shall be assisted by a Committee on the Prevention of Money Laundering and Terrorist Financing, hereinafter 'the Committee'.

2. Where reference is made to this paragraph, Articles 5 and 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof and provided that the implementing measures adopted in accordance with this procedure do not modify the essential provisions of this Directive.

The period laid down in Article 5(6) of Decision 1999/468/EC shall be set at three months.

3. The Committee shall adopt its Rules of Procedure.

4. Without prejudice to the implementing measures already adopted, the implementation of the provisions of this Directive concerning the adoption of technical rules and decisions in accordance with the procedure referred to in paragraph 2 shall be suspended four years after the entry into force of this Directive. On a proposal from the Commission, the European Parliament and the Council may renew the provisions concerned in accordance with the procedure laid down in Article 251 of the Treaty and, to that end, shall review them prior to the expiry of the four-year period.

CHAPTER VII

FINAL PROVISIONS

Article 42

By 15 December 2009, and at least at three-yearly intervals thereafter, the Commission shall draw up a report on the implementation of this Directive and submit it to the European Parliament and the Council. For the first such report, the Commission shall include a specific examination of the treatment of lawyers and other independent legal professionals.

Article 43

By 15 December 2010, the Commission shall present a report to the European Parliament and to the Council on the threshold percentages in Article 3(6), paying particular attention to the possible expediency and consequences of a reduction of the percentage in points (a)(i), (b)(i) and (b)(iii) of Article 3(6) from 25 % to 20 %. On the basis of the report the Commission may submit a proposal for amendments to this Directive.

Article 44

Directive 91/308/EEC is hereby repealed.

References made to the repealed Directive shall be construed as being made to this Directive and should be read in accordance with the correlation table set out in the Annex.

Article 45

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 15 December 2007. They shall forthwith communicate to the Commission the text of those provisions together with a table showing how the provisions of this Directive correspond to the national provisions adopted.

When Member States adopt those measures, they shall contain a reference to this Directive or be accompanied by such a refer-

ence on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

2. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

Article 46

This Directive shall enter into force on the 20th day after its publication in the *Official Journal of the European Union*.

Article 47

This Directive is addressed to the Member States.

Done at Strasbourg, 26 October 2005.

For the European Parliament
The President
J. BORRELL FONTELLES

For the Council
The President
D. ALEXANDER

ANNEX

CORRELATION TABLE

This Directive	Directive 91/308/EEC
Article 1(1)	Article 2
Article 1(2)	Article 1(C)
Article 1(2)(a)	Article 1(C) first point
Article 1(2)(b)	Article 1(C) second point
Article 1(2)(c)	Article 1(C) third point
Article 1(2)(d)	Article 1(C) fourth point
Article 1(3)	Article 1(C), third paragraph
Article 1(4)	
Article 1(5)	Article 1(C), second paragraph
Article 2(1)(1)	Article 2a(1)
Article 2(1)(2)	Article 2a(2)
Article 2(1)(3)(a), (b) and (d) to (f)	Article 2a(3) to (7)
Article 2(1)(3)(c)	
Article 2(2)	
Article 3(1)	Article 1(A)
Article 3(2)(a)	Article 1(B)(1)
Article 3(2)(b)	Article 1(B)(2)
Article 3(2)(c)	Article 1(B)(3)
Article 3(2)(d)	Article 1(B)(4)
Article 3(2)(e)	
Article 3(2)(f)	Article 1(B), second paragraph
Article 3(3)	Article 1(D)
Article 3(4)	Article 1(E), first paragraph
Article 3(5)	Article 1(E), second paragraph
Article 3(5)(a)	
Article 3(5)(b)	Article 1(E), first indent

This Directive	Directive 91/308/EEC
Article 3(5)(c)	Article 1(E), second indent
Article 3(5)(d)	Article 1(E), third indent
Article 3(5)(e)	Article 1(E), fourth indent
Article 3(5)(f)	Article 1(E), fifth indent, and third paragraph
Article 3(6)	
Article 3(7)	
Article 3(8)	
Article 3(9)	
Article 3(10)	
Article 4	Article 12
Article 5	Article 15
Article 6	
Article 7(a)	Article 3(1)
Article 7(b)	Article 3(2)
Article 7(c)	Article 3(8)
Article 7(d)	Article 3(7)
Article 8(1)(a)	Article 3(1)
Article 8(1)(b) to (d)	
Article 8(2)	
Article 9(1)	Article 3(1)
Article 9(2) to (6)	
Article 10	Article 3(5) and (6)
Article 11(1)	Article 3(9)
Article 11(2)	
Article 11(3) and (4)	
Article 11(5)(a)	Article 3(3)
Article 11(5)(b)	Article 3(4)
Article 11(5)(c)	Article 3(4)
Article 11(5)(d)	

This Directive	Directive 91/308/EEC
Article 12	
Article 13(1) and (2)	Article 3(10) and (11)
Article 13(3) to (5)	
Article 13(6)	Article 5
Article 14	
Article 15	
Article 16	
Article 17	
Article 18	
Article 19	
Article 20	Article 5
Article 21	
Article 22	Article 6(1) and (2)
Article 23	Article 6(3)
Article 24	Article 7
Article 25	Article 10
Article 26	Article 9
Article 27	
Article 28(1)	Article 8(1)
Article 28(2) to (7)	
Article 29	
Article 30(a)	Article 4, first indent
Article 30(b)	Article 4, second indent
Article 31	
Article 32	
Article 33	
Article 34(1)	Article 11(1) (a)
Article 34(2)	
Article 35(1), first paragraph	Article 11(1)(b), first sentence
Article 35(1), second paragraph	Article 11(1)(b) second sentence
Article 35(1), third paragraph	Article 11(1), second paragraph

This Directive	Directive 91/308/EEC
Article 35(2)	
Article 35(3)	
Article 36	
Article 37	
Article 38	
Article 39(1)	Article 14
Article 39(2) to (4)	
Article 40	
Article 41	
Article 42	Article 17
Article 43	
Article 44	
Article 45	Article 16
Article 46	Article 16

STANDARD
SUSPICIOUS ACTIVITY REPORT
UNITED KINGDOM

and guide to completing the forms

Version 2.1 - Appendix 1

Serious Organised Crime Agency
 PO Box 8000
 London
 SE11 5EN
 Tel: 020 7238 8282
 Fax: 020 7238 8286



SOURCE REGISTRATION DOCUMENT

IMPORTANT - THE DETAILS IN THIS FORM MUST BE PROVIDED WITH YOUR FIRST DISCLOSURE TO SOCA OR FOLLOWING ANY SUBSEQUENT CHANGE TO THOSE DETAILS.

Institution Name:

Institution Type:

Regulator:

Regulator ID:

Contact Details (1): Forename:

Surname:

Position:

Address:

Telephone Details:

Facsimile Details:

E-mail Address:

Contact Details (2): Forename:

(where applicable) Surname:

Position:

Address:


Telephone Details:

Facsimile Details:

E-mail Address:

Version 2.1 - Appendix 2

Serious Organised Crime Agency
 PO Box 8000
 London
 SE11 5EN
 Tel: 020 7238 8282
 Fax: 020 7238 8286



DISCLOSURE REPORT DETAILS: STANDARD REPORT:

Reporting Institution:

Your Ref: Disclosure Reason:

PoCA 2002: Terrorism Act 2000:

Branch/Office: Consent Required:

Disclosure Date: - - Type: New OR Update

DD MMM YYYY

Existing Disclosure ID/s: (where applicable)

Please use whichever sheets you feel are necessary and indicate below how many of each you are submitting.

REPORT SUMMARY:

Number of 'Subject Details' sheet appended relating to a Main Subject:

Number of 'Additional Details' sheets appended relating to Main Subject:

Number of 'Subjects Details' sheets appended relating to Associated Subject/s:

Number of 'Additional Details' sheets' appended relating to Associated Subject/s:

Number of 'Transaction Detail' sheet/s appended:

Number of 'Reason For Disclosure Sheets' appended:

Once completed please collate your sheets in the above mentioned order and then sequentially number your sheets at the bottom of each page. This will ensure that the information is processed in the correct sequence.

Total number of pages submitted including this Header:

■ **SUBJECT DETAILS:** Version 2.0 - Appendix 3 ■

Subject Type: Main Subject: **OR** Associated Subject: (number of)

Individual's Details:

Subject Status: Suspect: **OR** Victim:

Surname:

Forename 1:

Forename 2:

Occupation:

DoB: - - Gender: Male Female
DD MM YY

Title: Mr Mrs Miss Ms Other

Reason for Association of this subject to the Main Subject (for use only with Associated Subject details)

OR

Legal Entity's Details

Subject Status: Suspect: **OR** Victim:

Legal Entity Name:

Legal Entity No: VAT No:

Country of Reg:

Type of Business:

Reason for Association of this subject to the Main Subject (for use only with Associated Subject details)

■ **ADDITIONAL DETAILS:** Version 2.0 - Appendix 4 ■

Do these details refer to the Main Subject: **OR** to an Associated Subject
 (Please indicate the Associate's number where applicable)

Subject Name:

Premise No/Name: Current: Type:

Street:

City/Town:

Country: Post Code:

Premise No/Name: Current: Type:

Street:

City/Town:

Country: Post Code:

Premise No/Name: Current: Type:

Street:

City/Town:

Country: Post Code:

Information Type: <input type="text"/>	Unique Information Identifier: <input type="text"/>
Extra Information / Description <input type="text"/>	

Information Type: <input type="text"/>	Unique Information Identifier: <input type="text"/>
Extra Information / Description <input type="text"/>	

TRANSACTION DETAILS: (Complete if applicable)

Version 2.0 - Appendix 5

MAIN SUBJECT ACCOUNT SUMMARY

Institution Name: <input type="text"/>	
Account Name: <input type="text"/>	
Sort Code: <input type="text"/>	Account No /Identifier: <input type="text"/>
Business Relationship Commenced: (DD-MMM-YYYY) <input type="text"/> - <input type="text"/> - <input type="text"/>	Acct Bal: <input type="text"/>
Business Relationship Finished: (DD-MMM-YYYY) <input type="text"/> - <input type="text"/> - <input type="text"/>	Bal Date: (DD-MMM-YYYY) <input type="text"/> - <input type="text"/> - <input type="text"/>
Turnover Period: <input type="text"/>	Credit Turnover: <input type="text"/>
	Debit Turnover: <input type="text"/>

TRANSACTION/S

Activity Type: <input type="text"/>	Activity Date: (DD-MMM-YYYY) <input type="text"/> - <input type="text"/> - <input type="text"/>
Amount: <input type="text"/>	Currency: <input type="text"/> Credit: <input type="radio"/> or Debit: <input type="radio"/>
Other party name: <input type="text"/>	Account No/Identifier: <input type="text"/>
Institution Name or Sort Code: <input type="text"/>	<input type="text"/>

Activity Type: <input type="text"/>	Activity Date: (DD-MMM-YYYY) <input type="text"/> - <input type="text"/> - <input type="text"/>
Amount: <input type="text"/>	Currency: <input type="text"/> Credit: <input type="radio"/> or Debit: <input type="radio"/>
Other party name: <input type="text"/>	Account No/Identifier: <input type="text"/>
Institution Name or Sort Code: <input type="text"/>	<input type="text"/>

Activity Type: <input type="text"/>	Activity Date: (DD-MMM-YYYY) <input type="text"/> - <input type="text"/> - <input type="text"/>
Amount: <input type="text"/>	Currency: <input type="text"/> Credit: <input type="radio"/> or Debit: <input type="radio"/>
Other party name: <input type="text"/>	Account No/Identifier: <input type="text"/>
Institution Name or Sort Code: <input type="text"/>	<input type="text"/>

Activity Type: <input type="text"/>	Activity Date: (DD-MMM-YYYY) <input type="text"/> - <input type="text"/> - <input type="text"/>
Amount: <input type="text"/>	Currency: <input type="text"/> Credit: <input type="radio"/> or Debit: <input type="radio"/>
Other party name: <input type="text"/>	Account No/Identifier: <input type="text"/>
Institution Name or Sort Code: <input type="text"/>	<input type="text"/>

REASON FOR DISCLOSURE:

Version 2.0 - Appendix 6

Main Subject Name: (cross reference purposes) <input type="text"/>
--

Report Activity Assessment (Please use only where you know or suspect what the offence behind the reported activity may be)

Drugs: Missing Trader, Inter Community (VAT) Fraud: Immigration: Tobacco/Alcohol Excise Fraud:

Personal Tax Fraud: Corporate Tax Fraud: Other Offences:

Reason for Disclosure:

REASON FOR DISCLOSURE CONTINUATION:

Version 2.0 - Appendix 8

Main Subject Name:
(cross reference purposes)

Reason for Disclosure Continuation:

Page of

SERIOUS ORGANISED CRIME AGENCY

GUIDE TO COMPLETING DISCLOSURE FORMS

The guidance notes explain what information is required in the Standard form template and are to be read in conjunction with the form itself. If you are not completing the form using one of the electronic methods outlined above, the form should be completed on the computer-generated template, which is available to download from the SOCA website, but if this is not possible it should be typed onto a paper copy. A number of fields within the computer-generated template can be completed by selecting options from dropdown menus.

It is important that the relevant information is completed within the appropriate fields and not merely placed within the 'Reasons for Suspicion' field.

There are a number of fields that should be completed in order for a report to be accepted by SOCA. These fields are: Your Ref (even if none), Disclosure Type, New or Update, Source ID, Source Outlet ID, Today's Date, (Main Subject) Surname or Company Name and Reasons for Suspicion'. Following this, according to the additional information you have available, a number of fields within each section must be completed if you are filling in that section and are identified below in bold italics.

For a more detailed explanation of the template itself, please contact the SOCA SAR Team at PO Box 8000, London, SE11 5EN.

Suspicious Activity Report

- Main subject (person or company)
- Address
- ID Information
- Disclosed account details
- Individual transactions with counterparty account details
- Associated subject (person and company)
- (Associated subject) address
- (Associated subject) ID information
- Reason for suspicion

Your ref:

The reference number or alphanumeric identifier that you allocate to the SAR within your own filing system

Sheet no:

The number of pages used to complete the SAR?

Disclosure type:

This field should contain the type of offence under which you report (i.e. Crime, Drugs or Terrorism)

Disclosure date:

The date on which the original report is made within your institution New or Update: New is any new suspicious activity or any further activity on a previously reported account/activity or arrangement. An update

is any further information that is not a transaction, on a previously reported account/activity or arrangement, e.g. a new address of a subject

Existing disclosure ID:

If you have entered 'Update' in the previous field, please enter here any reference number SOCA may previously have supplied relating to the subject in question

Constructive trust:

Fill this check box if the report relates to an issue of constructive trust. Further information: Fill this check box to indicate that you retain further information relating to the report that may be of interest to SOCA or another financial investigator. For example, if your disclosure relates to a mortgage application, it may not always be necessary to provide the full documentation. In this case, indicate its existence here and provide a concise description in the 'Reasons for Suspicion' field. DO NOT SEND THE FURTHER INFORMATION WITH YOUR FORM.

Source ID:

The name of your institution

Source outlet ID:

The name (or sort code) of the branch office from which the report originates

Today's date:

Date report submitted to SOCA (Automatic date field)

[Back to top](#)

Main subject (person or company)

This information describes the individual (or company) on whom you wish to report.

Surname:

Subject's family name

Forenames:

Subject's forenames

Title:

Title of subject (Mr, Mrs, Dr etc)

Date of birth:

Date of birth of subject

Gender:

Gender of subject

Occupation:

Occupation of subject

Employer:

Subject's employer

Or:

Company Name:

Company name of subject

Company No:

Company registration number of subject

Type of business:

Type of business of subject

VAT no:

VAT number of subject

Country of Registration:

Country of registration of subject

[Back to top](#)

Address

Number, street, city/town, county, country.

Full address of subject

Post code:

Post Code of address of subject

Type:

Type of address of subject (i.e. home, accommodation, trading etc)

Current:

Is the address of the subject current, Yes or No

[Back to top](#)

ID Information

ID Information:

Describes the type of identification offered or taken (e.g. driving licence)

Unique information ID:

Give details of the identification taken (e.g. driving licence number)

Extra information / description:

Give any further information relating to the identification taken, which may be relevant or of use (e.g. if passport, the country of issue)

Other information:

Give any further details that help to identify the subject

[Back to top](#)

Disclosed account details

This information describes an account with which the subject or suspicious activity is connected.

FI ID:

The name of the financial institution that holds the subject's account

Sort Code:

The sort code of the branch office that holds the subject's account

Opened:

Date account opened

Closed:

Date account closed (if applicable)

Turn' Cd:

Turnover credit

Turn' Db:

Turnover debit

Acct. Name:

Account name

Acct No:

Account number

Acct Bal:

Account balance

Bal Date:

Date of the balance

Turn Pd:

Turnover period

[Back to top](#)

Individual transactions with counterparty account details

This section contains details of the transaction, or series of transactions that have aroused your suspicion, and details of the counterparties involved.

Date:

The date of the transaction

Amount:

The amount of the transaction

Currency:

The currency concerned in the transaction (e.g. GBP, USD, DEM etc)

Cr/Db:

This field stipulates whether the transaction constitutes a credit or debit in relation to the account identified above

Type:

The type of transaction conducted (e.g. cash, cheque, electronic transfer, mortgage etc)

Notes:

This field is available for further information relating to the transaction identified above

FI ID:

The name of the institution that holds the counterparty account, if applicable

Sort Code:

The sort code of the branch office that holds the counterparty's account

Acct. Name:

The name of the counterparty

Acct. No:

The counterparty's account number

[Back to top](#)

Associated subject (person and company)

This information describes the person(s) or companies with which the subject or suspicious activity. It is a person or company that is linked to the main person/company in some direct way and is involved in the suspicious activity. Include the financial institution responsible for that account if it is involved in your suspicions.

Surname:

The associated subject's family name

Forenames:

The associated subject's forenames

Title:

Title of associated subject (Mr, Mrs, Dr etc)

Date of birth:

Date of birth of associated subject

Gender:

Gender of associated subject

Occupation:

Occupation of associated subject

Employer:

Associated subjects employer

Reason for association:

Give details of the connection between the Main Subject and associate subject

Or:

Company name:

The name of the associate company

Company no:

Company number of associated subject

Type of business:

Type of business of associated subject

VAT no:

VAT number of associated subject

Country of registration:

Country of registration of associated subject

Reason for association:

Give details of the connection between the Main Subject and associate subject

Or:

(Associated) subject already exists as main subject of a previous report and is provided for use if you have previously reported on the associated subject.

Existing disclosure ID:

The reference number which SOCA may have provided in relation to previous reports, relating to the associated subject

Your Ref:

The reference number or alphanumeric identifier that you allocated within your own file system to the previous report on the associated subject

Reason for association:

Details of the connection between the Main Subject and associate subject

[Back to top](#)

(Associated subject) address

Number, street, city/town, county, country:

Full address of associated subject

Post code:

Post code of address of associated subject

Type:

Type of address of associated subject (i.e. home, accommodation, trading etc)

Current:

Is the address of the associated subject current, Yes or No

[Back to top](#)

(Associated subject) ID information

ID information:

Describes the type of Identification offered or taken (e.g. driving licence)

Unique information ID:

Give details of the Identification taken (e.g. driving licence number)

Extra information/description:

Give any further information relating to the Identification taken, which may be relevant or of use (e.g. if passport, country of origin)

General information:

Give any further details that help to identify the subject

[Back to top](#)

Reason for suspicion

This section requires a clear and thorough explanation of the grounds for your suspicion. (Submissions that do not provide reasons for suspicion cannot be accepted as a SAR by SOCA).

For further information contact the SOCA UK Financial Intelligence Unit (UKFIU) SAR Team at PO Box 8000, London, SE11 5EN

LIMITED INTELLIGENCE VALUE

SUSPICIOUS ACTIVITY REPORT

UNITED KINGDOM

and guidance notes to completing the forms

Version 2.1 - Appendix 7

Serious Organised Crime Agency PO Box 8000 London SE11 5EN Tel: 020 7238 8282 Fax: 020 7238 8286	
---	---

PROCEEDS OF CRIME ACT 2002 - LIMITED INTELLIGENCE VALUE REPORT

Reporting Institution: <input type="text"/>	Disclosure Date: <input type="text"/> - <input type="text"/> - <input type="text"/>
Your Ref: <input type="text"/>	DD - MMM - YYYY
Branch/Office: <input type="text"/>	

SUBJECT DETAILS:

Individual's Details: Subject Status: Suspect : **OR** Victim:

Surname:

Forename:

DoB: - - Gender: Male Female

Title: Mr Mrs Miss Ms Other

Legal Entity Details: Subject Status: Suspect : **OR** Victim:

Legal Entity Name:

Legal entity No: VAT No:

REASON FOR DISCLOSURE:

APPENDIX SEVEN

Guidance Notes for the completion of the SOCA Regulated Sector Suspicious Activity Report
 Proceeds of Crime Act 2002 - Limited Intelligence Value Report

Content

- Scope and Purpose Statement
- 5 Limited Intelligence Value Report
 Examples of relevant circumstances suitable for such reports
- Completion Instructions:-
 'Source Registration Document' (Module/Appendix 1)
- 8 Completion Instructions:-
 'Limited Intelligence Value Report' (Module/Appendix 7)
 (Reporting Institution Details and Subject Details)
- Completion Instructions:-
 Reason for Disclosure Continuation Sheet (Module/Appendix 8)
 (Reason for Disclosure Continuation)

Guidance Notes for the completion of the SOCA Regulated Sector Suspicious Activity Report

Proceeds of Crime Act 2002 - Limited Intelligence Value Report

Scope and Purpose

This document provides guidance for the completion of authorised and protected disclosures, under sections 337 and 338 of the Proceeds of Crime Act (2002), categorised as 'Limited Intelligence Value Reports'. This guidance should be read alongside the Limited Intelligence Value Report (Appendix 7) which has been issued by SOCA. Both the Form and Guidance have been completed following consultation with organisations representing the Regulated Sector. **Please note that Limited Intelligence Value Reports should only be made under the Proceeds of Crime Act (PoCA). Any reports being made under the Terrorism Act (2000) should be Standard Reports.**

The Form has not been prescribed by the Secretary of State and therefore is not mandatory. However the Form was agreed by NCIS (a SOCA pre-cursor agency) and organisations representing the Regulated Sector as the preferred format for all reports. The Form has been designed to reflect the different needs of the sectors as well as SOCA's requirement to handle the disclosures as efficiently and effectively as possible.

Although none of the fields in the form is mandatory, since the format is not prescribed, those submitting disclosures should take account of regulatory and sectoral approved guidance. SOCA's feedback to reporting institutions will assess the quality of reporting against relevant guidance.

How to obtain the new Forms and Guidance

Those organisations which currently use the Money.web system or Bulk File submission should continue to submit reports electronically, using the existing input screens or reporting format. Additionally SAR Online, a new internet based reporting mechanism will be available from April 2006.

Organisations not able to use Money.web, Bulk File Submission or SAR Online, are advised to obtain a copy of the preferred Forms. Those reporters who wish to complete reports on their own computer should download the Form(s) from the SOCA website (www.soca.gov.uk).

If you wish to complete a report by hand you will need to request a special version of the Form by telephoning 020 7238 8282. **Please do not complete the version of the Form downloaded from the main SOCA website (www.soca.gov.uk) by hand.**

Sending your report to SOCA

Those organisations which currently use the money.web system or Bulk File submission method, should continue to submit reports in the same way.

Other organisations will need to submit reports by fax to 0207 238 8286 or by post to PO Box 8000, London SE11 5EN. Please do not email completed disclosures to SOCA without encryption.

Report Structure

These Guidance Notes are provided to explain the various fields within the Report and assist you in its completion and should be read alongside the Report Forms themselves.

The Form has been designed to be read by Image Character Recognition (ICR) technology. Therefore any amendments or additions outside the structure of the Form will significantly hamper SOCA's capability to process the disclosure efficiently.

Guidance Notes for the completion of the SOCA Regulated Sector Suspicious Activity Report

Proceeds of Crime Act 2002 - Limited Intelligence Value Report

Limited Intelligence Value Reports

SOCA recognises that POCA results in reports being required in some circumstances where, individually, there is likely to be limited intelligence value to law enforcement, although wider analysis of such reports may provide useful data. The table below provides guidance on the types of circumstance that are appropriate for abbreviated information to be provided in the form of a Limited Intelligence Value report. SOCA reserves the right, in all cases, to ask for the Standard Report format to be used and will monitor disclosures submitted to ensure that Limited Intelligence Value reporting is not exploited as a 'short cut' where its use is not justified.

Type	Detail	Comments
1 Certain classes of crimes committed overseas	This is intended to apply where the suspicious activity takes place outside the UK and:- <ul style="list-style-type: none"> Is not a criminal offence in the jurisdiction where committed, and Relates either to local differences in regulation or social and cultural practices 	A Limited Intelligence Value Report is <u>not</u> appropriate to report money laundering relating to serious tax evasion or occasions where the underlying offence is a serious crime such as terrorism, offences relating to drugs, paedophilia etc. In these circumstances, a full report is appropriate. Please note that s102 of SOCAP 2005 (not yet enacted) will remove certain crimes from reporting obligations. This will have the effect of defining the types of crime reportable in the context of jurisdictions etc.
2.Minor irregularities where there is nothing to suggest that these are the result of dishonest behaviour.	Balance discrepancies and minor credit balances not returned because of the administrative costs involved, or other small discrepancies which are judged to have resulted from a mistake rather than dishonest behaviour.	If reporting institutions are satisfied that no criminal property is involved (as defined by s340 (3) of the Proceeds of Crime Act, 2002), they may conclude that a report is not required. However where reporting institutions feel obliged to make a disclosure, a Limited Intelligence Value report is appropriate.
3 The subject of the report cannot be deduced from the information to hand and the proceeds have disappeared without trace.	This would include bank raids, driving away from a petrol station without paying, shoplifting, retail shrinkage and various cheque and credit card frauds.	Section 330 of POCA (as amended) means that such reports should not be made unless the Suspect, or the means to identify the Subject, is known.

**Guidance Notes for the completion of the SOCA Regulated Sector
Suspicious Activity Report**

Proceeds of Crime Act 2002 - Limited Intelligence Value Report

<p>4 Accountants, auditors and tax advisers. Multiple instances of suspicion arising during one audit: "Aggregation of incidents to form one report"</p>	<p>Multiple incidents may be aggregated within a single Limited Intelligence Value Report provided that:-</p> <ul style="list-style-type: none"> • One or more of the other categories in this table for limited intelligence value reporting is met, for example number three (above): bank raids, driving away from a petrol station without paying, shoplifting, retail shrinkage and various cheque and credit card frauds; • The reason for the aggregate report is summarised; • Aggregate reports relate to a single audit only. 	<p>The Act refers to reports being made "as soon as practicable". SOCA accepts that this will not always mean "immediately" and is content to receive aggregate Limited Intelligence Value Reports within one month of the completion of an audit, provided that during the assignment no time sensitive information is discovered (that may, for example, allow the recovery of proceeds of crime if communicated immediately).</p> <p>Reporters should note that a Standard Report is appropriate should the issue of a Hansard (CoP9) letter by the Inland Revenue, taken with such other information as may be available, cause (or provide reasonable grounds for) knowledge or suspicion of money laundering.</p>
<p>5 Law enforcement prosecutor, regulator or other Government agency already aware of an offence that also happens to be an instance of suspected money laundering</p>	<p>This category is intended to capture a range of regulatory/procedural offences. Examples include health and safety offences, environmental offences, and failure to file annual returns with the Companies Registrar.</p>	<p>Provided the caveat of "no additional information" is adhered to, a Limited Intelligence Value report is appropriate.</p> <p>However, any knowledge or suspicion of money laundering relating to serious crime or tax evasion, including cases covered by the Hansard procedure, should be reported in a Standard Report.</p>
<p>6 Section 167 (3) Customs and Excise Management Act 1979</p>	<p>This makes the submission of an incorrect VAT or Customs return, however innocent, a criminal offence.</p>	<p>It is the position of SOCA that a disclosure is not required for innocent error in these circumstances.</p> <p>Where the person knows of the omission and does not rectify the situation there will be a duty to report. Where reporting institutions feel obliged to make a disclosure, a Limited Intelligence Value report is appropriate.</p>

**Guidance Notes for the completion of the SOCA Regulated Sector
Suspicious Activity Report**

Proceeds of Crime Act 2002 - Limited Intelligence Value Report

<p>7 Reporting institution served with a Court Order, which prompts suspicion.</p>		<p>A Limited Intelligence Value report is appropriate except where the suspicion and report relate to matters <u>not</u> covered by the Court Order letter, in which case a report on the Standard Form should be submitted.</p>
<p>8 Where the benefit from criminal conduct is in the form of cost savings, such as breaches of employment law and the illegal copying or distribution of software licences within a company.</p>		<p>However If there are funds or criminal property to arrange the transfer of, and which may require consent to carry out a prohibited act, then a Standard form must be completed.</p>

Guidance Notes for the completion of the SOCA Regulated Sector Suspicious Activity Report

Proceeds of Crime Act 2002 - Limited Intelligence Value Report

Completion Instructions

Source Registration Document (Module 1)

In order to record disclosures and correspond accurately and in a timely manner with the regulated sector, SOCA needs accurate contact details of each reporting organisation. A **Source Registration Document** has been constructed to capture this information as concisely as possible. SOCA already holds such details for organisations which have previously disclosed, therefore **this sheet should only be used by organisations that have never previously reported and then only when making their first report.** It will not be required for each subsequent disclosure. However, **all organisations should use the source registration document to update SOCA about any changes to their contact details in order that SOCA's records can be accurately maintained.**

- Institution Name** Please provide details of the Registered and/or Trading name of the company or individual making the report.
- Institution Type** Please provide details of the type of company or individual making the report, e.g. Money Transmission Agent, Bank, Estate Agent etc.
- Regulator** Please provide details of your regulator, where applicable, (e.g. FSA, Gaming Board of Great Britain etc)
- Regulator ID** Please provide details of your regulator's Identity Number, where known to you.
- Contact Details (1)** This will be SOCA's primary point of contact with you.
 - Forename** Please provide full details of your Forename/s.
 - Surname** Please provide full details of your Surname.
 - Position** Please provide details as to the position you hold within your employer, where applicable.
 - Address** Please provide your full postal address details (inc Post Code).
 - Telephone Details** Please provide details of your principal contact number.
 - E-mail Address** Please provide details where applicable. The ability to use this medium will enhance the speed of delivery of our correspondence with you.
- Contact Details (2)** (where applicable) This will be SOCA's point of contact with you in the absence of the above detailed individual, if applicable.
 - Name** As above.
 - Position** As above.
 - Address** As above.
 - Telephone Details** As above.
 - E-mail Address** As above.

Guidance Notes for the completion of the SOCA Regulated Sector Suspicious Activity Report

Proceeds of Crime Act 2002 - Limited Intelligence Value Report

Limited Intelligence Value Report (Module 7)

Reporting Institution

Please provide details of the company or individual **making** the report. If a Money Laundering Reporting Officer (MLRO) is completing the form it is not essential at any point to mention by name the person making the initial disclosure.

Your Reference

Please provide details of your own reference number relevant to the disclosure in question. **This is an important field as the information supplied will be quoted by us SOCA in any correspondence with you relating to this disclosure.** We are shortly to explore a system change so that our automated response letters will quote **only** your reference number (alongside our own Intelligence Reference Number).

Branch/Office

This information will enable SOCA to ascertain which of your outlets is reporting the activity, assisting SOCA decide which law enforcement agency to allocate the disclosure to.

Disclosure Date

The date upon which you submit your report to SOCA. The format DD/MMM/YYYY has been used to prevent any transposition of Day and Month. Please insert two digits in the DD field to state the day, three letters in the MMM field (for example, JAN for January) and four digits to show the year in the YYYY field.

Subject Details

This is the Person/Legal Entity about whom/which the report is being made. Normally, reporters will be in a position to complete one of these fields, although in some circumstances this is not the case. For example you may be reporting a fraud where the perpetrator is unknown

This section of the sheet can be used to refer to an Individual or a Legal Entity. **However only one of these sections should be completed.** This sheet should not be used for both an individual and a Legal Entity at the same time.

Subject Status

Please indicate **only one** box from 'Suspect' or 'Victim'.

Suspect should be ticked if you know or suspect or have reasonable grounds for knowing or suspecting that this person is engaged in money laundering.

Victim is the person or entity who/which is harmed by or loses as a result of the criminal activity which you are reporting. To ensure that any intrusion against a victim's privacy is minimised, the victim's details should not, ideally, be included in subject fields. **The personal details of victims should only be included if, in the judgement of the nominated officer, the details are essential to understanding the activity being reported.**

**Guidance Notes for the completion of the SOCA Regulated Sector
Suspicious Activity Report**

Proceeds of Crime Act 2002 - Limited Intelligence Value Report

PLEASE COMPLETE EITHER THE INDIVIDUAL'S DETAILS SECTION OF THE SHEET OR THE LEGAL ENTITY SECTION. PLEASE DO NOT COMPLETE BOTH.

- Surname** Please provide details, as appropriate.
- Forename 1** Please provide details, as appropriate.
- Date of Birth** This is an important field. Date of birth information helps law enforcement to positively identify individuals when cross-matching personal data. The format DD/MMM/YYYY has been used to prevent any transposition of Day and Month. Please insert two digits in the DD field to state the day, three letters in the MMM field (for example, JAN for January) and four digits to show the year in the YYYY field.
- Gender** Please select from options provided.
- Title** Please select from options provided. If the correct title is not shown, please specify the relevant title within the 'Other' field. *Appropriate options are provided with the Field Values List.*
- OR**
- Legal Entity Name** Please provide details as appropriate, e.g. a Company or Charity Name.
- Legal Entity Number** Please provide details as appropriate, e.g. a Company or charity Number.
- VAT Number** Please provide details as appropriate.

Reason for Disclosure

This area is free text and should include any information not already provided which you feel is relevant to your Report. It should provide details of the reason(s) why you have knowledge or suspicion or reasonable grounds for knowledge or suspicion that another person is engaged in money laundering and why you feel that a Limited Value Report is suitable.

Reason for Disclosure Continuation Sheet (Module/Appendix 8)

Where required, please use this section to continue your reasons for knowledge or suspicion, where the space provided within Appendix 7 is insufficient. Multiples of this module can be utilised as required.

Please ensure that you complete the Main Subject Name at the top of any of these modules completed in order that we may cross reference this module to the rest of your report.

L 157/38

EN

Official Journal of the European Union

26.6.2003

**COUNCIL DIRECTIVE 2003/48/EC
of 3 June 2003**

on taxation of savings income in the form of interest payments

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 94 thereof,

Having regard to the proposal from the Commission ⁽¹⁾,

Having regard to the opinion of the European Parliament ⁽²⁾,

Having regard to the opinion of the European Economic and Social Committee ⁽³⁾,

Whereas:

- (1) Articles 56 to 60 of the Treaty guarantee the free movement of capital.
- (2) Savings income in the form of interest payments from debt claims constitutes taxable income for residents of all Member States.
- (3) By virtue of Article 58(1) of the Treaty Member States have the right to apply the relevant provisions of their tax law which distinguish between taxpayers who are not in the same situation with regard to their place of residence or with regard to the place where their capital is invested, and to take all requisite measures to prevent infringements of national law and regulations, in particular in the field of taxation.
- (4) In accordance with Article 58(3) of the Treaty, the provisions of Member States' tax law designed to counter abuse or fraud should not constitute a means of arbitrary discrimination or a disguised restriction on the free movement of capital and payments as established by Article 56 of the Treaty.
- (5) In the absence of any coordination of national tax systems for taxation of savings income in the form of interest payments, particularly as far as the treatment of interest received by non-residents is concerned, residents of Member States are currently often able to avoid any form of taxation in their Member State of residence on interest they receive in another Member State.
- (6) This situation is creating distortions in the capital movements between Member States, which are incompatible with the internal market.
- (7) This Directive builds on the consensus reached at the Santa Maria da Feira European Council of 19 and 20 June 2000 and the subsequent Ecofin Council meetings of 26 and 27 November 2000, 13 December 2001 and 21 January 2003.
- (8) The ultimate aim of this Directive is to enable savings income in the form of interest payments made in one Member State to beneficial owners who are individuals resident in another Member State to be made subject to effective taxation in accordance with the laws of the latter Member State.
- (9) The aim of this Directive can best be achieved by targeting interest payments made or secured by economic operators established in the Member States to or for the benefit of beneficial owners who are individuals resident in another Member State.
- (10) Since the objective of this Directive cannot be sufficiently achieved by the Member States, because of the lack of any coordination of national systems for the taxation of savings income, and can therefore be better achieved at Community level, the Community may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty. In accordance with the principle of proportionality, as set out in that Article, this Directive confines itself to the minimum required in order to achieve those objectives and does not go beyond what is necessary for that purpose.
- (11) The paying agent is the economic operator who pays interest to or secures the payment of interest for the immediate benefit of the beneficial owner.
- (12) In defining the notion of interest payment and the paying agent mechanism, reference should be made, where appropriate, to Council Directive 85/611/EEC of 20 December 1985 on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS) ⁽⁴⁾.
- (13) The scope of this Directive should be limited to taxation of savings income in the form of interest payments on debt claims, to the exclusion, *inter alia*, of the issues relating to the taxation of pension and insurance benefits.
- (14) The ultimate aim of bringing about effective taxation of interest payments in the beneficial owner's Member State of residence for tax purposes can be achieved through the exchange of information concerning interest payments between Member States.

⁽¹⁾ OJ C 270 E, 25.9.2001, p. 259.

⁽²⁾ OJ C 47 E, 27.2.2003, p. 553.

⁽³⁾ OJ C 48, 21.2.2002, p. 55.

⁽⁴⁾ OJ L 375, 31.12.1985, p. 3. Directive as last amended by Directive 2001/108/EC of the European Parliament and of the Council (OJ L 41, 13.2.2002, p. 35).

- (15) Council Directive 77/799/EEC of 19 December 1977 concerning mutual assistance by the competent authorities of the Member States in the field of direct and indirect taxation (*) already provides a basis for Member States to exchange information for tax purposes on the income covered by this Directive. It should continue to apply to such exchanges of information in addition to this Directive insofar as this Directive does not derogate from it.
- (16) The automatic exchange of information between Member States concerning interest payments covered by this Directive makes possible the effective taxation of those payments in the beneficial owner's Member State of residence for tax purposes in accordance with the national laws of that State. It is therefore necessary to stipulate that Member States which exchange information pursuant to this Directive should not be permitted to rely on the limits to the exchange of information as set out in Article 8 of Directive 77/799/EEC.
- (17) In view of structural differences, Austria, Belgium and Luxembourg cannot apply the automatic exchange of information at the same time as the other Member States. During a transitional period, given that a withholding tax can ensure a minimum level of effective taxation, especially at a rate increasing progressively to 35 %, these three Member States should apply a withholding tax to the savings income covered by this Directive.
- (18) In order to avoid differences in treatment, Austria, Belgium and Luxembourg should not be obliged to apply automatic exchange of information before the Swiss Confederation, the Principality of Andorra, the Principality of Liechtenstein, the Principality of Monaco and the Republic of San Marino ensure effective exchange of information on request concerning payments of interest.
- (19) Those Member States should transfer the greater part of their revenue of this withholding tax to the Member State of residence of the beneficial owner of the interest.
- (20) Those Member States should provide for a procedure allowing beneficial owners resident for tax purposes in other Member States to avoid the imposition of this withholding tax by authorising their paying agent to report the interest payments or by presenting a certificate issued by the competent authority of their Member State of residence for tax purposes.
- (21) The Member State of residence for tax purposes of the beneficial owner should ensure the elimination of any double taxation of the interest payments which might result from the imposition of this withholding tax in accordance with the procedures laid down in this Directive.

It should do so by crediting this withholding tax up to the amount of tax due in its territory and by reimbursing to the beneficial owner any excess amount of tax withheld. It may, however, instead of applying this tax credit mechanism, grant a refund of the withholding tax.

- (22) In order to avoid market disruption, this Directive should, during the transitional period, not apply to interest payments on certain negotiable debt securities.
- (23) This Directive should not preclude Member States from levying other types of withholding tax than that referred to in this Directive on interest arising in their territories.
- (24) So long as the United States of America, Switzerland, Andorra, Liechtenstein, Monaco, San Marino and the relevant dependent or associated territories of the Member States do not all apply measures equivalent to, or the same as, those provided for by this Directive, capital flight towards these countries and territories could imperil the attainment of its objectives. Therefore, it is necessary for the Directive to apply from the same date as that on which all these countries and territories apply such measures.
- (25) The Commission should report every three years on the operation of this Directive and propose to the Council any amendments that prove necessary in order better to ensure effective taxation of savings income and to remove undesirable distortions of competition.
- (26) This Directive respects the fundamental rights and principles which are recognised, in particular, by the Charter of Fundamental Rights of the European Union,

HAS ADOPTED THIS DIRECTIVE:

CHAPTER I

INTRODUCTORY PROVISIONS

Article 1

Aim

- The ultimate aim of the Directive is to enable savings income in the form of interest payments made in one Member State to beneficial owners who are individuals resident for tax purposes in another Member State to be made subject to effective taxation in accordance with the laws of the latter Member State.
- Member States shall take the necessary measures to ensure that the tasks necessary for the implementation of this Directive are carried out by paying agents established within their territory, irrespective of the place of establishment of the debtor of the debt claim producing the interest.

Article 2

Definition of beneficial owner

- For the purposes of this Directive, 'beneficial owner' means any individual who receives an interest payment or any individual for whom an interest payment is secured, unless he provides evidence that it was not received or secured for his own benefit, that is to say that:
 - he acts as a paying agent within the meaning of Article 4(1); or
 - he acts on behalf of a legal person, an entity which is taxed on its profits under the general arrangements for business taxation, an UCITS authorised in accordance with Directive 85/611/EEC or an entity referred to in Article 4(2) of this Directive and, in the last mentioned case, discloses the name and address of that entity to the economic operator making the interest payment and the latter communicates such information to the competent authority of its Member State of establishment, or
 - he acts on behalf of another individual who is the beneficial owner and discloses to the paying agent the identity of that beneficial owner in accordance with Article 3(2).
- Where a paying agent has information suggesting that the individual who receives an interest payment or for whom an interest payment is secured may not be the beneficial owner, and where neither paragraph 1(a) nor 1(b) applies to that individual, it shall take reasonable steps to establish the identity of the beneficial owner in accordance with Article 3(2). If the paying agent is unable to identify the beneficial owner, it shall treat the individual in question as the beneficial owner.

Article 3

Identity and residence of beneficial owners

- Each Member State shall, within its territory, adopt and ensure the application of the procedures necessary to allow the paying agent to identify the beneficial owners and their residence for the purposes of Articles 8 to 12.

Such procedures shall comply with the minimum standards established in paragraphs 2 and 3.

- The paying agent shall establish the identity of the beneficial owner on the basis of minimum standards which vary according to when relations between the paying agent and the recipient of the interest are entered into, as follows:
 - for contractual relations entered into before 1 January 2004, the paying agent shall establish the identity of the beneficial owner, consisting of his name and address, by using the information at its disposal, in particular pursuant to the regulations in force in its State of establishment and to Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering (*);
 - for contractual relations entered into, or transactions carried out in the absence of contractual relations, on or after 1 January 2004, the paying agent shall establish the

(*) OJ L 166, 28.6.1991, p. 77. Directive as last amended by Directive 2001/97/EC of the European Parliament and of the Council (OJ L 344, 28.12.2001, p. 76).

identity of the beneficial owner, consisting of the name, address and, if there is one, the tax identification number allocated by the Member State of residence for tax purposes. These details shall be established on the basis of the passport or of the official identity card presented by the beneficial owner. If it does not appear on that passport or on that official identity card, the address shall be established on the basis of any other documentary proof of identity presented by the beneficial owner. If the tax identification number is not mentioned on the passport, on the official identity card or any other documentary proof of identity, including, possibly, the certificate of residence for tax purposes, presented by the beneficial owner, the identity shall be supplemented by a reference to the latter's date and place of birth established on the basis of his passport or official identification card.

- The paying agent shall establish the residence of the beneficial owner on the basis of minimum standards which vary according to when relations between the paying agent and the recipient of the interest are entered into. Subject to the conditions set out below, residence shall be considered to be situated in the country where the beneficial owner has his permanent address:

- for contractual relations entered into before 1 January 2004, the paying agent shall establish the residence of the beneficial owner by using the information at its disposal, in particular pursuant to the regulations in force in its State of establishment and to Directive 91/308/EEC;
- for contractual relations entered into, or transactions carried out in the absence of contractual relations, on or after 1 January 2004, the paying agent shall establish the residence of the beneficial owner on the basis of the address mentioned on the passport, on the official identity card or, if necessary, on the basis of any documentary proof of identity presented by the beneficial owner and according to the following procedure: for individuals presenting a passport or official identity card issued by a Member State who declare themselves to be resident in a third country, residence shall be established by means of a tax residence certificate issued by the competent authority of the third country in which the individual claims to be resident. Failing the presentation of such a certificate, the Member State which issued the passport or other official identity document shall be considered to be the country of residence.

Article 4

Definition of paying agent

- For the purposes of this Directive, 'paying agent' means any economic operator who pays interest to or secures the payment of interest for the immediate benefit of the beneficial owner, whether the operator is the debtor of the debt claim which produces the interest or the operator charged by the debtor or the beneficial owner with paying interest or securing the payment of interest.

(*) OJ L 336, 27.12.1977, p. 15. Directive as last amended by the 1994 Act of Accession.

2. Any entity established in a Member State to which interest is paid or for which interest is secured for the benefit of the beneficial owner shall also be considered a paying agent upon such payment or securing of such payment. This provision shall not apply if the economic operator has reason to believe, on the basis of official evidence produced by that entity, that:

- (a) it is a legal person, with the exception of those legal persons referred to in paragraph 5; or
- (b) its profits are taxed under the general arrangements for business taxation; or
- (c) it is an UCITS recognised in accordance with Directive 85/611/EEC.

An economic operator paying interest to, or securing interest for, such an entity established in another Member State which is considered a paying agent under this paragraph shall communicate the name and address of the entity and the total amount of interest paid to, or secured for, the entity to the competent authority of its Member State of establishment, which shall pass this information on to the competent authority of the Member State where the entity is established.

3. The entity referred to in paragraph 2 shall, however, have the option of being treated for the purposes of this Directive as an UCITS as referred to in 2(c). The exercise of this option shall require a certificate to be issued by the Member State in which the entity is established and presented to the economic operator by that entity.

Member States shall lay down the detailed rules for this option for entities established in their territory.

4. Where the economic operator and the entity referred to in paragraph 2 are established in the same Member State, that Member State shall take the necessary measures to ensure that the entity complies with the provisions of this Directive when it acts as a paying agent.

5. The legal persons exempted from paragraph 2(a) are:

- (a) in Finland: avoin yhtiö (Ay) and kommandiittiyhtiö (Ky)/ öppet bolag and kommanditbolag;
- (b) in Sweden: handelsbolag (HB) and kommanditbolag (KB).

Article 5

Definition of competent authority

For the purposes of this Directive, 'competent authority' means:

- (a) for Member States, any of the authorities notified by the Member States to the Commission;

(b) for third countries, the competent authority for the purposes of bilateral or multilateral tax conventions or, failing that, such other authority as is competent to issue certificates of residence for tax purposes.

Article 6

Definition of interest payment

1. For the purposes of this Directive, 'interest payment' means:

- (a) interest paid or credited to an account, relating to debt claims of every kind, whether or not secured by mortgage and whether or not carrying a right to participate in the debtor's profits, and, in particular, income from government securities and income from bonds or debentures, including premiums and prizes attaching to such securities, bonds or debentures; penalty charges for late payments shall not be regarded as interest payments;
- (b) interest accrued or capitalised at the sale, refund or redemption of the debt claims referred to in (a);
- (c) income deriving from interest payments either directly or through an entity referred to in Article 4(2), distributed by:
 - (i) an UCITS authorised in accordance with Directive 85/611/EEC,
 - (ii) entities which qualify for the option under Article 4(3),
 - (iii) undertakings for collective investment established outside the territory referred to in Article 7;
- (d) income realised upon the sale, refund or redemption of shares or units in the following undertakings and entities, if they invest directly or indirectly, via other undertakings for collective investment or entities referred to below, more than 40 % of their assets in debt claims as referred to in (a):
 - (i) an UCITS authorised in accordance with Directive 85/611/EEC,
 - (ii) entities which qualify for the option under Article 4(3),
 - (iii) undertakings for collective investment established outside the territory referred to in Article 7.

However, Member States shall have the option of including income mentioned under (d) in the definition of interest only to the extent that such income corresponds to gains directly or indirectly deriving from interest payments within the meaning of (a) and (b).

2. As regards paragraph 1(c) and (d), when a paying agent has no information concerning the proportion of the income which derives from interest payments, the total amount of the income shall be considered an interest payment.

CHAPTER II

EXCHANGE OF INFORMATION

Article 8

Information reporting by the paying agent

1. Where the beneficial owner is resident in a Member State other than that in which the paying agent is established, the minimum amount of information to be reported by the paying agent to the competent authority of its Member State of establishment shall consist of:

- (a) the identity and residence of the beneficial owner established in accordance with Article 3;
- (b) the name and address of the paying agent;
- (c) the account number of the beneficial owner or, where there is none, identification of the debt claim giving rise to the interest;
- (d) information concerning the interest payment in accordance with paragraph 2.

2. The minimum amount of information concerning interest payment to be reported by the paying agent shall distinguish between the following categories of interest and indicate:

- (a) in the case of an interest payment within the meaning of Article 6(1)(a): the amount of interest paid or credited;
- (b) in the case of an interest payment within the meaning of Article 6(1)(b) or (d): either the amount of interest or income referred to in those paragraphs or the full amount of the proceeds from the sale, redemption or refund;
- (c) in the case of an interest payment within the meaning of Article 6(1)(c): either the amount of income referred to in that paragraph or the full amount of the distribution;
- (d) in the case of an interest payment within the meaning of Article 6(4): the amount of interest attributable to each of the members of the entity referred to in Article 4(2) who meet the conditions of Articles 1(1) and 2(1);
- (e) where a Member State exercises the option under Article 6(5): the amount of annualised interest.

However, Member States may restrict the minimum amount of information concerning interest payment to be reported by the paying agent to the total amount of interest or income and to the total amount of the proceeds from sale, redemption or refund.

3. As regards paragraph 1(d), when a paying agent has no information concerning the percentage of the assets invested in debt claims or in shares or units as defined in that paragraph, that percentage shall be considered to be above 40 %. Where he cannot determine the amount of income realised by the beneficial owner, the income shall be deemed to correspond to the proceeds of the sale, refund or redemption of the shares or units.

4. When interest, as defined in paragraph 1, is paid to or credited to an account held by an entity referred to in Article 4(2), such entity not having qualified for the option under Article 4(3), it shall be considered an interest payment by such entity.

5. As regards paragraph 1(b) and (d), Member States shall have the option of requiring paying agents in their territory to annualise the interest over a period of time which may not exceed one year, and treating such annualised interest as an interest payment even if no sale, redemption or refund occurs during that period.

6. By way of derogation from paragraphs 1(c) and (d), Member States shall have the option of excluding from the definition of interest payment any income referred to in those provisions from undertakings or entities established within their territory where the investment in debt claims referred to in paragraph 1(a) of such entities has not exceeded 15 % of their assets. Likewise, by way of derogation from paragraph 4, Member States shall have the option of excluding from the definition of interest payment in paragraph 1 interest paid or credited to an account of an entity referred to in Article 4(2) which has not qualified for the option under Article 4(3) and is established within their territory, where the investment of such an entity in debt claims referred to in paragraph 1(a) has not exceeded 15 % of its assets.

The exercise of such option by a Member State shall be binding on other Member States.

7. The percentage referred to in paragraph 1(d) and paragraph 3 shall from 1 January 2011 be 25 %.

8. The percentages referred to in paragraph 1(d) and in paragraph 6 shall be determined by reference to the investment policy as laid down in the fund rules or instruments of incorporation of the undertakings or entities concerned and, failing which, by reference to the actual composition of the assets of the undertakings or entities concerned.

Article 7

Territorial scope

This Directive shall apply to interest paid by a paying agent established within the territory to which the Treaty applies by virtue of Article 299 thereof.

Article 9

Automatic exchange of information

1. The competent authority of the Member State of the paying agent shall communicate the information referred to in Article 8 to the competent authority of the Member State of residence of the beneficial owner.

2. The communication of information shall be automatic and shall take place at least once a year, within six months following the end of the tax year of the Member State of the paying agent, for all interest payments made during that year.

3. The provisions of Directive 77/799/EEC shall apply to the exchange of information under this Directive, provided that the provisions of this Directive do not derogate therefrom. However, Article 8 of Directive 77/799/EEC shall not apply to the information to be provided pursuant to this chapter.

CHAPTER III

TRANSITIONAL PROVISIONS

Article 10

Transitional period

1. During a transitional period starting on the date referred to in Article 17(2) and (3) and subject to Article 13(1), Belgium, Luxembourg and Austria shall not be required to apply the provisions of Chapter II.

They shall, however, receive information from the other Member States in accordance with Chapter II.

During the transitional period, the aim of this Directive shall be to ensure minimum effective taxation of savings in the form of interest payments made in one Member State to beneficial owners who are individuals resident for tax purposes in another Member State.

2. The transitional period shall end at the end of the first full fiscal year following the later of the following dates:

— the date of entry into force of an agreement between the European Community, following a unanimous decision of the Council, and the last of the Swiss Confederation, the Principality of Liechtenstein, the Republic of San Marino, the Principality of Monaco and the Principality of Andorra, providing for the exchange of information upon request as defined in the OECD Model Agreement on Exchange of Information on Tax Matters released on 18 April 2002 (hereinafter the 'OECD Model Agreement') with respect to interest payments, as defined in this Directive, made by paying agents established within their respective territories to beneficial owners resident in the territory to which the Directive applies, in addition to the simultaneous application by those same countries of a withholding tax on such payments at the rate defined for the corresponding periods referred to in Article 11(1),

— the date on which the Council agrees by unanimity that the United States of America is committed to exchange of information upon request as defined in the OECD Model Agreement with respect to interest payments, as defined in this directive, made by paying agents established within its territory to beneficial owners resident in the territory to which the Directive applies.

3. At the end of the transitional period, Belgium, Luxembourg and Austria shall be required to apply the provisions of Chapter II and they shall cease to apply the withholding tax and the revenue sharing provided for in Articles 11 and 12. If, during the transitional period, Belgium, Luxembourg or Austria elects to apply the provisions of Chapter II, it shall no longer apply the withholding tax and the revenue sharing provided for in Articles 11 and 12.

Article 11

Withholding tax

1. During the transitional period referred to in Article 10, where the beneficial owner is resident in a Member State other than that in which the paying agent is established, Belgium, Luxembourg and Austria shall levy a withholding tax at a rate of 15 % during the first three years of the transitional period, 20 % for the subsequent three years and 35 % thereafter.

2. The paying agent shall levy withholding tax as follows:

- (a) in the case of an interest payment within the meaning of Article 6(1)(a): on the amount of interest paid or credited;
- (b) in the case of an interest payment within the meaning of Article 6(1)(b) or (d): on the amount of interest or income referred to in those paragraphs or by a levy of equivalent effect to be borne by the recipient on the full amount of the proceeds of the sale, redemption or refund;
- (c) in the case of an interest payment within the meaning of Article 6(1)(c): on the amount of income referred to in that paragraph;
- (d) in the case of an interest payment within the meaning of Article 6(4): on the amount of interest attributable to each of the members of the entity referred to in Article 4(2) who meet the conditions of Articles 1(1) and 2(1);
- (e) where a Member State exercises the option under Article 6(5): on the amount of annualised interest.

3. For the purposes of points (a) and (b) of paragraph 2, withholding tax shall be levied pro rata to the period of holding of the debt claim by the beneficial owner. When the paying agent is unable to determine the period of holding on the basis of information in its possession, it shall treat the beneficial owner as having held the debt claim throughout its period of existence unless he provides evidence of the date of acquisition.

4. The imposition of withholding tax by the Member State of the paying agent shall not preclude the Member State of residence for tax purposes of the beneficial owner from taxing the income in accordance with its national law, subject to compliance with the Treaty.

5. During the transitional period, Member States levying withholding tax may provide that an economic operator paying interest to, or securing interest for, an entity referred to in Article 4(2) established in another Member State shall be considered the paying agent in place of the entity and shall levy the withholding tax on that interest, unless the entity has formally agreed to its name, address and the total amount of interest paid to it or secured for it being communicated in accordance with the last subparagraph of Article 4(2).

Article 12

Revenue sharing

1. Member States levying withholding tax in accordance with Article 11(1) shall retain 25 % of their revenue and transfer 75 % of the revenue to the Member State of residence of the beneficial owner of the interest.

2. Member States levying withholding tax in accordance with Article 11(5) shall retain 25 % of the revenue and transfer 75 % to the other Member States proportionate to the transfers carried out pursuant to paragraph 1 of this Article.

3. Such transfers shall take place at the latest within a period of six months following the end of the tax year of the Member State of the paying agent in the case of paragraph 1, or that of the Member State of the economic operator in the case of paragraph 2.

4. Member States levying withholding tax shall take the necessary measures to ensure the proper functioning of the revenue-sharing system.

Article 13

Exceptions to the withholding tax procedure

1. Member States levying withholding tax in accordance with Article 11 shall provide for one or both of the following procedures in order to ensure that the beneficial owners may request that no tax be withheld:

- (a) a procedure which allows the beneficial owner expressly to authorise the paying agent to report information in accordance with Chapter II, such authorisation covering all interest paid to the beneficial owner by that paying agent; in such cases, the provisions of Article 9 shall apply;

- (b) a procedure which ensures that withholding tax shall not be levied where the beneficial owner presents to his paying agent a certificate drawn up in his name by the competent authority of his Member State of residence for tax purposes in accordance with paragraph 2.

2. At the request of the beneficial owner, the competent authority of his Member State of residence for tax purposes shall issue a certificate indicating:

- (a) the name, address and tax or other identification number or, failing such, the date and place of birth of the beneficial owner;
- (b) the name and address of the paying agent;
- (c) the account number of the beneficial owner or, where there is none, the identification of the security.

Such certificate shall be valid for a period not exceeding three years. It shall be issued to any beneficial owner who requests it, within two months following such request.

Article 14

Elimination of double taxation

1. The Member State of residence for tax purposes of the beneficial owner shall ensure the elimination of any double taxation which might result from the imposition of the withholding tax referred to in Article 11, in accordance with the provisions of paragraphs 2 and 3.

2. If interest received by a beneficial owner has been subject to withholding tax in the Member State of the paying agent, the Member State of residence for tax purposes of the beneficial owner shall grant him a tax credit equal to the amount of the tax withheld in accordance with its national law. Where this amount exceeds the amount of tax due in accordance with its national law, the Member State of residence for tax purposes shall repay the excess amount of tax withheld to the beneficial owner.

3. If, in addition to the withholding tax referred to in Article 11, interest received by a beneficial owner has been subject to any other type of withholding tax and the Member State of residence for tax purposes grants a tax credit for such withholding tax in accordance with its national law or double taxation conventions, such other withholding tax shall be credited before the procedure in paragraph 2 is applied.

4. The Member State of residence for tax purposes of the beneficial owner may replace the tax credit mechanism referred to in paragraphs 2 and 3 by a refund of the withholding tax referred to in Article 11.

Article 15

Negotiable debt securities

1. During the transitional period referred to in Article 10, but until 31 December 2010 at the latest, domestic and international bonds and other negotiable debt securities which have been first issued before 1 March 2001 or for which the original issuing prospectuses have been approved before that date by the competent authorities within the meaning of Council Directive 80/390/EEC (°) or by the responsible authorities in third countries shall not be considered as debt claims within the meaning of Article 6(1)(a), provided that no further issues of such negotiable debt securities are made on or after 1 March 2002. However, should the transitional period referred to in Article 10 continue beyond 31 December 2010, the provisions of this Article shall only continue to apply in respect of such negotiable debt securities:

- which contain gross-up and early redemption clauses and
- where the paying agent as defined in Article 4 is established in a Member State applying the withholding tax referred to in Article 11 and that paying agent pays interest to, or secures the payment of interest for the immediate benefit of, a beneficial owner resident in another Member State.

If a further issue is made on or after 1 March 2002 of an aforementioned negotiable debt security issued by a Government or a related entity acting as a public authority or whose role is recognised by an international treaty, as defined in the Annex, the entire issue of such security, consisting of the original issue and any further issue, shall be considered a debt claim within the meaning of Article 6(1)(a).

If a further issue is made on or after 1 March 2002 of an aforementioned negotiable debt security issued by any other issuer not covered by the second subparagraph, such further issue shall be considered a debt claim within the meaning of Article 6(1)(a).

2. Nothing in this Article shall prevent Member States from taxing the income from the negotiable debt securities referred to in paragraph 1 in accordance with their national laws.

CHAPTER IV

MISCELLANEOUS AND FINAL PROVISIONS

Article 16

Other withholding taxes

This Directive shall not preclude Member States from levying other types of withholding tax than that referred to in Article 11 in accordance with their national laws or double-taxation conventions.

(°) OJ L 100, 17.4.1980, p. 1. Directive repealed by Directive 2001/34/EC of the European Parliament and of the Council (OJ L 184, 6.7.2001, p. 1).

Article 17

Transposition

1. Before 1 January 2004 Member States shall adopt and publish the laws, regulations and administrative provisions necessary to comply with this Directive. They shall forthwith inform the Commission thereof.

2. Member States shall apply these provisions from 1 January 2005 provided that:

- (i) the Swiss Confederation, the Principality of Liechtenstein, the Republic of San Marino, the Principality of Monaco and the Principality of Andorra apply from that same date measures equivalent to those contained in this Directive, in accordance with agreements entered into by them with the European Community, following unanimous decisions of the Council;
- (ii) all agreements or other arrangements are in place, which provide that all the relevant dependent or associated territories (the Channel Islands, the Isle of Man and the dependent or associated territories in the Caribbean) apply from that same date automatic exchange of information in the same manner as is provided for in Chapter II of this Directive, (or, during the transitional period defined in Article 10, apply a withholding tax on the same terms as are contained in Articles 11 and 12).

3. The Council shall decide, by unanimity, at least six months before 1 January 2005, whether the condition set out in paragraph 2 will be met, having regard to the dates of entry into force of the relevant measures in the third countries and dependent or associated territories concerned. If the Council does not decide that the condition will be met, it shall, acting unanimously on a proposal by the Commission, adopt a new date for the purposes of paragraph 2.

4. When Member States adopt the provisions necessary to comply with this Directive, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.

5. Member States shall forthwith inform the Commission thereof and communicate to the Commission the main provisions of national law which they adopt in the field covered by this Directive and a correlation table between this Directive and the national provisions adopted.

Article 18

Review

The Commission shall report to the Council every three years on the operation of this Directive. On the basis of these reports, the Commission shall, where appropriate, propose to the Council any amendments to the Directive that prove necessary in order better to ensure effective taxation of savings income and to remove undesirable distortions of competition.

Article 19

Entry into force

This Directive shall enter into force on the 20th day following that of its publication in the *Official Journal of the European Union*.

Article 20

Addressees

This Directive is addressed to the Member States.

Done at Luxembourg, 3 June 2003.

For the Council
The President
N. CHRISTODOULAKIS

ANNEX

LIST OF RELATED ENTITIES REFERRED TO IN ARTICLE 15

For the purposes of Article 15, the following entities will be considered to be a 'related entity acting as a public authority or whose role is recognised by an international treaty':

— entities within the European Union:

Belgium	Vlaams Gewest (Flemish Region) Région wallonne (Walloon Region) Région bruxelloise/Brussels Gewest (Brussels Region) Communauté française (French Community) Vlaamse Gemeenschap (Flemish Community) Deutschsprachige Gemeinschaft (German-speaking Community)
Spain	Xunta de Galicia (Regional Executive of Galicia) Junta de Andalucía (Regional Executive of Andalusia) Junta de Extremadura (Regional Executive of Extremadura) Junta de Castilla-La Mancha (Regional Executive of Castilla-La Mancha) Junta de Castilla-León (Regional Executive of Castilla-León) Gobierno Foral de Navarra (Regional Government of Navarre) Goverm de les Illes Balears (Government of the Balearic Islands) Generalitat de Catalunya (Autonomous Government of Catalonia) Generalitat de Valencia (Autonomous Government of Valencia) Diputación General de Aragón (Regional Council of Aragón) Gobierno de las Islas Canarias (Government of the Canary Islands) Gobierno de Murcia (Government of Murcia) Gobierno de Madrid (Government of Madrid) Gobierno de la Comunidad Autónoma del País Vasco/Euzkadi (Government of the Autonomous Community of the Basque Country) Diputación Foral de Guipúzcoa (Regional Council of Guipúzcoa) Diputación Foral de Vizcaya/Bizkaia (Regional Council of Vizcaya) Diputación Foral de Alava (Regional Council of Alava) Ayuntamiento de Madrid (City Council of Madrid) Ayuntamiento de Barcelona (City Council of Barcelona) Cabildo Insular de Gran Canaria (Island Council of Gran Canaria) Cabildo Insular de Tenerife (Island Council of Tenerife) Instituto de Crédito Oficial (Public Credit Institution) Instituto Catalán de Finanzas (Finance Institution of Catalonia) Instituto Valenciano de Finanzas (Finance Institution of Valencia)
Greece	Οργανισμός Τηλεπικοινωνιών Ελλάδος (National Telecommunications Organisation) Οργανισμός Σιδηροδρόμων Ελλάδος (National Railways Organisation) Δημόσια Επιχείρηση Ηλεκτρισμού (Public Electricity Company)
France	La Caisse d'amortissement de la dette sociale (CADES) (Social Debt Redemption Fund) L'Agence française de développement (AFD) (French Development Agency) Réseau Ferré de France (RFF) (French Rail Network) Caisse Nationale des Autoroutes (CNA) (National Motorways Fund) Assistance publique Hôpitaux de Paris (APHP) (Paris Hospitals Public Assistance) Charbonnages de France (CDF) (French Coal Board) Entreprise minière et chimique (EMC) (Mining and Chemicals Company)
Italy	Regions Provinces Municipalities Cassa Depositi e Prestiti (Deposits and Loans Fund)
Portugal	Região Autónoma da Madeira (Autonomous Region of Madeira) Região Autónoma dos Açores (Autonomous Region of Azores) Municipalities

— international entities:

European Bank for Reconstruction and Development
European Investment Bank
Asian Development Bank
African Development Bank
World Bank/IBRD/IMF
International Finance Corporation
Inter-American Development Bank
Council of Europe Soc. Dev. Fund
Euratom
European Community
Corporación Andina de Fomento (CAF) (Andean Development Corporation)
Eurofima
European Coal & Steel Community
Nordic Investment Bank
Caribbean Development Bank

The provisions of Article 15 are without prejudice to any international obligations that Member States may have entered into with respect to the abovementioned international entities.

— entities in third countries:

Those entities that meet the following criteria:

1. the entity is clearly considered to be a public entity according to the national criteria;
2. such public entity is a non-market producer which administers and finances a group of activities, principally providing non-market goods and services, intended for the benefit of the community and which are effectively controlled by general government;
3. such public entity is a large and regular issuer of debt;
4. the State concerned is able to guarantee that such public entity will not exercise early redemption in the event of gross-up clauses.

ML

Schedule 1
Record keeping requirements

Money Laundering

**Schedule 1
Record keeping requirements**

The aim of the *guidance* in the following table is to give the reader a quick over-all view of the relevant record keeping requirements.

It is not a complete statement of those requirements and should not be relied on as if it were.

Reference	Requirement	Details	When	Retention period
ML 7.3.2 R (1)(a)	Customer identification	Full details of evidence of identity	As soon as reasonably practicable after first contact	5 years from end of relationship with client
ML 7.3.2 R (1)(b)	Transactions	Full details	On effecting the transaction	5 years from the date when the transaction was completed
ML 7.3.2 R (1)(d)	Internal and external reporting	Full details of actions taken	Once actions have been taken	5 years from the creation of the record
ML 7.3.2 R (1)(e)	Information not acted upon	Full details of information considered by the <i>MLRO</i> but not made an external report	Once decision not to report has been made	5 years from the obtaining of the information



Financial Action Task Force
Groupe d'action financière

TRADE BASED MONEY LAUNDERING

23 JUNE 2006

Table of Contents

Executive Summary

1. Introduction.....

2. The International Trade System

3. Abuse of the International Trade System

 Tax Avoidance and Evasion.....

 Capital Flight

 Trade-Based Money Laundering.....

4. Basic Trade-Based Money Laundering Techniques

 Over- and Under-Invoicing of Goods and Services

 Multiple Invoicing of Goods and Services.....

 Over- and Under-Shipments of Goods and Services

 Falsely Described Goods and Services.....

5. Complex Trade-Based Money Laundering Techniques.....

 Black Market Peso Exchange Arrangements

6. Case Studies

7. Current Practices.....

 Customs Agencies

 Law Enforcement Agencies.....

 Financial Intelligence Units.....

 Tax Authorities

 Banking Supervisors

 Red Flag Indicators

8. Key Findings.....

9. Issues for Consideration.....

Annex I.....

 Role of Financial Institutions in the Settlement of Trade Transactions

Annex II.....

 Customs Agencies (24 respondents)

 Law Enforcement Agencies (20 respondents).....

 Financial Intelligence Units (21 respondents).....

 Banking Supervisors (23 respondents)

Glossary.....

Bibliography.....

© 2006 FATF/OECD

All rights reserved. No reproduction or translation of this publication may be made without prior written permission. Applications for such permission should be made to: FATF Secretariat, 2 rue André-Pascal, 75775 Paris Cedex 16, France Fax: +33 1 44 30 61 37 or Contact@fatf-gafi.org

Typologies_TBML_200606.doc

Executive Summary

There are three main methods by which criminal organisations and terrorist financiers move money for the purpose of disguising its origins and integrating it into the formal economy. The first is through the use of the financial system; the second involves the physical movement of money (e.g. through the use of cash couriers); and the third is through the physical movement of goods through the trade system. In recent years, the Financial Action Task Force has focused considerable attention on the first two of these methods. By comparison, the scope for abuse of the international trade system has received relatively little attention.

The international trade system is clearly subject to a wide range of risks and vulnerabilities that can be exploited by criminal organisations and terrorist financiers. In part, these arise from the enormous volume of trade flows, which obscures individual transactions; the complexities associated with the use of multiple foreign exchange transactions and diverse trade financing arrangements; the commingling of legitimate and illicit funds; and the limited resources that most customs agencies have available to detect suspicious trade transactions.

For the purpose of this study, *trade-based money laundering* is defined as the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise their illicit origins. In practice, this can be achieved through the misrepresentation of the price, quantity or quality of imports or exports. Moreover, trade-based money laundering techniques vary in complexity and are frequently used in combination with other money laundering techniques to further obscure the money trail.

This study provides a number of case studies that illustrate how the international trade system has been exploited by criminal organisations. It also has made use of a detailed questionnaire to gather information on the current practices of more than thirty countries. This information focuses on the ability of various government agencies to identify suspicious activities related to trade transactions, to share this information with domestic and foreign partner agencies, and to act on this information.

The study concludes that trade-based money laundering represents an important channel of criminal activity and, given the growth of world trade, an increasingly important money laundering and terrorist financing vulnerability. Moreover, as the standards applied to other money laundering techniques become increasingly effective, the use of trade-based money laundering can be expected to become increasingly attractive.

Looking ahead there are a number of practical steps that can be taken to improve the capacity of national authorities to address the threat of trade-based money laundering. Among these are the need for a stronger focus on training programs to better identify trade-based money laundering techniques, the need for more effective information sharing among competent authorities at the national level, and greater recourse to memoranda of understanding and mutual assistance agreements to strengthen international cooperation.

Trade-Based Money Laundering

1. Introduction

In general, there are three main methods by which criminal organisations and terrorist financiers move money for the purpose of disguising its origins and integrating it back into the formal economy.

- The first involves the movement of value through the financial system using methods such as cheques and wire transfers;
- The second involves the physical movement of banknotes using methods such as cash couriers and bulk cash smuggling; and
- The third involves the movement of value using methods such as the false documentation and declaration of traded goods and services.

Each of these methods involves the movement of enormous volumes of funds and can operate at a domestic or international level. *The primary focus of this study is trade-based money laundering involving the international exchange of goods.*¹

Over the past few years, the Financial Action Task Force (FATF) has focussed considerable attention on the first two of these methods. In 2003, the FATF significantly toughened the standards that apply to the financial system and various non-financial intermediaries. Two years later, it extended these standards to cover the activities of cash couriers. To date, however, limited attention has been focussed on trade-related activities.

Not surprisingly, research has shown that when governments take action against certain methods of money laundering or terrorist financing, criminal activities tend to migrate to other methods. In part, this reflects the fact that more aggressive policy actions and enforcement measures increase the risk of detection and therefore raise the economic cost of using these methods.

This suggests that the FATF's recent actions to revise the 40 Recommendations on money laundering and extend the 8 Special Recommendations on terrorist financing to cover cash couriers, as well as the ongoing efforts of countries to implement these stricter standards, may have the unintended effect of increasing the attractiveness of the international trade system for money laundering and terrorist financing activities.²

This report is the product of research carried out by a project team operating under the umbrella of the FATF typologies initiative. The FATF project team was led by Canada with the participation of Aruba, Australia, Belgium, Brazil, China, India, Mexico, the Netherlands, the Netherlands Antilles, South Africa, South Korea, Spain, the United Kingdom, the United States, the Asia Development Bank, the Asia-Pacific Group on Money Laundering, the Eastern and Southern Africa Anti-Money Laundering Group, the Egmont Group (represented by the Ukraine), the Gulf Cooperation Council, the World Bank, and the World Customs Organisation.

¹ The specific risks associated with trade-based money laundering involving the international trade of services warrant further study.

² FATF Special Recommendation IX pertains to cash couriers.

Trade Based Money Laundering

Trade Based Money Laundering

2. The International Trade System

The international trade system is subject to a wide range of risks and vulnerabilities, which provide criminal organisations with the opportunity to launder the proceeds of crime and provide funding to terrorist organisations, with a relatively low risk of detection. The relative attractiveness of the international trade system is associated with:

- The enormous volume of trade flows, which obscures individual transactions and provides abundant opportunity for criminal organisations to transfer value across borders;
- The complexity associated with (often multiple) foreign exchange transactions and recourse to diverse financing arrangements;
- The additional complexity that can arise from the practice of commingling illicit funds with the cash flows of legitimate businesses;
- The limited recourse to verification procedures or programs to exchange customs data between countries; and
- The limited resources that most customs agencies have available to detect illegal trade transactions.

On this last point, research suggests that most customs agencies inspect less than 5 percent of all cargo shipments entering or leaving their jurisdictions. In addition, most custom agencies are able to direct relatively limited analytical resources to improved targeting and identification of suspicious trade transactions.

In recent decades, international trade has grown significantly: global merchandise trade now exceeds US\$9 trillion a year and global trade in services accounts for a further US\$2 trillion³. Much of this trade is associated with the financial system, as a significant amount of goods and services are financed by banks and other financial institutions.

In industrial countries the growth of trade has significantly exceeded the growth of gross domestic product, while in developing countries it has increased even faster. In addition, virtually all economies have become more open to trade. This has placed increasing pressure on the limited resources that most countries, especially developing countries, have available to scrutinise these activities.

3. Abuse of the International Trade System

Researchers have documented how the international trade system can be used to move money and goods with limited scrutiny by government authorities. In addition to money laundering, a considerable amount of academic attention has focused on the related activities of tax avoidance and evasion, and capital flight. A brief review of the recent literature in these areas is provided below.

Tax Avoidance and Evasion

A number of authors, including Li and Balachandran (1996), Fisman and Wei (2001), Swenson (2001) and Tomohara (2004), have described the impact that differing tax rates have on the incentives of corporations to shift taxable income from jurisdictions with relatively high tax rates to jurisdictions with relatively low tax rates in order to minimise income tax payments.

For example, this could arise in the context of a domestic parent company headquartered in a low-tax jurisdiction, which has a foreign affiliate operating in a high-tax jurisdiction. In such a situation, a common technique would be the over- or under-invoicing of imports and exports. For example, a foreign parent could use internal "transfer prices" to overstate the value of the goods and services that it provides to its foreign affiliate in order to shift

³ See *International Trade Statistics 2005*, World Trade Organisation.

taxable income from the operations of the affiliate in a high-tax jurisdiction to its operations in a low-tax jurisdiction.⁴

Similarly, the foreign affiliate might understate the value of the goods and services that it provides the domestic parent in order to shift taxable income from its high-tax jurisdiction to the low-tax jurisdiction of its parent. Both of these strategies would shift the company's profits to the low-tax jurisdiction and in doing so, reduce its worldwide tax payments. Imports can also be under-invoiced to reduce the payment of import duties and exports can be over-invoiced to obtain larger export subsidies. For example, studies by Vincent (2004) and Goetzl (2005) have documented the use of under-invoicing to reduce import duties in the case of forest products.

Capital Flight

A number of authors, including Cuddington (1986), Gulati (1987), Lessard and Williamson (1984), Kahn (1991), Anthony and Hallet (1992), Wood and Moll (1994), Fatehi (1994), Baker (2005) and de Boyrie, Pak and Zdanowicz (2005), have shown that companies and individuals also shift money from one country to another to diversify risk and protect their wealth against the impact of financial or political crises. Several of these studies also show that a common technique used to circumvent currency restrictions is to over-invoice imports or under-invoice exports.

For example, the International Monetary Fund (IMF) (1991), Kahn (1991), Wood and Moll (1994) and Fatehi (1994) examined the impact of controls imposed by South Africa in the 1970s and 1980s. They found that the primary method used to evade these controls was the falsification of import and export invoices. By comparing discrepancies between the value of exports reported by South Africa and the value of imports reported by key trading partners, the Kahn study concluded that at least \$20 billion had been transferred out of South Africa through the use of the international trade system. Other studies, including Smit and Mocke (1991) and Rustonjee (1991), suggested outflows ranging from \$12 billion to more than \$50 billion.

Trade-Based Money Laundering

Unlike tax avoidance and capital flight, which usually involve the transfer of legitimately earned funds across borders, capital movements relating to money laundering – or trade-based money laundering – involve the proceeds of crime, which are more difficult to track.

Trade-based money laundering has received considerably less attention in academic circles than the other means of transferring value. The literature has primarily focussed on alternative remittance systems and black market peso exchange transactions. However, a number of authors and institutions, including Baker (2005), de Boyrie, Pak and Zdanowicz (2005), the Department of Homeland Security, US Immigration and Customs Enforcement (2005), have recently examined a range of other methods used to launder money through the international trade system as well as the scope that jurisdictions have to identify and limit these activities.

A number of these studies have also analyzed techniques to establish whether reported import and export prices reflect fair market values. One of the methods currently being explored involves the use of statistical techniques to detect discrepancies in the information provided on shipping documents to better identify suspicious trading activity.

4. Basic Trade-Based Money Laundering Techniques

For the purpose of this study, *trade-based money laundering is defined as the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise their illicit origin*. In practice, this can be achieved through the misrepresentation of the price, quantity or quality of imports or exports.

⁴ In the case of transfer pricing, the reference to over- and under-invoicing relates to the legitimate allocation of income between related parties, rather than customs fraud.

Trade Based Money Laundering

Trade Based Money Laundering

In many cases, this can also involve abuse of the financial system through fraudulent transactions involving a range of money transmission instruments, such as wire transfers. The basic techniques of trade-based money laundering include:

- over- and under-invoicing of goods and services;
- multiple invoicing of goods and services;
- over- and under-shipments of goods and services; and
- falsely described goods and services.

All of these techniques are not necessarily in use in every country.

Over- and Under-Invoicing of Goods and Services

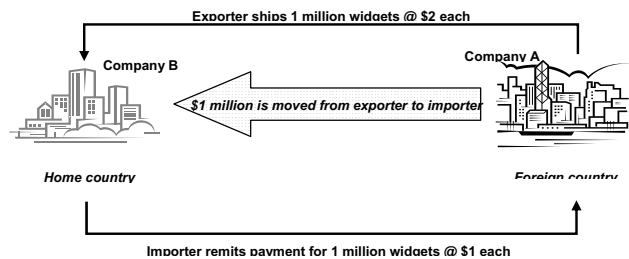
Money laundering through the over- and under-invoicing of goods and services, which is one of the oldest methods of fraudulently transferring value across borders, remains a common practice today. The key element of this technique is the misrepresentation of the price of the good or service in order to transfer additional value between the importer and exporter.

By invoicing the good or service at a price below the "fair market" price, the exporter is able to transfer value to the importer, as the payment for the good or service will be lower than the value that the importer receives when it is sold on the open market.

Alternatively, by invoicing the good or service at a price above the fair market price, the exporter is able to receive value from the importer, as the payment for the good or service is higher than the value that the importer will receive when it is sold on the open market.

Over- and Under-Invoicing of Goods – An Example

Company A (a foreign exporter) ships 1 million widgets worth \$2 each, but invoices Company B (a colluding domestic importer) for 1 million widgets at a price of only \$1 each. Company B pays Company A for the goods by sending a wire transfer for \$1 million. Company B then sells the widgets on the open market for \$2 million and deposits the extra \$1 million (the difference between the invoiced price and the "fair market" value) into a bank account to be disbursed according to Company A's instructions.



Alternatively, Company C (a domestic exporter) ships 1 million widgets worth \$2 each, but invoices Company D (a colluding foreign importer) for 1 million widgets at a price of \$3 each. Company D pays Company C for the goods by sending a wire transfer for \$3 million. Company C then pays \$2 million to its suppliers and deposits the remaining \$1 million (the difference between the invoiced price and the "fair market" price) into a bank account to be disbursed according to Company D's instructions.

Several points are worth noting. First, neither of the above transactions would be undertaken unless the exporter and importer had agreed to collude. For example, if Company A were to ship widgets worth \$2 each, but invoice them for \$1 each, it would lose \$1 million a shipment. Such a situation would not make sense unless the exporter and importer were colluding in a fraudulent transaction.

Second, there is no reason that Company A and Company B could not be controlled by the same organisation. In turn, there is nothing that precludes a parent company from setting up a foreign affiliate in a jurisdiction with less rigorous money laundering controls and selling widgets to the affiliate at a "fair market" price. In such a situation, the parent company could send its foreign affiliate a legitimate commercial invoice (e.g. an invoice of \$2 million for 1 million widgets) and the affiliate could then resell (and "re-invoice") these goods at a significantly higher or lower price to a final purchaser. In this way, the company could shift the location of its over- or under-invoicing to a foreign jurisdiction where such trading discrepancies might have less risk of being detected.

Third, the over- and under-invoicing of exports and imports can have significant tax implications. An exporter who over-invoices the value of the goods that he ships may be able to significantly increase the value of the export tax credit (or valued-added tax (VAT) rebate) that he receives. Similarly, an importer who is under-invoiced for the value of the goods that he receives may be able to significantly reduce the value of the import duties (or customs taxes) that he pays. Both of these cases illustrate the link between trade-based money laundering and abuse of the tax system.⁵

Research suggests that under-invoicing exports is one of the most common trade-based money laundering techniques used to move money. This reflects the fact that the primary focus of most customs agencies is to stop the importation of contraband and ensure that appropriate import duties are collected. Thus, customs agencies generally monitor exports less rigorously than imports.⁶

It is also worth noting that the more complex the good being traded, the greater the difficulty that customs agencies will have in identifying over- and under-invoicing and correctly assessing duties or taxes. In part, this is because many customs agencies do not have access to data and resources to establish the "fair market" price of many goods. In addition, most customs agencies do not share trade data with other countries and therefore see only one side of the transaction. As such, their ability to identify incorrectly priced goods is often limited to those that are widely traded (and whose prices are widely quoted) in international markets.⁷

Multiple Invoicing of Goods and Services

Another technique used to launder funds involves issuing more than one invoice for the same international trade transaction. By invoicing the same good or service more than once, a money launderer or terrorist financier is able to justify multiple payments for the same shipment of goods or delivery of services. Employing a number of different financial institutions to make these additional payments can further increase the level of complexity surrounding such transactions.

In addition, even if a case of multiple payments relating to the same shipment of goods or delivery of services is detected, there are a number of legitimate explanations for such situations including the amendment of payment terms, corrections to previous payment instructions or the payment of late fees. Unlike over- and under-invoicing, it should be noted that there is no need for the exporter or importer to misrepresent the price of the good or service on the commercial invoice.⁸

⁵ For the purposes of this paper, cases of over- or under-invoicing primarily designed to gain a tax advantage are considered customs fraud rather than trade-based money laundering.

⁶ For the same reasons, non-dutiable goods may also be subject to less rigorous scrutiny.

⁷ High-value goods, such as works of art, which have limited markets and highly "speculative" values present significant valuation difficulties.

⁸ If prices are correctly reported to customs agencies, detection of criminal activity is more difficult and may depend on intelligence-led operations.

Trade Based Money Laundering

Trade Based Money Laundering

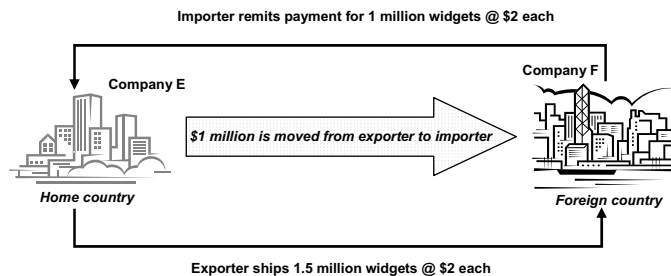
Over- and Under-Shipments of Goods and Services

In addition to manipulating export and import prices, a money launderer can overstate or understate the quantity of goods being shipped or services being provided. In the extreme, an exporter may not ship any goods at all, but simply collude with an importer to ensure that all shipping and customs documents associated with this so-called "phantom shipment" are routinely processed. Banks and other financial institutions may unknowingly be involved in the provision of trade financing for these phantom shipments.

Falsely Described Goods and Services

Over- and Under-Shipment of Goods – An Example

Company E (a domestic exporter) sells 1 million widgets to Company F (a colluding foreign importer) at a price of \$2 each, but ships 1.5 million widgets. Company F pays Company E for the goods by sending a wire transfer for \$2 million. Company F then sells the widgets on the open market for \$3 million and deposits the extra \$1 million (the difference between the invoiced quantity and the actual quantity) into a bank account to be disbursed according to Company E's instructions.

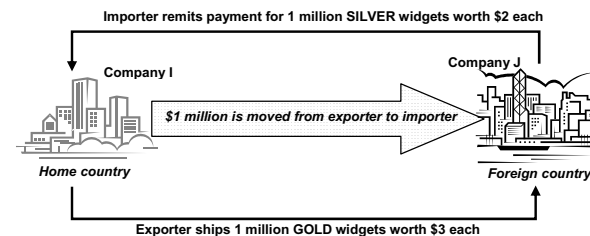


Alternatively, Company G (a foreign exporter) sells 1 million widgets to Company H (a colluding domestic importer) at a price of \$2 each, but only ships 500,000 widgets. Company H pays Company G for the goods by sending a wire transfer for \$2 million. Company G then pays \$1 million to its suppliers and deposits the remaining \$1 million (the difference between the invoiced quantity and the actual quantity) into a bank account to be disbursed according to Company H's instructions.

In addition to manipulating export and import prices, a money launderer can misrepresent the quality or type of a good or service. For example, an exporter may ship a relatively inexpensive good and falsely invoice it as a more expensive item or an entirely different item. This creates a discrepancy between what appears on the shipping and customs documents and what is actually shipped. The use of false descriptions can also be used in the trade in services, such as financial advice, consulting services and market research. In practice, the fair market value of these services can present additional valuation difficulties.

Falsely Described Goods – An Example

Company I (a domestic exporter) ships 1 million gold widgets worth \$3 each to Company J (a colluding foreign importer), but invoices Company J for 1 million silver widgets worth \$2 each. Company J pays Company I for the goods by sending a wire transfer for \$2 million. Company J then sells the gold widgets on the open market for \$3 million and deposits the extra \$1 million (the difference between the invoice value and the actual value) into a bank account to be disbursed according to Company I's instructions.



Alternatively, Company K (a foreign exporter) ships 1 million bronze widgets worth \$1 each to Company L (a colluding domestic importer), but invoices Company L for 1 million silver widgets worth \$2 each. Company L pays Company K for the goods by sending a wire transfer of \$2 million. Company K then pays \$1 million to its suppliers and deposits the remaining \$1 million (the difference between the invoiced value and the actual value) into a bank account to be disbursed according to Company L's instructions.

5. Complex Trade-Based Money Laundering Techniques

In practice, strategies to launder money usually combine several different techniques. Often these involve abuse of both the financial and international trade systems. Black market peso exchange arrangements provide a useful illustration of how a number of different money laundering techniques can be combined into a single criminal operation.

Black Market Peso Exchange Arrangements

The mechanics of black market peso exchange arrangements became the subject of considerable study in the 1980s when Colombia became the dominant exporter of cocaine into the United States. These illegal drug sales generated about \$10 billion a year for the Colombian drug cartels, of which as much as \$4 billion a year was laundered through black market peso arrangements. The mechanics of a simple black market peso arrangement can be set out in the following steps.

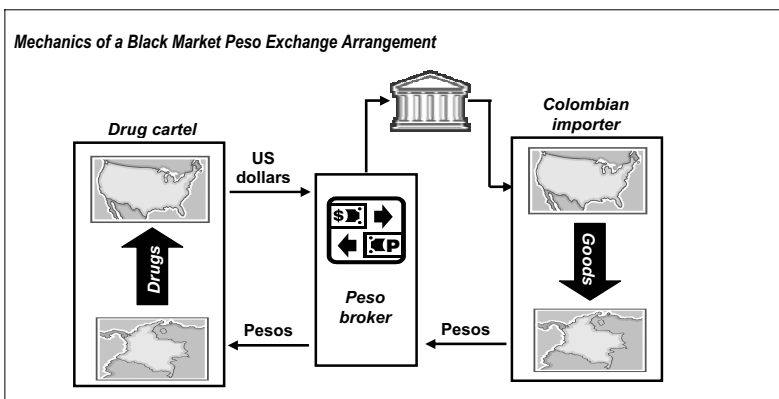
- First, the Colombian drug cartel smuggles illegal drugs into the United States and sells them for cash;
- Second, the drug cartel arranges to sell the US dollars at a discount to a peso broker for Colombian pesos;⁹
- Third, the peso broker pays the drug cartel with pesos from his bank account in Colombia (which eliminates the drug cartel from any further involvement in the arrangement);

⁹ The peso broker does need not to be located in the United States and, in fact, will usually operate out of Colombia. However, the peso broker will need to have a relationship with a correspondent in the United States to execute the transaction.

Trade Based Money Laundering

- Fourth, the peso broker structures or “smurfs” the US currency into the US banking system to avoid reporting requirements and consolidates this money in his US bank account;
- Fifth, the peso broker identifies a Colombian importer that needs US dollars to purchase goods from a US exporter¹⁰;
- Sixth, the peso broker arranges to pay the US exporter (on behalf of the Colombian importer) from his US bank account;
- Seventh, the US exporter ships the goods to Colombia¹¹; and
- Finally, the Colombian importer sells the goods (often high-value items such as personal computers, consumer electronics and household appliances) for pesos and repays the peso broker. This replenishes the peso broker’s supply of pesos.

These transactions combine a number of different illegal activities, such as drug smuggling, money laundering through the financial system and trade-based money laundering.¹² In addition, there is no reason why the drug cartel cannot act as its own peso broker or import business. In fact, many drug cartels appear to have internalised these functions.



Unlike the basic trade-based money laundering techniques discussed above, there is also no need for the importer and exporter to collude in a fraudulent transaction for the black market peso exchange arrangement to work. Instead, the prices and quantities of the goods can be correctly reported to customs agencies and value can still be transferred across borders.¹³ Although the term “black market peso exchange” refers to a money

¹⁰ The peso broker generally offers an exchange rate that is significantly better than that available through a Colombian bank.

¹¹ In practice, these goods would frequently be under-invoiced to reduce import duties or smuggled into the country to avoid import duties.

¹² Banks and other financial institutions provide a number of arrangements for the settlement of international trade transactions. (For more information, see Annex 1).

¹³ If prices and quantities are correctly reported to customs agencies, detection of the criminal activity is more difficult and may depend on intelligence-led operations. In practice, the goods associated with most black market peso exchange transactions are smuggled into the country to avoid duties and taxes.

Trade Based Money Laundering

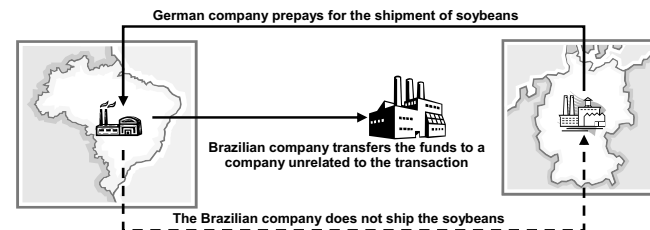
laundering technique that was originally associated with Colombian narcotics trafficking, these arrangements are widely used in many countries to repatriate the proceeds of various types of crimes.

6. Case Studies

This section provides a number of case studies that illustrate the various ways that trade-based money laundering techniques can be used separately or in combination with other money laundering techniques to obscure the origins of illegal funds and complicate efforts to trace this money.

Case Study 1

- A Brazilian company signs a contract to export soybeans to a German company.
- The German company prepays the Brazilian company for the shipment.
- The Brazilian company immediately transfers the funds to a third party that is unrelated to the transaction.
- The soybeans that were purchased by the German company are never shipped.

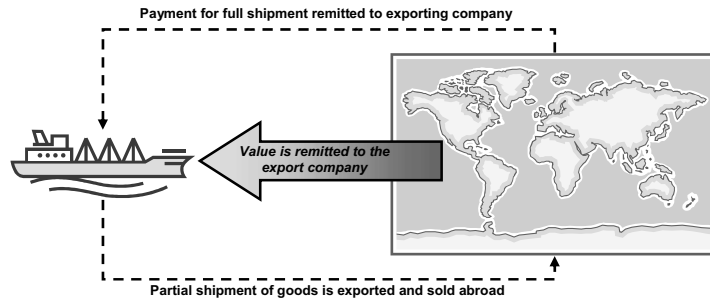


Source: Information provided by Brazil.

Commentary -- In this case, the German company transferred funds to the Brazilian company as an advance payment for a shipment of soybeans. Suspicions were raised when it was found that exports of soybeans were inconsistent with the Brazilian company’s regular business activities and the size of the reported shipment was inconsistent with the scale of the company’s operations.

Case Study 2

- A criminal organisation exports a relatively small shipment of scrap metal, but falsely reports the shipment as weighing several hundred tons.
- Commercial invoices, bills of lading and other shipping documents are prepared to support the fraudulent transaction.
- When the cargo is loaded on board the ship, a Canadian customs officer notices that the hull of the ship is still well above the water line. This is inconsistent with the reported weight of the shipment of scrap metal.
- The cargo is examined and the discrepancy between the reported and actual weight of the shipment is detected.
- It is assumed that the inflated value of the invoice would have been used to transfer criminal funds to Canada.

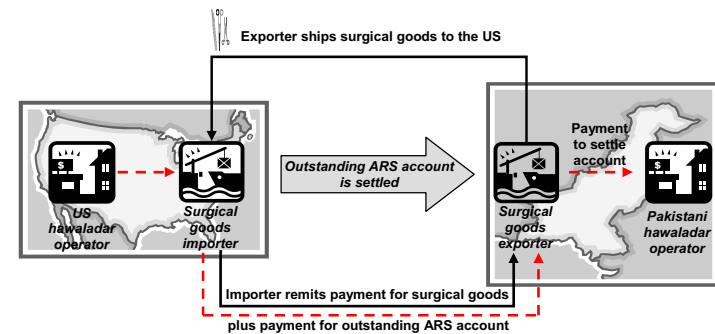


Source: Information provided by Canada.

Commentary -- In this case, the criminal organisation appears to have intended to over-invoice a colluding foreign importer by misrepresenting the quantity of goods. Using the international trade system, the criminal organisation would then have been able to transfer illegal funds back into the country using the trade transaction to justify payment through the financial system.

Case Study 3

- An alternative remittance system (ARS) operator (e.g. a "hawaladar") in the United States wants to transfer funds to his Pakistani counterpart to settle an outstanding account.
- The US operator colludes with a Pakistani exporter, who agrees to significantly over-invoice a US importer for the purchase of surgical goods.
- The US operator transfers funds to the US importer to cover the extra cost related to the over-invoicing.
- The Pakistani exporter uses the over-invoiced amount to settle the US operator's outstanding account with his Pakistani counterpart.
- The Pakistani exporter additionally benefits from a 20 percent VAT rebate on the higher prices of the exported goods.

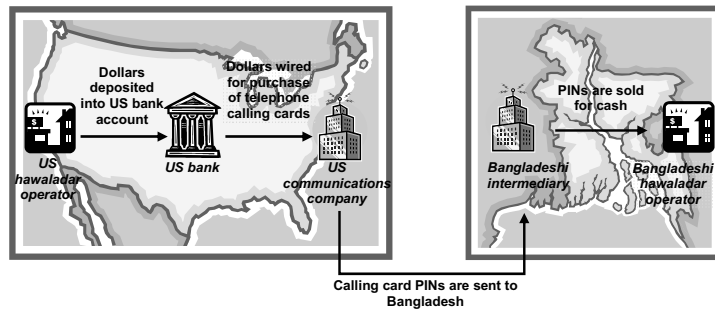


Source: Information provided by the United States.

Commentary -- In this case, rather than simply wiring the funds to his Pakistani counterpart, the US operator convinces a Pakistani exporter to over-invoice a colluding US importer. Using the international trade system, the US operator was then able to transfer the funds to settle his account using the trade transaction to justify payment through the financial system.

Case Study 4

- An alternative remittance system operator in the United States wants to transfer funds to his Bangladeshi counterpart to settle an outstanding account.
- The US operator deposits US dollars into his bank account and then wires the money to the corporate account of a large communications company to purchase telephone calling cards.
- The personal identification numbers (PINs) of these calling cards are sent to Bangladesh and sold for cash.
- The cash is given to the Bangladeshi counterpart to settle the US operator's outstanding account.

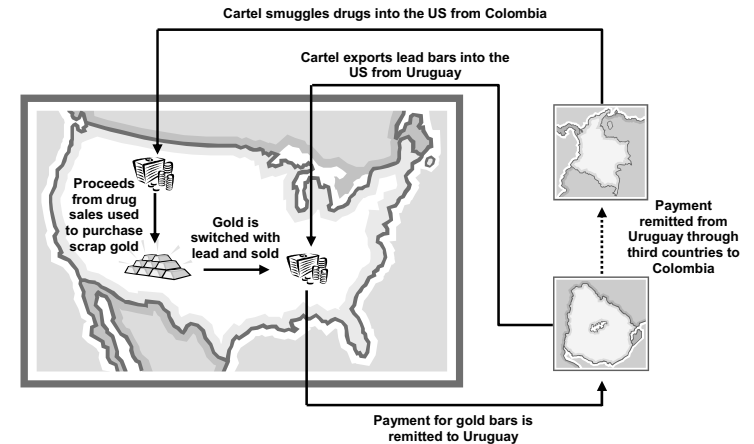


Source: FATF Money Laundering and Terrorist Financing Typologies for 2004-2005.

Commentary -- In this case, rather than simply wiring the funds to his Bangladeshi counterpart, the US operator chose to minimise the risk of detection through use of the international trade system. Interestingly, the operator's scheme does not depend on fraudulently reporting the price or quantity of the goods in order to transfer the funds required to settle the outstanding account. In addition, the calling cards are not actually exported. All that is required is the cross-border transfer of the PINs (i.e. the sale of an "intangible" good).

Case Study 5

- A Colombian cartel smuggles illegal drugs into the United States and sells them for cash.
- The cartel uses the cash to buy scrap gold in the United States, which is melted down and recast as gold bars.
- At the same time, the cartel ships lead bars from Uruguay to the United States, which are invoiced as bars of gold.
- When the shipment arrives, the lead bars are destroyed and the recast gold bars are substituted.
- With authentic documentation, the gold bars are sold on the open market. The money is wired back to Uruguay and then eventually to Panama.



Source: Jeffrey Robinson, *The Laundrymen* (1995). Used by permission of the author.

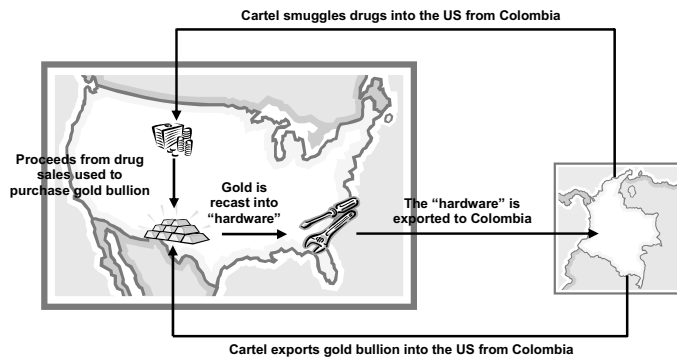
Commentary -- Unlike black market peso exchange arrangements, rather than smurfing the US currency into the US banking system, the cartel chose to minimise the risk of detection through the use of a falsely described shipment of goods. The shipping documents associated with these falsely described South American "gold bars" were used to legitimise the sale of the US gold bars. The receipts from these US gold sales were then deposited into the US banking system.

Trade Based Money Laundering

Trade Based Money Laundering

Case Study 6

- A Colombian cartel smuggles illegal drugs into the United States and sells them for cash.
- The cash is deposited into the US banking system and then used to purchase gold bullion that the cartel exports from Colombia.
- A group of cooperative jewellers in New York melts down the gold bullion and recasts them as low-value hardware items, such as nuts, bolts and household tools.
- The hardware items are enamelled and exported back to Colombia where they are melted down and recast as gold bullion again.
- The cartel re-exports the gold bullion to the United States where they are sold again and used to repatriate additional funds from drug sales to Colombia.

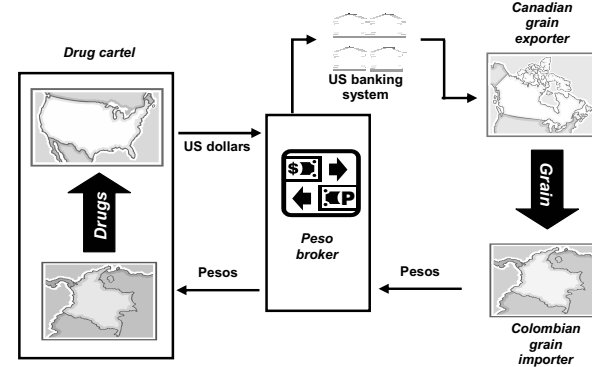


Source: Information provided by the United States.

Commentary -- Like black market peso exchange arrangements, the cartel smurfs the cash from drug sales into the US banking system and then uses this money to buy gold bullion that it has exported from Colombia. The gold is accurately reported to US Customs as "gold bullion", but falsely described to Colombian Customs as "manufactured gold products" in order to claim export credits. The shipping documents presented to US Customs are used to legitimise the sale of the Colombian gold bullion. By disguising the gold bullion as low-value exports to Colombia and then re-exporting the same gold bullion back to the United States, the cartel is able to repatriate the proceeds of the drug sales to Colombia by repeatedly invoicing the same gold bullion.

Case Study 7

- A Colombian drug cartel smuggles illegal drugs into the United States and sells them for cash.
- The drug cartel arranges to sell these US dollars at a discount to a peso broker for Colombian pesos.
- The broker "smurfs" the US dollars from the drug sales into the US banking system.
- The broker uses these funds to pay a Canadian company to ship grain to Colombia (on behalf of a Colombian grain importer). The payment is in the form of a letter of credit (covering 70% of the value of the contract) and third party cheques and electronic fund transfers (covering 30% of the value of the contract).
- The Colombian grain importer sells the grain in Colombia for pesos and repays the broker for financing the shipment.

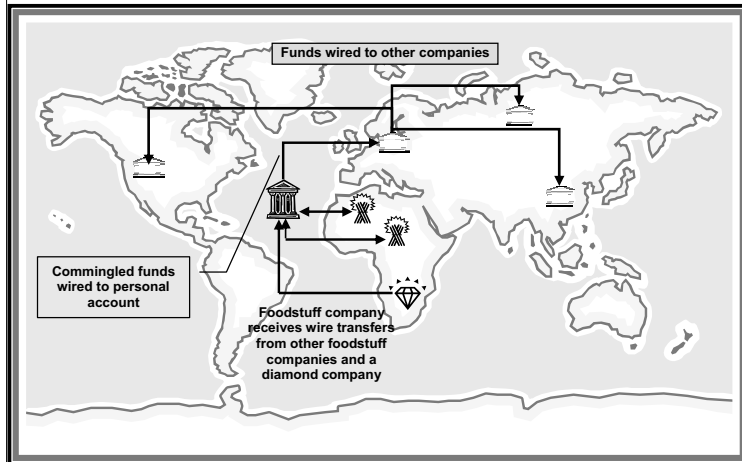


Source: Information provided by Canada.

Commentary -- This is a black market peso arrangement. Unlike the example that is used earlier in the paper, the peso broker smurfs the US dollars from the drug sales into the US banking system, but then uses these funds to purchase grain from a Canadian company for export to Colombia. In this case, the Colombian importer also made use of the two types of payments to try to defraud the Colombian Government of import duties by only declaring the 70 percent of the cost of the shipment covered by the letter of credit.

Case Study 8

- A food product trading company is established in an offshore financial centre and conducts business with several African food product companies.
- The money that the company receives for the sale of its products is immediately transferred from the company's offshore account to the personal account of its manager in Belgium. In turn, the funds are then quickly transferred to several foreign companies.
- The company also receives transfers from an unrelated company in the diamond business. The money from the diamond company is commingled with the company's other business receipts and transferred through Belgium to the same foreign companies.

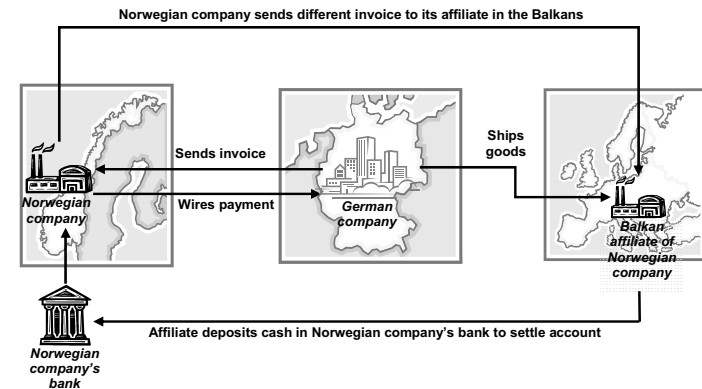


Source: Information provided by Belgium.

Commentary -- This case illustrates the level of additional complexity that can be added to the money trail by commingling illicit funds with the cash flows of legitimate businesses. In this case, the diamond company was subsequently the subject of an investigation into the trade in illegal "blood diamonds".

Case Study 9

- A Norwegian company purchases goods from a German company and directs that the goods be delivered to a branch of the Norwegian company in the Balkans.
- The German company sends the Norwegian company an invoice, which is settled by a wire transfer.
- The Norwegian company then sends the Balkan company a significantly higher invoice, which includes a range of inflated administrative costs.
- The Balkan company settles the invoice by paying cash into the Norwegian company's bank account.
- It is assumed that the Balkan company is transferring the proceeds of crime to the Norwegian company.



Source: Information provided by Norway.

Commentary -- In this case, the Norwegian company "re-invoices" the goods to significantly inflate their value. The Balkan company then deposits cash into the account of the Norwegian company. This "pay on account" transaction is done without any reference to the invoice for the shipped goods. This significantly complicates subsequent efforts to compare invoices and payments. The net effect is to transfer funds from the Balkan company to the Norwegian company with a relatively limited risk of detection.

Trade Based Money Laundering

Trade Based Money Laundering

Case Study 10

- A criminal group imports counterfeit goods from Asia into Belgium using a letter of credit and sells them for cash.
- The group deposits the money into a Belgian bank account and arranges a subsequent letter of credit.
- The group purchases additional counterfeit goods from Asia using the new letter of credit.
- These additional counterfeit goods are sold and the receipts deposited in the bank and used to arrange additional letters of credit.

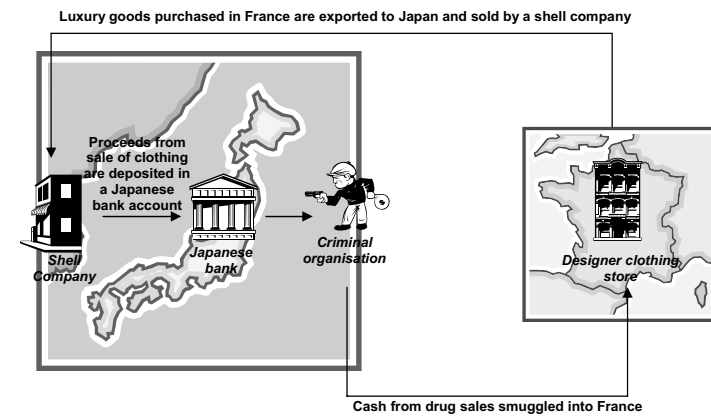


Source: Information provided by Belgium.

Commentary -- In this case, the criminal group was able to use the cash deposited in the bank to arrange letters of credit. Subsequently, it was able to make use of these letters of credit to purchase a series of shipments of counterfeit goods. The criminal group thought that the use of letters of credit related to trade transactions, rather than wire transfers, would increase the appearance of legitimacy of these transactions and reduce their risk of detection.

Case Study 11

- A criminal organisation sells illegal drugs in Japan. The organisation then smuggles the cash out of the country and into France.
- The money is used to purchase luxury goods in designer fashion stores, which are then exported to Japan and resold by a shell company.
- Proceeds from the sales of these luxury goods are deposited into the Japanese banking system.

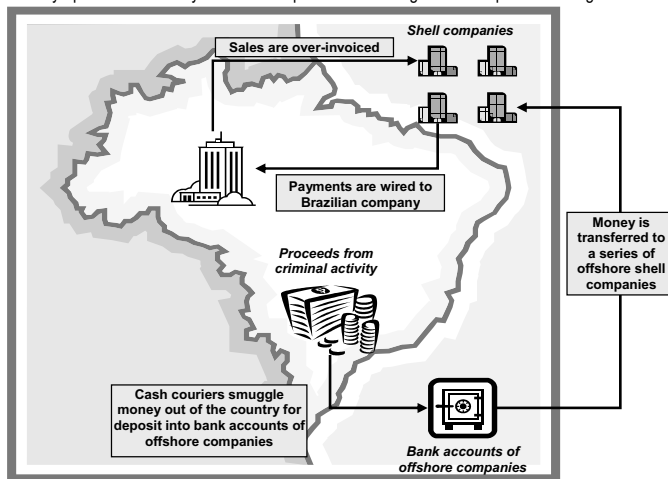


Source: Jeffrey Robinson, *The Laundrymen* (1995). Used by permission of the author.

Commentary -- Rather than smurfing, the Japanese currency into the Japanese banking system, the criminal organisation chose to minimise the risk of detection by smuggling the cash out of the country and then using the international trade system to import luxury goods back into Japan. The proceeds from the sale of these goods were then deposited into the Japanese banking system. Suspicions were raised when it was discovered that forged documents were used to export these goods and that the organisation had never applied for a value added tax rebate.

Case Study 12

- A Brazilian company is engaged in a range of illegal activities.
- The cash, which is generated from these activities, is smuggled out of the country by cash couriers and deposited in the bank accounts of offshore companies controlled by the company.
- Funds from these offshore accounts are transferred to offshore shell companies and used to purchase concentrated syrup for soft drinks from the Brazilian company at highly inflated prices.
- The syrup was then sold by the shell companies to other legitimate companies at a significant loss.



Source: Information provided by Brazil.

Commentary – In this case, the proceeds of crime were transferred to a Brazilian company through the sale of syrup at significantly inflated prices to a number of shell companies. The earnings from these sales were deposited into the company's Brazilian bank account and effectively reintegrated into the legitimate economy. Interestingly, unlike the shipment of scrap metal in Case Study 2, the weight and other physical characteristics of the shipment was unchanged, however, the process of dilution was used to reduce its value from US\$40 a litre to US\$1 a litre.

7. Current Practices

These case studies illustrate that the international trade system is subject to a wide range of vulnerabilities that can be exploited by criminal organisations and terrorist financiers. To examine the capacity of national authorities to combat trade-based money laundering, the FATF project team has made use of a detailed questionnaire to survey current practices in a range of countries.¹⁴ This questionnaire focuses on the ability of various

¹⁴ The 36 countries that responded to this questionnaire were Aruba, Australia, Austria, The Bahamas, Belgium, Brazil, Cambodia, Canada, Chinese Taipei, Fiji, France, Guatemala, Hong Kong, China, Indonesia, Italy, Japan, Kenya, Republic of

government agencies to identify suspicious activities related to trade transactions, to share this information with domestic and foreign partner agencies, and to act on this information. In carrying out this work, particular attention has been focused on the practices of customs agencies, law enforcement agencies, financial intelligence units, tax authorities and banking supervisors.

Customs Agencies

About half of customs agencies indicated that they make use of red flag indicators or other forms of risk analysis to detect potential trade-based money laundering activities. Moreover, almost three-quarters of those performing such analysis believe there is significant scope to make better use of trade data to identify anomalies that could be associated to money laundering or terrorist financing. In turn, this analysis triggered investigations in the case of more than half of respondents and prosecutions in about a quarter of respondents.

Similarly, almost all of respondents indicated that they were able to share trade-based information with law enforcement, financial intelligence units, tax authorities and foreign competent authorities. In the majority of cases, information sharing with law enforcement, financial intelligence units and tax authorities is voluntary. In the case of foreign competent authorities, the standard requirement for information sharing is a memorandum of understanding or customs mutual assistance agreement. Interestingly, less than half of respondents indicated that their customs agencies file suspicious activity reports with their financial intelligence units.

Only a third of respondents indicated that they had training programs in place, while virtually all agreed on the need for better training and understanding of the techniques of trade-based money laundering. In addition, more than half thought that there was scope to better use new technologies, such as X-ray scanners, electronic container seals and radio-frequency identification data. As a general proposition, two-thirds of respondents believed that their countries face serious vulnerabilities to trade-based money laundering activities.

Trade Transparency Units

Customs and law enforcement experience has shown that one of the most effective means of analyzing and investigating suspect trade-based activity is to have systems in place that monitor reported imports and exports between countries. Consistent with the FATF standards on international cooperation, a number of governments are now sharing import and export information in order to detect anomalies in their trade data.

To deal with the massive amounts of data generated by such exercises, new technologies have been developed that standardise this information against a range of variables to establish general patterns of trade activity. In turn, "trade transparency units" make use of this analysis to identify suspicious trading activities that often merit further investigation.

The sharing of trade data can be accomplished between cooperating customs authorities through customs mutual assistance agreements. The success of such arrangements underscores the importance of cooperating nations working together to establish bilateral mechanisms to detect trade anomalies, which may be associated with money laundering, terrorist financing or other financial crimes.

Experience shows that trade transparency units create effective gateways for the prompt exchange of trade data and information between foreign counterparts. As such, they represent a new and important investigative tool to better combat trade-based money laundering and customs fraud.

Korea, Macau, China, Malaysia, Mauritius, Mexico, Mongolia, Montserrat, Namibia, the Netherlands, the Netherlands Antilles, New Zealand, Norway, Peru, Qatar, South Africa, Spain, St. Lucia, Swaziland, United Kingdom and the United States. A detailed summary of the responses of each country has been provided to the FATF Secretariat to facilitate future analytical work in this area.

Trade Based Money Laundering

Trade Based Money Laundering

Law Enforcement Agencies

Interestingly, two-thirds of law enforcement agencies indicated they use trade information as part of their analysis of money laundering and terrorist financing activities. While the bulk of this information is received from financial intelligence units, customs agencies and financial institutions, significant information is also made available by banking supervisors and tax authorities. Almost all of the respondents that made use of this information indicated that it had triggered investigations and two-thirds of these investigations resulted in prosecutions.

While only a third of respondents have access to trade databases, those that do agree that there is significant scope for greater cooperation between customs and law enforcement agencies in this area. Half of the respondents make use of red flag indicators and similarly believe that there is scope for more extensive use of such techniques.

Law enforcement agencies appear to have few problems sharing information with customs agencies, financial intelligence units and tax authorities, although this is largely done on a voluntary basis and under certain conditions, such as to further an ongoing criminal investigation. Most respondents indicated that information sharing with banking supervisors is significantly more complicated (and frequently prohibited) and that information sharing with foreign competent authorities generally requires that a memorandum of understanding or mutual legal assistance treaty is in place. Nevertheless, several respondents indicated that they are generally able to share information on the basis of international reciprocity.

A third of respondents appear to have some level of expertise in the area of trade and a similar number indicated that they have training programs in place. Virtually all respondents agreed on the need for better training and awareness of the techniques of trade-based money laundering. In general, two-thirds of respondents viewed trade-based money laundering activities as presenting a serious risk to their country.

Financial Intelligence Units

Half of financial intelligence units receive suspicious activities reports triggered by concerns about trade-related activities. However, in most countries, the number of such reports is relatively low (e.g. often less than 25 a year). In addition to financial institutions, these reports are received from customs and law enforcement agencies and, to a lesser extent, tax authorities and banking supervisors. About a third of financial intelligence units use trade information as part of their ongoing analysis of money laundering and terrorist financing activities and this information frequently contributes to investigations and prosecutions.

Financial intelligence units indicated that they make extensive use of red flag indicators. In addition, the majority of respondents believe that there is considerable scope to make better use of such indicators and other analytical techniques to promote a more risk-based approach to detecting trade-based money laundering activities. This being the case, it is interesting that only a quarter of financial intelligence units reported that they make use of trade databanks as part of their analysis.

Not surprisingly, financial intelligence units are able to share information with law enforcement agencies, customs agencies, tax authorities and banking supervisors. However, some respondents cautioned that strict commercial confidentiality continues to apply to this information, which limits its use to intelligence purposes. Others indicated that the sharing of trade information is often limited to cases of ongoing criminal investigation. Respondents confirmed that domestic financial intelligence units are able to share information with foreign financial intelligence units, but this generally requires a memorandum of understanding or international reciprocity.

About half of the respondents have trade specialists on their staff, but only a quarter provide training to improve their analysts' understanding of trade-based money laundering techniques. Respondents were virtually unanimous that financial intelligence units would benefit from better training and awareness of the techniques of trade-based money laundering activities. In general, two-thirds of respondents believe that their countries are seriously vulnerable to abuse of the trade system for criminal purposes.

Tax Authorities

Two-thirds of tax authorities indicate that they receive information from customs and law enforcement agencies and financial intelligence units, which directly relates to trade-based money laundering. However, these respondents appear to make limited use of this information in pursuing investigations or prosecutions. This said, a third of tax authorities indicated that they perform analysis that is useful in identifying trade-based money laundering and routinely file suspicious activity reports with their financial intelligence units.

While half of tax authorities have the power to conduct investigations, only a third have a mandate that permits them to examine trade-based money laundering activities. Moreover, if a suspicion of money laundering arises in the course of an audit, only half of the respondents indicated that they are required to report it to competent authorities. Most tax authorities are able to voluntarily share information with customs agencies, law enforcement agencies and financing intelligence units under certain conditions, such as to further an ongoing investigation. Most respondents indicated that sharing information with banking supervisors is significantly more complicated (and frequently prohibited), but that trade-related information from tax audits can be shared with their foreign counterparts if appropriate memoranda of understanding or mutual legal assistance treaties are in place.

Few tax authorities have trade specialists on their staffs or training programs to improve the understanding of trade-based money laundering. Nevertheless, tax authorities unanimously agreed on the need for better training and awareness of trade-based money laundering techniques. In general, two-thirds of respondents considered their countries to be vulnerable to the use of trade transactions for criminal purposes.

Banking Supervisors

In most countries, banking supervisors have limited involvement in trade-based money laundering activities. However, a third of respondents indicated that they frequently receive information related to suspicious trade-based activities from their financial institutions. Moreover, a third of respondents indicated that they undertake analysis that can be used to identify trade-based money laundering and routinely report suspicious activities to their financial intelligence units. Just under half of respondents use red flag indicators and other analytical techniques to identify high-risk commodities, companies or countries and most see significant scope to make better use of such techniques. A third of respondents have used this information to trigger investigations, but in only 10 percent of these cases has it led to prosecutions.

Banking supervisors appear to have considerable scope to voluntarily share trade-related information with customs agencies, law enforcement agencies, financial intelligence units and tax authorities. In addition, the majority of banking supervisors indicated that they could share trade information with foreign competent authorities with certain restrictions. Not surprisingly, few banking authorities have expertise on the techniques of trade-based money laundering and most have little or no training programs in this area. In general, about half of respondents considered their countries to be vulnerable to the use of trade transactions for criminal purposes.

Trade Based Money Laundering

Trade Based Money Laundering

Red Flag Indicators***Trade-Based Money Laundering "Red Flag" Indicators***

The respondents to the FATF project team's questionnaire reported a number of red flag indicators that are routinely used to identify trade-based money laundering activities. These include situations in which:

- Significant discrepancies appear between the description of the commodity on the bill of lading and the invoice;
- Significant discrepancies appear between the description of the goods on the bill of lading (or invoice) and the actual goods shipped;
- Significant discrepancies appear between the value of the commodity reported on the invoice and the commodity's fair market value;
- The size of the shipment appears inconsistent with the scale of the exporter or importer's regular business activities;
- The type of commodity being shipped is designated as "high risk" for money laundering activities; *
- The type of commodity being shipped appears inconsistent with the exporter or importer's regular business activities;
- The shipment does not make economic sense; **
- The commodity is shipped to (or from) a jurisdiction designated as "high risk" for money laundering activities;
- The commodity is transhipped through one or more jurisdictions for no apparent economic reason;
- The method of payment appears inconsistent with the risk characteristics of the transaction; ***
- The transaction involves the receipt of cash (or other payments) from third party entities that have no apparent connection with the transaction;
- The transaction involves the use of repeatedly amended or frequently extended letters of credit; and
- The transaction involves the use of front (or shell) companies.

Customs agencies make use of more targeted information that relates to specific exporting, importing or shipping companies. In addition, red flag indicators that are used to detect other methods of money laundering could be useful in identifying potential trade-based money laundering cases.

* For example, high-value, low-volume goods (e.g. consumer electronics), which have high turnover rates and present valuation difficulties.

** For example, the use of a forty-foot container to transport a small amount of relatively low-value goods.

** For example, the use of an advance payment for a shipment from a new supplier in a high-risk country.

8. Key Findings

The research work carried out for this project has led to the following key findings with respect to trade-based money laundering:

- Trade-based money laundering is an important channel of criminal activity and, given the growth in world trade, it represents an increasingly important money laundering and terrorist financing vulnerability.
- Trade-based money laundering practices vary in complexity. The most basic schemes are fraudulent trade practices (e.g. under- or over-invoicing of receipts). However, more complicated schemes integrate these fraudulent practices into a web of complex transactions, which also involve the movement of value through the financial system (e.g. cheques or wire transfers) and/or the physical movement of banknotes (e.g. cash couriers). The use of these complex transactions further obscures the money trail and complicates detection.
- Trade data analysis and the international sharing of trade data are useful tools for identifying trade anomalies, which may lead to the investigation and prosecution of trade-based money laundering cases.
- While customs agencies, law enforcement agencies, financial intelligence units, tax authorities and banking supervisors can exchange trade-related information, this is frequently restricted to certain circumstances or undertaken on a voluntary rather than mandatory basis. In addition, most financial intelligence units do not consistently receive suspicious activity reports related to trade transactions.
- Most customs agencies, law enforcement agencies, financial intelligence units, tax authorities and banking supervisors appear less capable of identifying and combating trade-based money laundering than they are in dealing with other forms of money laundering and terrorist financing. In part, this appears to reflect their more limited understanding of the techniques of this form of money laundering.
- Most customs agencies, law enforcement agencies, financial intelligence units, tax authorities and banking supervisors identified a pressing need for more training to ensure that their staff has sufficient knowledge to recognise trade-based money laundering.
- Most customs agencies, law enforcement agencies, financial intelligence units, tax authorities and banking supervisors indicated serious concerns about the vulnerabilities of their countries to trade-based money laundering. In addition, most believe that their countries have only limited measures in place to mitigate trade-based money laundering activities.

Trade Based Money Laundering

Trade Based Money Laundering

9. Issues for Consideration

Trade-based money laundering is an important money laundering technique that has received limited attention from policymakers. As international trade continues to grow and the standards applied to other money laundering techniques have become increasingly effective, the use of trade-based money laundering channels can be expected to become increasingly attractive.

This study suggests that the level of understanding of trade-based money laundering appears broadly similar to that relating to the movement of value through the financial system a decade ago. At that time, "front line" workers in most financial institutions were largely unaware as to what constituted suspicious activity as well as what actions they should take if such activities were detected.

This study suggests that customs agencies, law enforcement agencies, financial intelligence units, tax authorities and banking supervisors currently face similar challenges with respect to understanding the techniques of trade-based money laundering and detecting such activities.

Looking ahead, there appears to be a number of practical steps that could initially be taken to improve the capacity of national authorities to cope with trade-based money laundering. These can be summarised as building better awareness, strengthening measures to identify trade-based illicit activity and improving international co-operation.

Building Better Awareness

The review of current practices of those countries responding to the FATF questionnaire showed that there was almost unanimous agreement on the need for a stronger focus on training programs for competent authorities (e.g. customs agencies, law enforcement agencies, financial intelligence units, tax authorities and banking supervisors) to better identify trade-based money laundering techniques. In turn, improved training could result in substantial increases in the number of suspicious transaction reports filed with financial intelligence units. In addition, such training programs could be usefully supplemented by outreach sessions to the private sector.

Strengthening Current Measures

There are a number of actions that countries could take to better identify trade-based illicit activity. The simplest is to ensure that competent authorities and financial institutions have access to the case studies and red flag indicators in this study. In addition, most countries would benefit from more effective information sharing among competent authorities at the domestic level. For example, it would be useful if law enforcement agencies could seek information from customs agencies on specific trade transactions in advance of a full-fledged criminal investigation.

Improving International Co-operation

Countries need to work cooperatively to identify and combat trade-based money laundering. Consistent with FATF standards, countries could put clear and effective gateways in place to facilitate the prompt and constructive exchange of information. In practice, this may require broader use of memoranda of understanding and mutual legal assistance treaties between countries to facilitate the sharing of information related to specific transactions. It also means greater recourse to mutual assistance agreements between customs agencies to facilitate the exchange of export and import data in order to identify trade anomalies that may indicate potential trade-based money laundering abuses.

Annex I

Role of Financial Institutions in the Settlement of Trade Transactions

Financial institutions can play three roles in the settlement of international trade transactions, namely, money transmission, provision of finance, and lending the institution's name to the transaction. Below is a simple description of these roles.

Money transmission – is the transfer of funds between parties associated with the trade transaction. (e.g. a wire transfer).

Provision of finance – is the provision of credit to support the trade transaction. In these situations, as a standard practice, the financial institution conducts standard credit checks against the customer. In addition, the financial institution may conduct a check against the underlying transaction.

Lending the financial institution's name to the transaction – occurs in two situations: (1) where the financial institution undertakes to make payment subject to certain conditions (e.g. a letter of credit), and (2) where the financial institution undertakes to make payment if the buyer defaults (e.g. a guarantee).

In addition to monitoring in accordance with domestic anti-money laundering and counter-terrorist financing regulations, the levels of scrutiny and information available on the underlying transaction will depend upon the bank's exposure to credit and reputational risk associated with the provision of finance and lending of the bank's name to the transaction. For example, because an institution's risk exposure when conducting a money transmission is low, it is unlikely that the institution will closely scrutinise or even see the documents supporting the transaction (e.g. bills of lading or invoices).

Trade Based Money Laundering

Trade Based Money Laundering

Annex II

This annex contains a sample of the key information that was provided in the responses to the FATF Project Team's questionnaire. In some cases, the respondents did not answer all questions.

Customs Agencies (24 respondents)

	Yes	No
Do you perform analysis that could be used to identify, investigate, or prosecute trade-based money laundering?	12	12
Do you undertake analysis of trade data to identify trade anomalies that could be related to money laundering or terrorist financing?	13	11
Can you provide a list of "red-flag" indicators of potential trade-based money laundering that could trigger suspicions or a possible investigation?	12	12
Do you make use of any risk models or analytical tools to identify high-risk companies, commodities, countries or activities?	19	5
Is there scope to make better use of trade data analysis to identify trade anomalies that could justify further investigation	18	5

Has information or analysis led to specific investigations and subsequent prosecutions?	
Investigations	14
Prosecutions	6
No	10

Is information sharing between customs agencies and other domestic agencies mandatory or voluntary?				
	Law Enforcement	Financial Intelligence Unit	Tax Authority	Banking Supervision
Mandatory	10	9	6	1
Voluntary	13	11	14	10
Not applicable	1	0	0	8

With which of the following domestic agencies can trade-related information be shared?				
	Law Enforcement	Financial Intelligence Unit	Tax Authority	Banking Supervision
Yes	10	6	10	2
Yes, with restrictions	13	15	10	11
No	1	0	0	7

Can trade-related information be shared with foreign competent authorities?	
Yes	7
Yes, with restrictions	16
No	0

	Yes	No
Do you have training programs in place that deal with the subject of trade-based money laundering?	8	15
Do you see the need for better training and awareness of the techniques of trade-based money laundering?	22	1
Do you consider your country to be vulnerable to the use of trade-based money laundering for criminal purposes?	17	7

Law Enforcement Agencies (20 respondents)

From which sources does your organisation receive information related to trade-based money laundering?	
Customs Agencies	11
Financial Intelligence Units	13
Tax Authorities	7
Banking Supervisors	5
Financial Institutions	10
Others	9

Has this information led to investigations and subsequent prosecutions?	
Investigations	18
Prosecutions	13
No	2

	Yes	No
Has trade information been used as part of your analysis or investigations of money laundering or terrorist financing?	15	5
Do you have access to a trade information database that you can use to advance analysis or investigations of money laundering or terrorist financing?	7	13
Is there scope to improve cooperation between law enforcement and customs agencies through the use of searchable databases relating to individual companies or transactions?	15	5
Can you provide a list of ("red flag") risk indicators of potential trade-based money laundering activity that could trigger suspicions or a possible investigation?	7	12
Is there scope to make better use of risk indicators to promote a more risk-based approach to detecting trade-based money laundering activity?	8	10

Is information sharing between law enforcement and other domestic agencies mandatory or voluntary?				
	Customs Agencies	FIU	Tax Authority	Banking Supervisor
Mandatory	6	5	5	2
Voluntary	11	9	11	8
Not applicable	1	1	0	8

Trade Based Money Laundering

Trade Based Money Laundering

With which of the following domestic agencies can trade-related information be shared?				
	<i>Customs Agencies</i>	<i>FIU</i>	<i>Tax Authority</i>	<i>Banking Supervisor</i>
Yes	6	6	3	0
Yes, with restrictions	12	8	14	8
No	0	0	0	6

Can trade-related information be shared with foreign competent authorities?	
Yes	3
Yes, with restrictions	13
No	1

	Yes	No
Do you have training programs in place that deal with the subject of trade-based money laundering?	6	13
Do you see the need for better training and awareness of the techniques of trade-based money laundering?	17	2
Do you consider your country to be vulnerable to the use of trade transactions for criminal purposes?	13	6

Financial Intelligence Units (21 respondents)

Have you received Suspicious Activity Reports (SARs) that were triggered by suspicious trade transactions?	
Yes	12
No	2
Not applicable	5

Have you received SARs that were triggered by suspicious trade transactions?		
	<i>In the past year?</i>	<i>In the past three years?</i>
0	1	1
1 - 5	0	4
6 - 25	6	4
More than 25	8	5
Not applicable	5	5

From which sources does your organisation receive information related to trade-based money laundering?	
<i>Customs Agencies</i>	11
<i>Law Enforcement Agencies</i>	12
<i>Tax Authorities</i>	8
<i>Banking Supervisors</i>	3
<i>Financial Institutions</i>	17
<i>Others</i>	3
Not applicable	2

	Yes	No
Has trade information been used as part of your analysis or investigations of money laundering or terrorist financing?	11	10
Is trade information routinely used in your analysis or investigations?	8	13

Has this information led to investigations and subsequent prosecutions?	
Investigations	14
Prosecutions	10
No	5

	Yes	No
In situations where trade-based money laundering is suspected, do transactions involve trade finance products such as letters of credit or documentary collections?	11	8
Does your organisation collect SWIFT transactional data that is used in your analysis or investigations of money laundering or terrorist financing?	8	13
Can you provide a list of ("red flag") risk indicators of potential trade-based money laundering activity that could trigger suspicions or a possible investigation?	14	7
Is there scope to make better use of risk indicators to promote a more risk-based approach to detecting trade-based money laundering activity?	10	6
Do you have access to a trade information database that you can use to advance analysis or investigations of money laundering or terrorist financing?	6	15

With which of the following domestic agencies can trade-related information be shared?				
	<i>Customs Agencies</i>	<i>Law Enforcement</i>	<i>Tax Authority</i>	<i>Banking Supervisor</i>
Yes	10	11	9	9
Yes, with restrictions	8	7	7	3
No	0	1	1	2

Can trade-related information be shared with foreign competent authorities?	
Yes	7
Yes, with restrictions	14
No	0

	Yes	No
Does your agency have specialists with particular expertise in the area of trade?	12	9
Do you have training programs in place that deal with the subject of trade-based money laundering?	4	16
Do you see the need for better training and awareness of the techniques of trade-based money laundering?	18	2
Do you consider your country vulnerable to the use of trade transactions for criminal purposes?	15	4

Trade Based Money Laundering

Trade Based Money Laundering

Tax Authorities (21 respondents)

Do you receive information on suspicious activities related to trade-based money laundering?	
Yes	10
No	11

Do you have access to a trade information database that you can use to advance analysis or investigations of money laundering or terrorist financing?	
Yes	5
No	8
Not applicable	8

	Yes	No
Do you perform analysis that could be used to identify, investigate, or prosecute trade-based money laundering?	7	13
Do you file suspicious activity reports (SARs) with your financial intelligence unit relating to suspicious trade transactions?	7	14
Can you provide a list of "red-flag" indicators of potential trade-based money laundering that could trigger suspicions or a possible investigation?	9	12
Is there scope to make better use of risk indicators to promote a more risk-based approach to detecting trade-based money laundering activity?	5	10
Do you conduct your own investigations or are you involved with other agencies in investigations into potential trade-based money laundering activity?	10	10
Do you have a mandate to look for money laundering activities in the course of conducting an audit?	7	14
If a suspicion of money laundering arises in the course of an audit, are you required to report it to a competent authority?	12	9

Can a competent authority request tax information as part of an investigation on trade-based money laundering?	
Yes, in all cases	6
Yes, with restrictions	14
No	1

Is information sharing between tax authorities and other domestic agencies mandatory or voluntary?				
	Customs Agencies	Law Enforcement	FIU	Banking Supervisor
Mandatory	7	6	10	2
Voluntary	10	9	4	5
Not applicable	1	3	4	11

With which of the following domestic agencies can trade-related information be shared?				
	Customs Agencies	Law Enforcement	FIU	Banking Supervisor
Yes	9	4	8	2
Yes, with restrictions	8	11	6	4
No	2	3	5	10

Can trade-related information be shared with foreign competent authorities?	
Yes	2
Yes, with restrictions	12
No	5

	Yes	No
Does your agency have specialists with particular expertise in the area of trade?	4	15
Do you have training programs in place that deal with the subject of trade-based money laundering?	5	15
Do you see the need for better training and awareness of the techniques of trade-based money laundering?	20	1
Do you consider your country to be vulnerable to the use of trade-based money laundering for criminal purposes?	15	5

Banking Supervisors (23 respondents)

From which sources does your organisation receive information related to trade-based money laundering?	
Customs Agencies	2
Law Enforcement Agencies	2
Financial Intelligence Units	4
Banking Supervisors	1
Financial Institutions	7
Others	2

	Yes	No
Do you perform analysis that could be used to identify, investigate, or prosecute trade-based money laundering?	6	17
Can you provide a list of ("red flag") risk indicators of potential trade-based money laundering activity that could trigger suspicions or a possible investigation?	12	6
Do you make use of any risk models or analytical tools to identify high-risk companies, commodities, countries or activities?	9	14

With which of the following domestic agencies can trade-related information be shared?				
	Customs Agencies	Law Enforcement	FIU	Tax Authority
Yes	2	4	11	3
Yes, with restrictions	10	11	3	9
No	5	3	3	4

Is information sharing between banking supervisor and other domestic agencies mandatory or voluntary?				
	Customs Agencies	Law Enforcement	FIU	Tax Authority
Mandatory	1	6	9	2
Voluntary	10	8	4	9
Not applicable	5	3	3	4

Trade Based Money Laundering

Trade Based Money Laundering

Can trade-related information be shared with foreign competent authorities?	
Yes	1
Yes, with restrictions	12
No	4

	Yes	No
Does your agency have specialists with particular expertise in the area of trade?	3	20
Do you have training programs in place that deal with the subject of trade-based money laundering?	3	18
Do you consider your country to be vulnerable to the use of trade transactions for criminal purposes?	12	5

Glossary

Alternative remittance systems (ARS) -- are operations to transfer money outside of the formal banking system. These include unregulated networks (e.g. underground banks) and regulated operations (e.g. money service businesses).*

Bill of lading -- is a document signed by a carrier to confirm the receipt of goods to and from the points indicated.

Capital flight -- is the rapid outflow of money from a country often in response to an economic event that disturbs investors and causes them to lose confidence in the country's financial stability.

Cash couriers -- are individuals that transport currency or bearer-negotiable instruments from one country to another country for the purpose of laundering the proceeds of crime or financing terrorist activities.

Commingling -- is the process of combining the proceeds of illicit activities with the earnings of legitimate businesses for the purpose of disguising the source of these illicit funds and complicating the money trail.

Front company -- is a corporate vehicle that can be used to obscure the beneficial ownership of an organisation.

Guarantee -- is an undertaking, usually on the part of a bank, to fulfill the obligations of another party or to pay a specified amount of money upon presentation of specified documents indicating that the guaranteed party has defaulted on certain obligations.

Hawala -- is a specific form of an alternative remittance system operation. A hawaladar is the operator or owner of a hawala.

Letter of credit -- is an undertaking, usually on the part of a bank and at the request of a customer, to pay a named beneficiary a specified amount of money upon presentation of specified documents set out in the terms and conditions of the letter of credit.

Shell Company -- is a company that is incorporated but has no significant assets or operations.

Smurfing (or structuring) -- is a money laundering technique, which involves the splitting up of a large bank deposit into a number of smaller deposits to evade the suspicious activity reporting requirements of financial institutions.

Trade-based money laundering -- is the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise their illicit origin.

Trade Transparency Units -- are arrangements to promote the sharing of trade data between cooperating customs agencies for the purpose of detecting and analysing suspicious trading activities.

Transfer pricing -- are pricing agreements established by mutual agreement rather than free market forces. In practice, these are often associated with intra-company transactions.

* For more information, see the Financial Action Task Force's *Money Laundering and Terrorist Financing Typologies Report for 2004-2005*.

--

Trade Based Money Laundering

Trade Based Money Laundering

Bibliography

1. Anthony and Hallet (1992), "How Successfully Do We Measure Capital Flight? The Empirical Evidence from Five Developing Countries", *Journal of Development Studies*, Vol. 23.3: 538-556.
2. Baker, R. (1999), *The Biggest Loophole in the Free-Market System*, The Washington Quarterly, Autumn, 1999.
3. Baker, R. (2005), *Capitalism's Achilles Heel – Dirty Money and How to Renew the Free-Market System*, John Wiley and Sons.
4. Bartlett, B. (2002), "The Negative Effects of Money Laundering on Economic Development", Asian Development Bank Regional Technical Assistance Project No. 5967 – Countering Money Laundering in the Asian and Pacific Region, May 2002.
5. Bhagwati, J. N. (1967), "Fiscal Policies, the Faking of Foreign Trade Declarations and the Balance of Payment". *Bulletin of the Oxford University Institute of Statistics*, February.
6. Brittain-Catlin, W. (2005), *Offshore: The Dark Side of the Global Economy*. ISBN: 0374256985.
7. Caribbean Financial Action Task Force (2001), *Money Laundering Prevention Guidelines For CFATF Member Governments, Free Trade Zone Authorities, And Merchants*
8. Caribbean Financial Action Task Force (2001), *Report of the Working Group - Free Trade Zones Typology Exercise II*
9. Cuddington, J. (1986), "Capital Flight: Estimates, Issues, and Explanations", *Princeton Studies in International Finance*, No. 58.
10. de Boyrie, M. E., S. J. Pak, and J. Zdanowicz (2005), "Estimating The Magnitude Of Capital Flight Due To Abnormal Pricing In International Trade: The Russia-USA Case", Center for International Business and Education Research (CIBER) Working Paper, Florida International University.
11. de Boyrie, M. E., S. J. Pak, and J. Zdanowicz (2004), "The Impact of Switzerland's Money Laundering Law on Capital Flows Through Abnormal Pricing in International Trade", *Applied Financial Economics*. 2005, 15, pp. 217-230.
12. De Wulf, L. (1979), "Statistical Analysis of Under- and Over-Invoicing of Imports", *Journal of Development Economics* 8 (1981).
13. EurAsianGroup (2005), "Use of Non-Resident Organisations for Reinvestment of Proceeds from Crime into the Economy (through Offshore Companies)" *EAG Typologies Research. Final Report*.
14. EurAsianGroup (2005), "Use of Fraudulent VAT Pay-Back Schemes in Exports of Goods and Services for the Purpose of Obtaining Proceeds of Crime and their Laundering", *EAG Typologies Research. Final Report*.
15. Fatehi J. (1994), "Capital Flight from Latin America as a Barometer of Political Instability", *Journal of Business Research*, 30(2), 187-195.
16. Feenstra, R., Wen Hai, Wing T. Woo, and Shunli Tao (1999), "Discrepancies in International Data: An Application to China-Hong Kong Entrepôt Trade", *American Economic Review*, May 1999, Volume 89, Issue 2.
17. Financial Action Task Force (2004), "Alternative Remittance Systems", *Money Laundering and Terrorist Financing Typologies 2004-2005*, June 2005.
18. Financial Action Task Force (2004), "Money Laundering and Terrorist Financing Trends and Indicators: Initial Perspectives", *Money Laundering and Terrorist Financing Typologies 2004-2005*, June 2005.
19. Financial Action Task Force (2006), Background Documents – Summaries of Trade-Based Money Laundering Case Studies and Domestic Regimes, FATF Secure Website.
20. Financial Action Task Force (2006), Background Documents – Summary of Responses to Trade-Based Money Laundering Questionnaire, FATF Secure Website.
21. Fisman, R. and Shang-Jin Wei (2001), "Tax Rates and Tax Evasion: Evidence from "Missing Imports" in China", *National Bureau of Economic Research Working Paper 8551*, October 2001.
22. Goetzl, A. (2005), "Why Don't Trade Numbers Add Up?" ITTO (International Tropical Timber Organisation) Tropical Forest Update 15/1 2005.
23. Gulati (1987), "A Note on Trade Misinvoicing", in *Capital Flight and Third World Debt*, Lessard, Donald and John Williamson (eds.), Washington DC: Institute for International Economics, pp. 68-78.
24. IMF (1991), "Determinants and Systemic Consequences of International Capital Flows", *A Study by the Research Department of the International Monetary Fund*.
25. Joint Money Laundering Steering Group (2006), "Guidance Notes on Prevention of Money Laundering and Combating the Financing of Terrorism", www.jmlsg.org.uk.
26. Kahn, B. (1991), "Capital Flight and Exchange Controls in South Africa", *Research Paper No. 4, Centre for the Study of the South African Economy and International Finance*, London School of Economics.
27. Khilji, F. (1993), "Comments on "Under-Invoicing of Imports: A Case Study of Pakistan"" *The Pakistan Development Review*, 32, Part II, Winter 1993.
28. Kochan, N. (2005), *The Washing Machine: How Money Laundering and Terrorist Financing Soils Us*. ISBN: 1587991594.
29. Komisar, L. (2005), "Profit Laundering and Tax Evasion - The Dirty Little Secret of Financial Globalization", *Dissent Magazine*, Spring, 2005.
30. Lessard, Donald and John Williamson eds. (1984), *Capital Flight and Third World Debt*, Washington, DC: Institute for International Economics.
31. Li, S. H. and Balachandran, K. R. (1996), "Effects of Differential Tax Rates on Transfer Pricing", *Journal of Accounting, Auditing and Finance*, 11(2), 183-96.
32. Mahmood, Z. and R. Mahmood (1993), "Under-Invoicing of Imports: A Case Study of Pakistan", *The Pakistan Development Review*, 32, Part II, Winter 1993.
33. Motala, John (1997), "Statistical Discrepancies in the World Current Account", in an *IMF Quarterly Periodical, Finance and Development*, March 1997, Volume 34, Number 1.
34. Pritchett, Lant and Sethi, Geeta (1994), "Tariff Rates, Tariff Revenue, and Tariff Reform: Some New Facts", *The World Bank Economic Review*, Volume 8, Number 1, 1994.
35. Robinson, Jeffrey (1995), *The Laundrymen – Inside the World's Third Largest Business*. Simon and Schuster, London.
36. Rustomjee, Z. (1991), "Capital Flight under Apartheid", *Transformation*, No. 15: 89-103.
37. Setiono, B. and Y. Husein, (2005), "Fighting Forest Crime and Promoting Prudent Banking for Sustainable

Trade Based Money Laundering

- Forest Management", *Centre for International Forestry Research (CIFOR) Occasional Paper No. 44*, ISSN 0854-9818.
38. Smit, B. W. and Mocke, B.A. (1991), "Capital Flight from South Africa: Magnitude and Causes", *The South African Journal of Economics*, Vol. 59.2: 101-117.
 39. Stasavage, David and Daubrée, Cécile (1998), "Determinants of Customs Fraud and Corruption: Evidence from Two African Countries", *OECD Development Centre, Working Paper No. 138*, August 1998.
 40. Swenson (2001), "Tax Reforms and Evidence of Transfer Pricing", in *National Tax Journal*, Vol. 54, No. 1, pp. 7-26.
 41. Tomohara, A. (2004), "Inefficiencies of Bilateral Advanced Pricing Agreements (BAPA) in Taxing Multinational Companies", *National Tax Journal*, Vol. LVII, No. 4, 863-873.
 42. United Nations Office on Drugs and Crime, *The Money Laundering Cycle*, http://www.unodc.org/unodc/en/money_laundering_cycle.html.
 43. US Department of State (2004), *International Narcotics Control Strategy Report for 2003*. Released by the Bureau for International Narcotics and Law Enforcement Affairs, March 2004.
 44. US Immigration and Customs Enforcement (2005), *Trade-Based Money Laundering and The ICE Trade Transparency Unit*, A Presentation for the APG, Asia Pacific Group on Money Laundering. Cairns, Australia, July 2005.
 45. Vincent, Jeffrey R. (2004), "Detecting Illegal Trade Practices by Analyzing Discrepancies in Forest Products Trade Statistics: An Application to Europe, with a Focus on Romania", *World Bank Policy Research Working Paper 3261*, April 2004.
 46. Wood, E. and T. Moll (1994), "Capital Flight from South Africa: Is Under-Invoicing Exaggerated?", *The South African Journal of Economics*, 62, 1, 1994.
 47. Woolley, Herbert (1966), "Measuring Transactions Between World Areas", *Studies in International Economic Relations*, National Bureau of Economic Research.
 48. World Trade Organisation (2005), *International Trade Statistics 2005*, http://www.wto.org/english/res_e/statis_e/its2005_e/its2005_e.pdf.
 49. Yeats, Alexander J. (1990), "On the Accuracy of Economic Observations: Do Sub-Saharan Trade Statistics Mean Anything?" *The World Bank Economic Review*, Volume 4, Number 2, May 1990.
 50. Zdanowicz, John (2004), "Who's Watching Our Back Door?" *Business Accents Magazine*, Volume 1, Number 1, Florida International University, Fall 2004.