GUIDELINES FOR PREPARATION AND SUBMISSION OF A SUSPICIOUS ACTIVITY OR TRANSACTION REPORT ON FORM 1

These guidelines are provided to assist financial institutions in preparing the revised Suspicious Activity Report (SAR), effective 30 April, 2008 and supercedes prior guidelines.

Notes

Safe Harbour: Section 13(4) of the MLPA provides protection from criminal, civil, and administrative liability for all reports of suspicious transactions made to the Supervisory Authority in good faith. Specifically, the law provides that financial institutions and their employees, staff, directors, owners or other representatives as authorized by law "shall be exempted from criminal, civil or administrative liability, as the case may be, for complying with this section for breach of any restriction on disclosure of information imposed by contract or by any legislative regulatory or administrative provision, regardless of the result of the communication."

Notification prohibited: Section 13(3) of the MLPA provides that financial institutions shall not notify any person, other than a court, or other person authorized by law, that information has been requested by or furnished to a court or the Supervisory Authority. Financial institutions should not notify any unauthorized person that the institution has detected suspicious activity or is in process of determining whether an activity or transaction is suspicious.

Tipping off prohibited: Section 7 of the MLPA prohibits any person who knows or suspects that an investigation into money laundering has been, is being or is about to be made to divulge that fact or other information to another whereby the investigation is likely to be prejudiced.

When to File a Report

1. Financial institutions listed in the First Schedule to the Money Laundering (Prevention) Act are subject to the requirements of the Act and its implementing Regulations and Guidelines and are required to promptly make a suspicious transaction report to the Supervisory Authority with respect to:
    a. Transactions that are:
        (i) Complex, unusual or large business transactions, whether completed or not
        (ii) Unusual patterns of transactions
        (iii) Insignificant but periodic transactions which have no apparent economic or lawful purpose
        (iv) Relations and transactions with persons, including business and other financial institutions, from countries that have not adopted a comprehensive anti-money laundering programme.

b. Any transaction conducted or attempted by, at or through the financial institution when the financial institution knows, suspects or has reason to suspect that:

(i) The transaction involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade anti-money laundering laws or regulations or to avoid any transaction reporting requirements.

(ii) The transaction is designed, whether through structuring (smurfing) or other means, to evade any anti-money laundering regulations.

(iii) The transaction has no business or apparent lawful purpose 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.

2. Computer intrusion. For purposes of this report, "computer intrusion" is defined as gaining access to a computer system of a financial institution to:
   a. Remove, steal, procure, or otherwise affect funds of the institution or the institution's customers;
   b. Remove, steal, procure, or otherwise affect critical information of the institution including customer account information; or
   c. Damage, disable, or otherwise affect critical systems of the institution.

   For purposes of this reporting requirement, computer intrusion does not mean attempted intrusions of websites or other non-critical information systems of the institution that provide no access to institution or customer financial or other critical information.
3. File promptly (but no later than 30 calendar days) after the date of initial detection of facts that constitute a basis for making the report. In situations involving suspicious transactions requiring immediate attention, such as ongoing money laundering schemes, a financial institution shall immediately notify by telephone the Supervisory Authority. When the STR form is finally lodged with the Supervisory Authority, the telephone notification to the Supervisory Authority should be recorded as part of the STR.

Guidelines for Filling out a Suspicious Activity/Transaction Report Form

A. Abbreviations and Definitions

1. ONDCP: Office of National Drug and Money Laundering Control Policy
2. MLPA: Money Laundering (Prevention) Act 1996 as amended
3. MLPR: Money Laundering (Prevention) Regulations 2007
4. MLG: Money Laundering and Financing of Terrorism Guidelines
5. SAR: Suspicious Activity Report

B. How to Make a Report

1. Send each completed suspicious activity report to:

   The Supervisory Authority
   ONDCP Headquarters
   P.O. Box W827
   Camp Blizard
   Antigua

2. Leave blank any items on the form that do not apply or for which information is unavailable. All other items should be filled in.

3. Items marked with an **asterisk *** are considered critical and are required to **be completed if known.**

4. Do not include original documents with the suspicious activity report submitted. Provide copies. Identify and retain a copy of the suspicious activity report and all supporting documentation or business record equivalent for your files for six (6) years from the date of the suspicious activity report. All supporting documentation such as, copies of instruments; receipts; sale, transaction or clearing records; photographs, surveillance audio and/or video recording medium, must be made available to authorized persons acting on behalf of the Supervisory Authority.

5. Type or complete the report using block written letters.

6. Enter all **dates** in DD/MM/YYYY format where DD=day, MM=month, and YYYY=year. Precede any single number with a zero, i.e., 01, 02 etc.

7. Enter all **telephone numbers** with (country and area code) first and then the remaining numbers.

8. Addresses, general.

C. Instructions for Preparing a Suspicious Activity Report

Item 1 — Corrects prior report: If you are correcting a previously filed report, check the box at the beginning of the report. Complete the report in its entirety and include the corrected information in the applicable boxes. Then describe the changes that are being made in Part D – Description and Explanation of Suspicious Transaction/Activity.

Part A – IDENTITY OF SUBJECT(S) CONDUCTING THE SUSPICIOUS ACTIVITY OR TRANSACTION

In this Part, the word subject refers to any person (natural or legal) or legal arrangement that is suspected of conducting a suspicious transaction or engaging in suspicious activity.

Item 2 — Subject information unavailable: If information on the subject suspected of conducting the transaction or engaging in the suspect activity is not available check the box. Describe the reasons why the information is not available in Part D – Description

and Explanation of Suspicious Transaction/Activity. This serves to alert the FIU that this information have not been inadvertently omitted.

Item 3 — Multiple subjects involved: If more than one subject is involved in the suspicious transaction/activity check the box. Print extra copies of Part A (the first page of the report) and fill in the details of the additional subjects and attach it (them) behind page 1 of the report.

SUBJECT INFORMATION

Item 4 — Name of individual or entity: If the suspicious activity involves an individual, enter his or her last name in Item 4(a), first name in Item 4(b) and middle name or initial in Item 4(c). If there it no middle name or initial leave Item 4(c) blank. If the reporting institution has knowledge of the subject using an alias enter the full alias in Item 4(d). If the suspicious activity involves an organization, enter its name in Item 4(a).

If the reporting institution has knowledge of the subject using a trading name ("trading as"), enter the individual or organization's trading name in Item 4(e) starting with "T/A" followed by the name of the business.

For example, 4(a) Smith, (b) John, (c) D., (d) John D. Smythe, (e) T/A Smithies' Car Parts; or for an organization 4(a) John D. Smith Ltd., (e) T/A Smithies' Car Parts.

If additional space is needed to report more than one alias, attach additional copies of page 1 to report the additional information.

Item 5 — Address: Enter the permanent street address including any apartment or suite number of the person identified in Item 5(a); a Post Office Box should only be used if there is no street address. Enter the city, town or village in which the person shown in Item 4 resides or in which the organization is located in Item 5(b). Enter the state, province or territory in Item 5(c), and the postcode or zipcode in Item 5(d). Write out the full name of the country that corresponds to Items 5(a) to (d).

Item 6 — Date of birth: If an individual is named in Item 4, enter his or her date of birth by using the method for entering dates described at the beginning of these Guidelines, [DD/MMM/YYYY].

Item 7 — Country of registration: If the subject named in Item 4 is an organization, enter the name of the country where it is registered or incorporated.

Item 8 —Occupation/Type of business: Fully identify the occupation, profession or business of the person on whose behalf the transaction(s) was conducted. For example, secretary, fisherman, carpenter, attorney, housewife, restaurant owner, liquor store clerk, disc jockey, director of computer company, etc. Do not use non-specific terms such as merchant, self-employed, director, manager, businessman, etc.

Item 9 — Telephone number: In Item 9(a) enter the home telephone number, including the area code for the individual entered in Item 4. In Item 9(b) enter the business telephone number, including area code of the individual or organization entered in Item 4.

Item 10 —Forms of Identity Verification: In item 10(a) **c**heck the appropriate box or boxes for the form(s) of identification provided by the subject and use the line provided

to give specific data such as driver's licence or passport number. In item 10(b) enter the name of the authority that issued the identification document. If more than one form of identification was obtained enter the box number then the name of the authority, e.g. if the boxes for passport and driver's licence are checked, then in item 10(b) there could be entered (i) Government of the United States; (ii) State of Florida.

For Item 10(a)(vi), "other", provide a brief explanation in the space provided. If more space is required, enter the information in Part D.

Online version: In item 10 select the appropriate document type from the drop down menu. If the document type is not listed then type in an appropriate name. Next insert the document number in the box labeled "No." Then, enter the name of the authority that issued the identity document. Details for two identity documents can be entered. If more than two identity documents were obtained, details of the extra documents can be entered in Part D.

Item 11 — Subject's relationship to the reporting financial institution: Check each box that identifies the subject's relationship with the financial institution. More than one box may be checked. If the other box, Item 11(l) is checked, provide a brief explanation on the adjacent blank space. If more space is required, enter the information in Part D.

Item 12 — Is the subject working with or for the institution?: Check the appropriate box in Item 12(a) to indicate if the subject is or is not employed or retained by the reporting institution. If the "Yes" box is checked indicate if the subject is still employed, suspended, terminated or has resigned by checking box b, c, d or e.

Item 13 — Date of suspension, termination or resignation: Enter the date the subject was suspended, terminated or resigned by using the method for entering dates described at the beginning of the Guidelines. [DD/MMM/YYYY].

Part B – DETAILS OF THE TRANSACTION OR ACTIVITY

Item 14 — Type of financial services involved in suspicious transaction: Enter the type or category of service offered by the reporting institution that the subject described in Item 4 was trying to use or take advantage of.

Item 15 — Date or date range of suspicious transaction or activity: Enter the first known date suspicious activity and the last date of related suspicious activity. If only one date applies, include this date in the From field using the instruction at the beginning of these Guidelines. If multiple or related activity is conducted by the individual during the reporting period, the reporting institution may report all activity on one SAR. Enter the date of the initial activity in the From field and the last occurrence date in the To field. (The first known date is a mandatory field.) [DD/MMM/YYYY].

Item 16 — EC Dollar amount of transaction(s): Enter the dollar amount involved in the suspicious activity in Eastern Caribbean Currency. Where all or part of the amount is in a foreign currency covert it to its EC equivalent. If less than a full dollar is involved, round it to the next highest dollar.

An aggregated total of all transactions for multiple or related suspicious activities by the same individual or organization within the same reporting period may be shown in this field.

Item 17 — If non-E.C. currency is involved in the transaction(s) specify the currency and the amount: Enter the standardized three-letter code for the non-E.C. currency and then enter the amount in the appropriate boxes. The amount should be rounded up to the nearest primary denomination of the currency, eg. (United States Dollars)—USD100.50 to USD101.00; (United Kingdom Pounds Sterling)—GBP251.60 to GBP252.00; (European Euros)—EUR44,782.34 TO EUR44,783.00.

Item 18 — Type and quantity of instruments involved: List the type of monetary instrument(s) involved and the amount of money represented by each instrument in the transaction, eg. (1) Cash: USD$10,000; (2) Traveler's cheques: £5,000 sterling; (3) Wire transfers: €1,500. The amount for a single type of monetary instrument should be aggregated, eg. One traveler's cheque in the amount of USD$1,000 and a second traveler's cheque in the amount of USD$2,000 should be listed as USD$3,000. If there is more than one of the same type of monetary instrument, but they are for different currencies then specify the number and currencies, eg. If there was a traveler's cheque for USD$1,000 and another traveler's cheque for €5,000, then the should be listed as eg. (1) Two traveler's cheques --- USD$1,000 and €5,000. Where extra space would be needed then the break-down of the total may then be listed in Part D.

Item 19 — Transaction number(s): List the transaction number for each transaction involved.

Item 20 — Accounts affected: List the number of any account(s) that were affected by the suspicious transaction or activity. If more than four accounts are affected, provide the additional account numbers in Part D. If no account is affected, leave Item 20 blank.

Item 21 — If account closed, date closed: For each account listed in Item 20, if the account has been closed, indicate in the corresponding list number the date of closure.

Part C – Summary Characterization of Suspicious Activity

Item 22 — Category of Suspicious Activity: Check all box(es) which to the best of the knowledge of the reporting institution describes the suspicious activity and where there are sufficient indicators, identifies the nature of possible criminal conduct that may underlie the suspicious activity. A brief description of the categories can be found in the list titled "Explanation of Summary Categories of Suspicious Activity" at the end of these notes (before the Typologies). More than one box may be checked. If "other" is checked, enter a brief explanation in the space provided. Do not use this space in lieu of a full description of the activity/transaction in Part D — Description and Explanation of Suspicious Transaction/Activity (Part D is a mandatory field).

If box (r) is checked, then the number by which is listed a typology similar to the activity being reported must be entered in the space provided. For example, where the suspicious activity being reported resembles transactions that are not consistent with the customer's business or income level, then box (r) should be checked, and the line should read: "(r) The suspicious activity resembles typology No. A(8)".

List of typologies: The numbered list of typologies can be found at the end of these instructions in the section: "Typologies — Examples of Potentially Suspicious Transactions".

Item 23 — Character of suspicious activity: Check all box(es) which identify the general category of suspicious activity.

Part D – DESCRIPTION AND EXPLANATION OF SUSPICIOUS TRANSACTION/ACTIVITY

Item 24 — Give the reasons why you consider the transaction or activity reported in Part B to be suspicious: As stated in Part D, this section of the report is **critical.** The care with which it is written may determine whether or not the described conduct and its possible criminal nature are clearly understood. Provide a complete chronological account of what is unusual, irregular or suspicious about the transactions. The narrative should include the material indicated in Part B (bullet points a to s) but should also include any other information that you believe is necessary to better enable investigators to understand the transaction you are reporting. If necessary, continue the narrative on a separate sheet of paper headed "Part D (continued)". Remember that the originals of any supporting documentation provided such as spreadsheets, photocopies of canceled checks or other documents, photos, etc., must be retained at the financial institution.

Item 25 — Is additional information attached to this report?: Check the appropriate box to indicate whether additional information is attached to the SAR. If the "Yes" is checked, state what documents or materials accompany the SAR.

Part E – DETAILS OF REPORTING FINANCIAL INSTITUTION

Item 26 — Type of financial institution reporting: Enter the type of financial institution making the report, eg. Bank, insurance company, money transmission service, etc.

Item 27 — Name of financial institution: Enter the full legal [Trade] name of the reporting financial institution.

Item 28 — Address of financial institution: In the appropriate blanks enter the street address of the reporting institution shown in Item 27. A Post Office Box number should be used only if there is no street address. Enter the city where the reporting financial institution is located and the name of the state, province or territorial region where the financial institution is located. Enter the post or zip code that corresponds with the address entered. Enter the country where the address entered is located.

Item 29 — Location of branch where transaction, activity or the attempt took place: If the location where the suspicious transaction or activity took place is different from that provided in Item 28, enter the street address of the branch or office where the activity occurred. A P.O. Box may be used only if there is no street address. Otherwise, leave Item 29 blank. Enter the city where the branch is located and the name of the state, province or territorial region where the branch is located. Enter the post or zip code that corresponds with the address entered for the branch. Enter the country where the address entered for the branch is located.

Item 30 — Check the box if the suspicious activity took place in more than one branch or location: If the suspicious activity occurred at more than one branch, check the box indicating multiple branches, and include this information in Part D — Description and Explanation of Suspicious Transaction/Activity.

Item 31 — Details of Compliance Officer of authorized person who can be contacted for information in this matter: Enter the name of the person charged with the responsibility of completing the SAR and lodging it with the Supervisory Authority. Ordinarily this should be the Compliance Officer, otherwise it must be someone officially authorized to carry out the function of completing and lodging the SAR. This person should also be the point of contact in the financial institution in relation to the matter being reported. The person should have specific knowledge of the underlying facts. In the appropriate blanks enter the title or position of the person, details of the person's office address within the reporting institution, enter a telephone number where the person can be contacted, enter a fax number where the person can be contacted; enter an email address where the person can be reached.

Part F – STATEMENT OF REPORTING FINANCIAL INSTITUTION

Item 32 — Statement of the Financial Institution: The person named in Item 31 must read the statement written in Item 32 and the declaration contained in it, "I declare the information contained in this report to be correct to the best of my knowledge, information and belief." The Compliance Officer or authorized person named in Item 31 should then fill in the date on completing preparation of the SAR by using the method for entering dates described at the beginning of these Guidelines, [DD/MMM/YYYY]. The person should then place his signature below in the space to the right of the words "SIGN HERE". The person should bear in mind that it is a criminal offence to make a false or falsified SAR under section 13(5) of the MLPA and there are provisions for criminal sanctions under section 13(6) of the Act.

Explanation of Summary Categories of Suspicious Activity

Category	Characterization of suspicious activity	Explanation/Description
a	Structuring/layering	Structuring or layering involves the carrying out of multiple transactions that aggregate to significant sums of money or transfer of a large sum by multiple transactions of much smaller amounts: 1. To avoid customer identity verification requirements under Regulations and Guidelines. 2. To avoid suspicious activity detection and conventional monitoring thresholds and filters. 3. To avoid enhanced scrutiny or additional review frequently triggered by higher transaction amounts and thresholds. 4. To avoid generating a suspicious activity report to the Supervisory Authority under the Money Laundering (Prevention) Act.
b	Money laundering	In money laundering: 1. The transaction involves funds derived from criminal activity or funds used to conduct criminal activity. 2. The transaction is conducted to receive, transfer or dispose of funds or assets derived from or used in criminal activity. 3. The transaction is conducted to hide or disguise funds or assets derived from criminal activity. This includes concealing the ownership, possession, control, location, source or nature of the funds or assets. 4. The transaction has no apparent lawful purpose or is not the type of transaction that would normally be expected to be conducted by the customer, and there is no reasonable explanation for the transaction after examining its background.
c	Cheque fraud	Use of counterfeit or altered cheques, withdrawal of funds against cheques with forged signatures or endorsements.
d	Computer intrusion	Where access is gained to a computer system of a financial institution to: ▪ steal, remove, procure or otherwise affect funds of the institution or its customers ▪ affect critical customer account information ▪ damage, disable or otherwise affect critical systems of a financial institution. (Does not include access to non critical systems which provide no access to customer financial or other critical information.)
e	Counterfeit cheque	A legitimate cheque that is altered or forged in some aspect (such as the payee's name) while being purported to be genuine.
f	Counterfeit instrument	Manufacture, copy or reproduction or forgery of an instrument with intent to defraud a financial institution.
g	Credit card fraud	The intentional procurement of goods, services or money without the authorization of the cardholder by using stolen, lost or cancelled credit cards.
h	Debit card fraud	The unauthorized use of a stolen, lost or cancelled debit card for payment of goods, services or to obtain money. Debit cards are used in place of cheques or cash. They directly deplete the funds in a customer's account.
i	Embezzlement	Stealing of money or funds from an employer or for personal

		benefit willfully misapplying money or funds entrusted to a person's possession or care by an organisation;
j	False invoicing	Deliberately overstating or understating the value of goods on trade documents with intent to avoid duties or as part of an arrangement to make concealed payments or transfers of value, eg. Invoices for goods that were never ordered or received, which could be used to obtain loans etc.
k	Identity theft	Use without authorization of the means of identification of another with the intent to commit unlawful activity.
l	Investment fraud	Receiving money from clients to invest on their behalf and either failing to invest or improperly disposing of the money, such as by using it for personal benefit. This can be related to customer accounts into which a large number of unrelated persons make deposits often of similar amounts, and the money is primarily being transferred to personal accounts or used for the personal affairs of the account holder or in an uneconomic manner.
m	Mysterious disappearance	Unexplained disappearance of moneys, or other instruments of value, in bearer form, from a financial institution's branch, agency, organization, or holding company.
n	Refusal/failure to complete CDD requirement	Refusal or failure by a customer to provide the identification and verification information required with no satisfactory explanation.
o	Refusal/failure to update CDD requirement	After an account is opened, refusal or failure by a customer to provide updated identification and verification information as required by law.
p	Terrorist financing	Funds belonging to or controlled by any declared terrorist. Provision or collection of funds intending, knowing or having reasonable grounds to believe that the funds will be used to commit or promote terrorist acts. Providing or making available financial or related services intending that they be used for committing or facilitating terrorist acts or benefiting a person committing such acts.
q	Wire transfer fraud	The transmission of electronic funds with the intent to obtain money or property by fraudulent means or false pretenses.

TYPOLOGIES — EXAMPLES OF POTENTIALLY SUSPICIOUS TRANSACTIONS

DEPOSIT TAKING INSTITUTIONS

A. General

(1) Refusal or reluctance to proceed with a transaction, or abruptly withdrawing a transaction.

(2) Customer refusal or reluctance to provide information or identification.

(3) Structured or recurring transactions below the threshold requiring customer verification.

(4) Multiple third parties conducting separate, but related transactions below the threshold requiring customer verification.

(5) Even dollar amount transactions.

(6) Transactions structured to lose the paper trail.

(7) Significant increases in the number or amount of transactions.

(8) Transactions which are not consistent with the customer's business or income level.

(9) Transactions by non-account holders.

B. Cash Transactions

(1) Unusually large cash deposits made by an individual or company whose ostensible business activities would normally be generated by cheques and other instruments.

(2) Substantial increases in cash deposits of any individual or business without apparent cause, especially if such deposits are subsequently transferred within a short period out of the account and/or to a destination not normally associated with the customer.

(3) Customer deposits cash by means of numerous credit slips so that the total of each deposit is unremarkable, but the total of all the credits is significant.

(4) Company accounts whose transactions, both deposits and withdrawals, are denominated by cash rather than the forms of debit and credit normally associated with commercial operations (e.g. cheques, Letters of Credit, Bills of Exchange, etc.)

(5) Customers who constantly pay in or deposit cash to cover requests for bankers drafts, money transfers or other negotiable and readily marketable money instruments.

(6) Customers who seek to exchange large quantities of low denomination notes for those of higher denomination.

(7) Frequent exchange of cash into other currencies without good reason.

(8) Branches that have a great deal more cash transactions than usual. (Head Office

statistics detect aberrations in cash transactions.)

(9) Customers whose deposits contain counterfeit notes or forged instruments.

(10) Customers transferring large sums of money to or from overseas locations with instructions for payment in cash.

(11) Large cash deposits using night safe facilities, thereby avoiding direct contact with deposit taking institution or financial institution staff.

C. Accounts

(1) Customers who wish to maintain a number of trustee or client accounts which do not appear consistent with the type of business, including transactions which involve nominee names.

(2) Customers who have numerous accounts and pay in amounts of cash to each of them in circumstances in which the total of credits would be a large amount.

(3) Any individual or company whose account shows virtually no normal personal banking or business related activities, but is used to receive or disburse large sums which have no obvious purpose or relationship to the account holder and/or his business (e.g. a substantial increase in turnover on an account).

(4) Reluctance to provide normal information when opening an account, providing minimal or fictional information or, when applying to open an account, providing information that is difficult or expensive for the financial institution to verify.

(5) Customers who appear to have accounts with several financial institutions within the same locality, especially when the deposit taking institution or building society is aware of a regular consolidation process from such accounts prior to a request for onward transmission of the funds.

(6) Matching of payments out with credits paid in by cash on the same or previous day.

(7) Paying in large third party cheques endorsed in favour of the customer.

(8) Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad.

(9) Customers who together, and simultaneously, use separate tellers to conduct large cash transactions or foreign exchange transactions.

(10) Greater use of safe deposit facilities. Increased activity by individuals. The use of sealed packets deposited and withdrawn.

(11) Companies' representatives avoiding contact with the branch.

(12) Substantial increases in deposits of cash or negotiable instruments by a professional firm or company, using client accounts or in-house company or trust accounts, especially if the deposits are promptly transferred between other client company and trust accounts.

(13) Customers who show an apparent disregard for accounts offering more favourable terms.

(14) Customers who decline to provide information that in normal circumstances would

make the customer eligible for credit or for other banking services that would be regarded as valuable.

(15) Insufficient use of normal investment facilities, e.g. avoidance of high interest rate accounts for large balances.

(16) Large number of individuals making payments into the same account without an adequate explanation.

(17) Customers who request that account statements and other correspondence be kept at the financial institution for collection or from whom correspondence is returned "not known at this address" etc.

D. International banking/trading finance

(1) Customer introduced by an overseas branch, affiliate or other deposit taking institution based in countries where production of drugs or drug trafficking may be prevalent.

(2) Use of Letter of Credit and other methods of trade finance to move money between countries where such trade is not consistent with the customer's usual business.

(3) Customers who make regular and large payments, including wire transactions, that cannot be clearly identified as bona fide transactions to, or receive regular and large payments from: countries which are commonly associated with the production, processing or marketing of drugs; or proscribed terrorist organisations.

(4) Building up of large balances, not consistent with the known turnover of the customer's business, and subsequent transfer to account(s) held overseas.

(5) Unexplained electronic fund transfers by customers on an in and out basis or without passing through an account.

(6) Wire transfers that do not contain complete originator information

(7) Frequent requests for travelers cheques, foreign currency drafts or other negotiable instruments to be issued that are not consistent with known customer profile.

(8) Customers who show apparent disregard for arrangements offering more favourable terms.

E. Institution employees and agents

(1) Changes in employee characteristics, e.g. lavish life styles or avoiding taking holidays.

(2) Changes in employee or agent performance, e.g. the salesman selling products for cash has a remarkable or unexpected increase in performance.

(3) Any dealing with an agent where the identity of the ultimate beneficiary or counterpart is undisclosed, contrary to normal procedure for the type of business concerned.

F. Secured and unsecured lending

(1) Customers who repay problem loans unexpectedly.

(2) Request to borrow against assets held by the financial institution or a third party, where the origin of the assets id not known or the assets are inconsistent with the customer's standing.

(3) Request by a customer for a financial institution to provide or arrange finance where the source of the customer's financial contribution to a deal is unclear, particularly where property is involved.

(4) Customers who unexpectedly repay in part or full a mortgage or other loan in a way inconsistent with their earnings capacity or asset base.

G. Casinos and internet gaming businesses

(1) Customers who request that payouts be sent to third parties, particularly in jurisdictions other than their jurisdiction of domicile.

(2) Customers who deposit significant sums into their player accounts and then withdraw the money without having undertaken much gaming activity.

(3) Customers who engage in structuring.

(4) Customer is paid on a losing bet.

INSURANCE:

H. General Indicators

(1) application for a policy from a potential client in a distant place where a comparable policy could be provided "closer to home"

(2) application for business outside the policyholder's normal pattern of business

(3) introduction by an agent/intermediary in an unregulated or loosely regulated jurisdiction or where organised criminal activities (e.g. drug trafficking or terrorist activity) or corruption are prevalent

(4) any want of information or delay in the provision of information to enable verification to be completed

(5) an atypical incidence of pre-payment of insurance premiums

(6) the client accepts very unfavourable conditions unrelated to his or her health or age

(7) the transaction involves use and payment of a performance bond resulting in a cross-border payment (wire transfers) = the first (or single) premium is paid from a bank account outside the country

(8) large fund flows through non-resident accounts with brokerage firms

(9) insurance policies with premiums that exceed the client's apparent means

(10) the client requests an insurance product that has no discernible purpose and is reluctant to divulge the reason for the investment

(11) insurance policies with values that appear to be inconsistent with the client's insurance needs

(12) the client conducts a transaction that results in a conspicuous increase of investment contributions

(13) any transaction involving an undisclosed party

(14) early termination of a product, especially at a loss, or where cash was tendered and/or the refund cheque is to a third party

(15) a transfer of the benefit of a product to an apparently unrelated third party

(16) a change of the designated beneficiaries (especially if this can be achieved without knowledge or consent of the insurer and/or the right to payment could be transferred simply by signing an endorsement on the policy)

(17) substitution, during the life of an insurance contract, or the ultimate beneficiary with a person without any apparent connection with the policyholder

(18) requests for a large purchase of a lump sum contract where the policyholder has usually made small, regular payment.

(19) attempts to use a third party cheque to make a proposed purchase of a policy but much interest in the early cancellation of the contract

(20) the applicant for insurance business attempts to use cash to complete a proposed transaction when this type of business transaction would normally be handled by cheques or other payment instruments

(21) the applicant for insurance business requests to make a lump sum payment by a wire transfer or with foreign currency

(22) the applicant for insurance business is reluctant to provide normal information when applying for a policy, providing minimal or fictitious information or, provides information that is difficult or expensive for the institution to verify

(23) the applicant for insurance business appears to have policies with several institutions

(24) the applicant for insurance business purchases policies in amounts considered beyond the customer's apparent means

(25) the applicant for insurance business establishes a large insurance policy and within a short time period cancels the policy, requests the return of the cash value payable to a third party

(26) the applicant for insurance business wants to borrow the maximum cash value of a single premium policy, soon after paying for the policy

(27) the applicant for insurance business uses a mailing address outside the insurance supervisor's jurisdiction and where during the verification process it is discovered that the home telephone has been disconnected.

I. Life insurance

(1) A company director from Company W, Mr. H, sets up a money laundering scheme involving two companies, each one established under two different legal systems. Both of the entities were to provide financial services and providing financial

guarantees for which he would act as director. These companies wired the sum of USD 1.1 million to the accounts of Mr. H in Country S. It is likely that the funds originated in some sort of criminal activity and had already been introduced in some way into the financial system. Mr. H also received transfers from Country C. Funds were transferred from one account to another (several types of accounts were involved, including both current and savings accounts). Through one of these transfers, the funds were transferred to Country U from a current account in order to make payments on life insurance policies. The investment in these policies was the main mechanism in the scheme for laundering the funds. The premiums paid for the life insurance policies in country U amounted to some USD 1.2 million and represented the last step in the laundering operation.

(2) An attempt was made to purchase life policies for a number of foreign nationals. The underwriter was requested to provide life coverage with an indemnity value identical to the premium. There were also indications that in the event that the policies were to be cancelled, the return premiums were to be paid into a bank account in a different jurisdiction to the assured.

(3) On a smaller scale, local police authorities were investigating the placement of cash by a drug trafficker. The funds were deposited into several bank accounts and then transferred to an account in another jurisdiction. The drug trafficker then entered into a USD 75,000 life insurance policy. Payment for the policy was made by two separate wire transfers from the overseas accounts. It was purported that the funds used for payment were the proceeds of overseas investments. At the time of the drug trafficker's arrest, the insurer has received instructions for the early surrender of the policy.

(4) In 1990, a British insurance sales agent was convicted of violating a money laundering statute. The insurance agent was involved in a money laundering scheme in which over USD 1.5 million was initially placed with a bank in England. The "layering process" involved the purchase of single premium insurance policies. The insurance agent became a top producer at his insurance company and later won a company award for his sales efforts. This particular case involved the efforts of more than just a sales agent. The insurance agent's supervisor was also charged with violating the money laundering statute.

This case has shown how money laundering, coupled with a corrupt employee, can expose an insurance company to negative publicity and possible criminal liability.

(5) Customs officials in Country X initiated an investigation which identified a narcotics trafficking organisation utilised the insurance sector to launder proceeds. Investigative efforts by law enforcement agencies in several different countries identified narcotic traffickers were laundering funds through insurance firm Z in an off-shore jurisdiction.

(6) Insurance firm Z offers investment products similar to mutual funds. The rate of return is tied to the major world stock market indices so the insurance policies were able to perform as investments. The account holders would over-fund the policy, moving monies into and out of the fund for the cost of the penalty for early withdrawal. The funds would then emerge as a wire transfer or cheque from an

insurance company and the funds were apparently clean. To date, this investigation has identified that over USD 29 million was laundered through this scheme, of which over USD 9 million dollars has been seized. Additionally, based on joint investigative efforts by Country Y (the source country of the narcotics) and country Z customs officials, several search warrants and arrest warrants were executed relating to money laundering activities that involved individuals associated with insurance firm Z.

(7) A customer contracted life insurance of a 10 year duration with a cash payment equivalent to around USD 400,000. Following payment, the customer refused to disclose the origin of the funds. The insurer reported the case. It appears that prosecution had been initiated in respect of the individual's fraudulent management activity.

(8) A life insurer learned from the media that a foreigner, with whom it had two life-insurance contracts, was involved in Mafia activities in his/her country. The contracts were of 33 years duration. One provided for a payment of close to the equivalent of USD 1 million in case of death. The other was a mixed insurance with value of over half this amount.

(9) A client domiciled in a country party to a treaty on the freedom of cross-border provision of insurance services, contracted with a life insurer for a foreign life insurance for 5 years with death cover for a down payment equivalent to around USD 7 million. The beneficiary was altered twice: 3 months after the establishment of the policy and 2 months before the expiry of the insurance. The insured remained the same. The insurer reported the case. The last beneficiary - an alias - turned out to be a PEP.

J. Non-life insurance

(1) A money launderer purchased marine property and casualty insurance for a phantom ocean-going vessel. He paid large premiums on the policy and suborned the intermediaries so that regular claims were made and paid. However, he was very careful to ensure that the claims were less than the premium payments, so that the insurer enjoyed a reasonable profit on the policy. In this way, the money launderer was able to receive claims cheques which could be used to launder funds. The funds appeared to come from a reputable insurance company, and few questioned the source of the funds having seen the name of the company on the cheque or wire transfer.

(2) Four broking agencies were forced to freeze funds after US court action that followed an investigation into Latin American drugs smuggling. The drug trafficking investigation, codenamed Golden Jet, was coordinated by the Drug Enforcement Agency (DEA) based in the USA but also involved the FBI and the UK authorities. The funds frozen by the court action related to insurance money deposited at insurance brokers for around 50 aircraft.

It is understood that the brokers affected by the court order included some of the largest US insurance brokers. The case highlighted the potential vulnerability of the insurance market to sophisticated and large scale drug trafficking and money

laundering operators. The court order froze aircraft insurance premiums taken out by 17 Colombian and Panamanian air cargo companies and by 9 individuals. The action named 50 aircraft, including 13 Boeing 727s, 1 Boeing 707, 1 French Caravelle and 2 Hercules C130 transport aircraft. The British end of the action was just one small part of a massive anti-drug trafficking action co-ordinated by the DEA. Officials of the DEA believe Golden Jet is one of the biggest blows they have been able to strike against the narcotics trade. The American authorities led by the DEA swooped on a n alleged Colombian drugs baron and tons of cocaine valued at many billions of dollars were seized and a massive cocaine processing factory located in Colombia together with aircraft valued at more than USD22 million were destroyed in the DEA coordinated action. According to the indictment, the cargo companies were responsible for shipping tons of cocaine from South to North America all through the 1980s and early 1990s, providing a link between the producers and the consumers of the drugs. Much of the cocaine flowing into the USA was transported into the country by air. During this period the Colombian cartels rose to wealth and prominence, aided by those transport links.

K. Intermediaries

(1) A person (later arrested for drug trafficking) made a financial investment (life insurance) of USD 250,000 by means of an insurance broker. He acted as follows. He contacted an insurance broker and delivered a total amount of USD 250,000 in three cash installments. The insurance broker did not report the delivery of that amount and deposited the three installments in the bank. These actions raise no suspicion at the bank, since the insurance broker is known to them as being connected to the insurance branch. The insurance broker delivers, afterwards, to the insurance company responsible for making the financial investment, three cheques from a bank account under his name, totaling USD 250,000, thus avoiding the raising suspicions with the insurance company.

(2) Clients in several countries used the services of an intermediary to purchase insurance policies. Identification was taken from the client by way of an ID card, but these details were unable to be clarified by the providing institution locally, which was reliant on the intermediary doing due diligence checks. The policy was put in place and the relevant payments were made by the intermediary to the local institution. Then, after a couple of months had elapsed, the institution would receive notification from the client stating that there was now a change in circumstances, and they would have to close the policy suffering the losses but coming away with a clean cheque from the institution. On other occasions the policy would be left to run for a couple of years before being closed with the request that the payment be made to a third party. This was often paid with the receiving institution, if local, not querying the payment as it had come from another reputable local institution.

(3) An insurance company was established by a well-established insurance management operation. One of the clients, a Russian insurance company, had been introduced through the management of the company's London office via an intermediary. In this particular deal, the client would receive a "profit commission" if the claims for the period were less than the premiums received. Following an on-site inspection of the company by the insurance regulators, it became apparent that

the payment route out for the profit commission did not match the flow of funds into the insurance company's account. Also, the regulators were unable to ascertain the origin and route of the funds as the intermediary involved refused to supply this information. Following further investigation, it was noted that there were several companies involved in the payment of funds and it was difficult to ascertain how these companies were connected with the original insured, the Russian insurance company.

(4) A construction project was being financed in Europe. The financing also provided for a consulting company's fees. To secure the payment of the fees, an investment account was established and a sum equivalent to around USD 400,000 deposited with a life insurer. The consulting company obtained powers of attorney for the account. Immediately following the setting up of the account, the consulting company withdrew the entire fee stipulated by the consulting contract. The insurer reported the transaction as suspicious. It turns out that an employee of the consulting company was involved in several similar cases. The account was frozen.

L. Reinsurance

(1) An insurer in country A sought reinsurance with a reputable reinsurance company in country B for its directors and officer cover of an investment firm in country A. The insurer was prepared to pay four times the market rate for this reinsurance cover. This raised the suspicion of the reinsurer which contacted law enforcement agencies. Investigation made clear that the investment firm was bogus and controlled by criminals with a drug background. The insurer had ownership links with the investment firm. The impression is that - although drug money would be laundered by a payment received from the reinsurer - the main purpose was to create the appearance of legitimacy by using the name of a reputable reinsurer. By offering to pay above the market rate the insurer probably intended to assure continuation of the reinsurance arrangement.

(2) A state insurer in country A sought reinsurance cover for its cover of an airline company. When checking publicly available information on the company it turned out that the company was linked to potential war lords and drug traffickers. A report was made to the law enforcement authorities.

M. Return premiums

There are several cases where the early cancellation of policies with return of premium has been used to launder money. This has occurred where there have been:

(1) a number of policies entered into by the same insurer/intermediary for small amounts and then cancelled at the same time

(2) return premium being credited to an account different from the original account

(3) requests for return premiums in currencies different to the original premium, and

(4) regular purchase and cancellation of policies.

N. Over payment of premiums

(1) Another simple method by which funds can be laundered is by arranging for excessive numbers or excessively high values of insurance reimbursements by cheque or wire transfer to be made. A money launderer may well own legitimate assets or businesses as well as an illegal enterprise. In this method, the launderer may arrange for insurance of the legitimate assets and 'accidentally', but in a recurring basis, significantly overpay his premiums and request a refund for the excess. Often, the person does so in the belief that his relationship with his representative at the company is such that the representative will be unwilling to confront a customer who is both profitable to the company and important to his own success.

(2) The overpayment of premiums, has been used as a method of money laundering, Insurers should be especially vigilant where:

(a) the overpayment is over a certain size (say USD 10,000 or equivalent)

(b) the request to refund the excess premium was to a third party

(c) the assured is in a jurisdiction associated with money laundering and

(d) where the size or regularity of overpayments is suspicious

O. High brokerage/third party payments/strange premium routes

(1) High brokerage can be used to pay off third parties unrelated to the insurance contract. This often coincides with examples of unusual premium routes.

P. Claims

A claim is one of the principal methods of laundering money through insurance. Outlined below are examples of where claims have resulted in reports of suspected money laundering and terrorist financing.

(1) A claim was notified by the assured, a solicitor, who was being sued by one of his clients. The solicitor was being sued for breach of confidentiality, which led to the client's creditors discovering funds that had allegedly been smuggled overseas. Documents indicated that the solicitor's client might be involved in tax evasion, currency smuggling and money laundering.

(2) A claim was notified relating to the loss of high value goods whilst in transit. The assured admitted to investigators that he was fronting for individuals who wanted to invest "dirt money" for profit. It is believed that either the goods, which were allegedly purchased with cash, did not exist, or that the removal of the goods was organised by the purchasers to ensure a claim occurred and that they received "clean" money as a claims settlement.

(3) Insurers have discovered instances where premiums have been paid in one currency and requests for claims to be paid in another as a method of laundering money.

(4) During an on-site visit, an insurance supervisor was referred to a professional

indemnity claim that the insurer did not believe was connected with money laundering. The insurer was considering whether to decline the claim on the basis that it had failed to comply with various conditions under the cover. The insurance supervisor reviewed the insurer's papers, which identified one of the bank's clients as being linked to a major fraud and money laundering investigation being carried out by international law enforcement agencies.

(5) After a successful High Court action for fraud, adjusters and lawyers working for an insurer involved in the litigation became aware that the guilty fraudster was linked to other potential crimes, including money laundering.

Q. Assignment of claims

(1) In a similar way, a money launderer may arrange with groups of otherwise legitimate people, perhaps owners of businesses, to assign any legitimate claims on their policies to be paid to the money launderer. The launderer promises to pay these businesses, perhaps in cash, money orders or travelers cheques, a percentage of any claim payments paid to him above and beyond the face value of the claim payment. In this case the money laundering strategy involves no traditional fraud against the insurer. Rather, the launderer has an interest in obtaining funds with a direct source from an insurance company, and is willing to pay others for this privilege. The launderer may even be strict in insisting that the person does not receive any fraudulent claims payments, because the person does not want to invite unwanted attention.

R. Non-life insurance - fraudulent claims

(1) Police in Country A uncovered a case of stolen car trafficking where the perpetrators provoked accidents in Country B to be able to claim the damages. The proceeds were laundered via public works companies. A network consisting of two teams operated in two different regions of Country A. Luxury vehicles were stolen and given false number plates before being taken to Country B. An insurance contract was taken out in the first country on these vehicles. In Country B, the vehicles were deliberately written off and junk vehicles with false number plates were bought using false identity documents to be able to claim the damages from the insurance firms in Country A. Around a hundred luxury stolen vehicles were used in this scheme to claim the damages resulting from the simulated or intentional accidents that were then fraudulently declared to the insurance firms. The total loss was over USD 2.5 million. The country in which the accidents occurred was chosen because its national legislation provided for prompt payment of damages.

(2) On receipt of the damages, the false claimant gave 50% of the sum in cash to the leader of the gang who invested these sums in Country B. The investigations uncovered bank transfers amounting to over USD 12,500 per month from the leader's accounts to the country in question. The money was invested in the purchase of numerous public works vehicles and in setting up companies in this sector in Country B. Investigations also revealed that the leader of the gang had a warehouse in which luxury vehicles used for his trafficking operation were stored. It was also established that there was a business relationship between the leader and a local property developer, suggesting that the network sought to place part of its

gains into real estate.

(3) An individual purchases an expensive car. The individual obtains a loan to pay for the vehicle. At the time of purchase, the buyer also enters into a medical insurance policy that will cover the loan payments if he were to suffer a medical disability that would prevent repayment. A month or two later, the individual is purportedly involved in an “accident” with the vehicle, and an injury (as included in the insurance policy) is reported. A doctor, working in collusion with the individual, confirms injury. The insurance company then honours the claim on the policy by paying off the loan on the vehicle. Thereafter, the organisation running the operation sells the motor vehicle and pockets the profit from its sale. In one instance, an insurance company suffered losses in excess of $2 million from similar fraud schemes carried out by terrorist groups.