GUIDELINES FOR **INTERNET GAMING COMPANIES** FOR PREPARATION AND SUBMISSION OF SUSPICIOUS ACTIVITY REPORTS ON FORM 1A or 1A-e

These guidelines are provided to assist internet gaming companies in using FORM 1A revised 17 August, 2009 to prepare Suspicious Activity Reports (SAR). They supercede any prior guidelines.

CONTENTS

1. Notes

Safe Harbour: Section 13(4) of the Money Laundering (Prevention) Act 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 Money Laundering (Prevention) Act 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(1) of the Money Laundering (Prevention) Act 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.

Also, section 7(2) prohibits any person who knows or suspects that a financial institution (a gaming company) has submitted or is about to submit a suspicious activity report to the Supervisory Authority to divulge that fact or other related information to another person.

2. When to File a Report

1. Businesses engaged in internet gambling activities are required by the Internet Gaming Internet Wagering Guidelines to report fraudulent or suspicious activity which may involve money laundering or an activity similar to money laundering.
2. Also, businesses engaged in internet gambling activities are subject to the requirements of the Money Laundering (Prevention) Act and are required to promptly make a suspicious transaction report to the Supervisory Authority in relation to:
    a. Transactions that could constitute or could be related to money laundering
    b. Suspicious transactions characterized as:
        (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) Relating to persons, including businesses and other financial institutions, from countries that have not adopted a comprehensive anti-money laundering programme.
    c. Any transaction conducted or attempted by, at or through the gaming company and its facilities when the gaming company 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 (gaming company) knows of no

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

d. Computer intrusion. For purposes of this report, "computer intrusion" is defined as gaining access to a computer system of an internet gaming company to:
   (i) Remove, steal, procure, or otherwise affect funds of the institution or the institution's customers;
   (ii) Remove, steal, procure, or otherwise affect critical information of the institution including customer account information; or
   (iii) Damage, disable, or otherwise affect critical systems of the institution.
   (iv) Conduct a *denial of service* attack.

3. **NOTE CAREFULLY:** Suspicious Activity Reports are required to be made in relation to: (a) customers of the company (players, account holders) (b) any employee of the company, which includes a director, manager, secretary, staff, authorized representative, etc.) or (c) other person who is suspected of being in possession of the proceeds of crime[1], conducting transactions with the proceeds of crime[2] or engaging in money laundering through the gaming company and its facilities.

4. File within 24 hours or as soon as practicable (but no later than 30 calendar days) after the date of initial detection of facts that constitute a basis for making the report. The report must not be held back for batch filing with other unrelated reports. In situations involving suspicious transactions requiring immediate attention, such as ongoing money laundering schemes, a financial institution should immediately notify by telephone the Supervisory Authority. When the STR form is finally lodged with the Supervisory Authority, details of the telephone notification to the Supervisory Authority should be mentioned as part of the STR.

3. Guidelines for Preparing a Suspicious Activity/Transaction Report

A. Abbreviations and Definitions

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

---

[1] This comes within the definition of money laundering.

[2] This comes within the definition of money laundering.

B. How to Submit a Report

1. Send each completed suspicious activity report to:

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

   Fax: (268) 460-8818

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 records for your files for six (6) years from the date of the suspicious activity report.
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. If using the online form 1A-e use format DD/MMM/YYYY.
7. Enter all **telephone numbers** with (country and area code) first and then the remaining numbers.
8. Addresses, should be in the format indicated by the form unless there are reason why it should be formatted differently.

C. Instructions for Filling In the Suspicious Activity Report Form

Item 1 — Correct a 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, and provide a date and subject reference to the previous report.

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 has 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 surname in Item 4(a), first name in Item 4(b), then middle name or initial in Item 4(c). If the suspicious activity involves an organization, enter its name in Item 4(a).
If the reporting institution has knowledge of the subject using an alias or alternate name, enter the full alias in Item 4(d).
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).
For example, 4(a) Surname: Smith, First name: John, Middle name: Charles, (b) alias (if any) John C. Smythe, (c) trading as: Smithies' Car Parts;

For an organization 4(a) Surname (or name of entity): John C. Smith Ltd., (c) trading as: 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 4; if there is no street address then a description of the area or district should be used; a Post Office Box should only be used if there is no street address. Enter the city in Item 5(a), the 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). Enter the full name of the country in which the address is located in Item 5(e).

Item 6 — Date of birth: If an individual is named in Item 4, enter his or her date of birth by using the format for entering dates described at the beginning of these Guidelines, [DD/MM/YYYY] or on the online form 1A-e [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 who is a subject of the report. For example, medical student, secretary of a law firm, fisherman, carpenter, attorney, housewife, restaurant owner, liquor store clerk, disc jockey, director of computer software company, etc. Avoid using non-specific terms such as merchant, self-employed, director, manager, businessman, etc. Similarly, if an organization is a subject of the report, fully identify the nature of the business of the organization.

Item 9 —Forms of Customer Identity Verification: In item 9(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 details such as driver's licence or passport number. In item 9(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 9(b) there could be entered (i) Government of the United States; (ii) State of Florida.

For Item 9(a)(vi), "other", provide a brief explanation in the space provided. If more space is required, enter the information in Part D.

Online form: For box headed "Form of identity verification:: Use the drop down list to choose the type of identification document. For box headed "No.": Enter the number of the identification document. For box headed "Authority that issued document": Enter the country or authority that issued the document.

Item 10 — Player account number: Where a player is the subject of the report enter the player's account number.

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(j) is checked, provide a brief explanation in the space provided. If more space is required, enter the information in the description in Part D.

Item 12 — Is the subject working with or for the reporting 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 as appropriate.

Item 13 — Date of suspension, termination or resignation: Enter the date the subject of the report was suspended, terminated or resigned using the format described at the beginning of the Guidelines. [DD/MM/YYYY] or on the online form 1A-e [DD/MMM/YYYY].

Part B – DETAILS OF THE TRANSACTION OR ACTIVITY

Item 14 — Date or date range of suspicious transactions or activity: Enter the first known date on which suspicious activity occurred and the last known date on which suspicious activity occurred using the format described at the beginning of these Guidelines. If only one date applies, include this date in the From field. 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/MM/YYYY] or on the online form 1A-e [DD/MMM/YYYY]..

Item 15 — 15a Type of gaming/wagering activity: If the suspicious transaction involved actual gaming or wagering activity, then enter a brief description of the type of gaming activity, such as the name of the game or sports event on which a wager was made, eg. Super Bowl of 2010, World Cup finals of June 2010, opening game of World Cup on June 2010, 1st test match West Indies v. England July 2010, winner of Australian Open Tennis Tournament 2010, Speed Demon to win the triple crown in 2010, parlay –

Los Angeles Lakers to win 1st, 3rd and 5th games of the NBA finals 2010, China to win the most gold medals in the Olympics of 2012 etc.

15b Type of transaction involved: Enter the type of financial transaction linked to the gaming activity entered in 15a above, eg. wager made by player, payment by company on winning wager, etc. If the transaction is not linked to gaming activity, a player is topping up his account or making a first deposit to his player account, then indicate this appropriately eg. deposit to player account, top up of player account.

Item 16 — URL of website involved (if any) Enter the address of the website used in the gaming activity, such as to make a wager, eg. internetgamer.com; or to conduct an illegal non-gaming activity; or which is subjected to unlawful activity aimed at disrupting ordinary online business commerce.

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 — Currency and the amount involved in transaction(s): Enter in caps the standardized three-letter code for the currency in which the transaction was carried out and then enter the amount of money 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; (Euros)—EUR44,782.34 to EUR44,783.00.

Online form 1A-e: In the currency box enter the three-letter code for the currency in which the transaction was carried out except for USD which is already entered. In the amount box enter accurately the amount involved. In the box headed conversion rate to USD enter the conversion rate of the currency to USD. Conversion rates can be checked at www.xe.com/ucc.

Item 18 — Total value of transaction(s) in U.S. Dollars: All amounts of money entered in item 17 which are not in U.S. dollars should be converted to U.S. then all amounts totaled and entered into item 18. Enter only the amount of dollars. If there are cents do not enter that. A fully accurate figure of the amount involved should be entered in the description in Part D.

Online form 1A-e: Do not enter anything into this box. The online form if working properly should automatically calculate the appropriate figure. Please note that the calculation may round up or round down the figure that represents the amounts entered in item 17. It is not intended to be precisely but only generally accurate. However, if the form does not appear to be working properly you should calculate and enter the correct figure.

Item 19 — Type and quantity of instrument involved: List the type of monetary instrument(s) involved and the amount of money represented by each instrument in the transaction, eg. (1) Type:Cash; Amount: USD$10,000; (2) Type: Traveler's cheques: Amount: £5,000 sterling; (3) Type: Wire transfers; Amount: €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 they should be listed as eg. (1) Two traveler's cheques — USD$1,000 and €5,000. Where extra space would be needed to enter the information then the break-down of the total may then be listed in Part D.

Item 20 – Transaction number(s): Enter the transaction numbers for the transactions being reported. If a large number of transactions are involved then if consecutive enter a number range eg. 12345 to 12300; if non-consecutive then list them in the explanation in Part D or attach a transaction number list in response to Item 26.

Item 21 — 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 the explanation in Part D.

Item 22 — If account(s) were closed date(s) 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 23 — Category of suspicious activity: Check all box(es) which help to identify the general nature of the suspicious activities being reported. A brief description of the categories can be found at the end of these notes (before the Typologies) in the list titled "Explanation of Summary Categories of Suspicious Activity". If "other" is checked, enter a brief explanation of the activity in the space provided. In addition to completing this item, a full description of the activity/transaction should be made in Part D — Description and Explanation of Suspicious Transaction/Activity (Part D is a mandatory field).

If box (q) is checked, then enter in the space provided the number of a typology listed at the end of these instructions, which is considered similar to the activity being reported. For example, where the suspicious activity being reported resembles a player being paid on a losing bet, then box (q) should be checked, and the line should read: "(q) The suspicious activity resembles typology No. A(1)".

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 24 — Character of financial transaction(s): Check the box(es) which best describes how funds in suspicious transactions were being dealt with or best identifies the manner in which the financial transaction(s) were taking place.

Part D – DESCRIPTION AND EXPLANATION OF SUSPICIOUS TRANSACTION/ACTIVITY

Item 25 — Give the reasons why you consider the transaction(s) or activity reported in Part B and C to be suspicious: State the reasons why you consider the transaction(s) reported in Part B to be suspicious and the reasons you consider that the reported activity is the same as or similar to that indicated in Part C: 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 transaction(s). The narrative should include an explanation of the activity indicated in Part C (the selected bullet points from a to r). It should also include any other information that you think is necessary to better enable analysts to understand the transaction being reported and put it in perspective. If necessary, continue the narrative on a separate sheet of paper headed "Part D (continued)". Remember that the originals of any supporting documentation provided must be retained at the reporting financial institution.

Item 26 — Is additional information attached to this report: Check the appropriate box to indicate whether additional information is attached to the report. If "Yes" is checked, state what documents or materials accompany the report.

Part E – DETAILS OF REPORTING COMPANY

Item 27 — (a) Name of Licence Holder (company filing report): Enter the full legal name of the reporting financial institution.

(b) Trade name of company (where relevant): Enter (where relevant) the name under which the company was trading or conducting business as a gaming entity in respect of which the suspicious activity arose if different from Item 27(a). The trade name would be relevant once an online gaming transaction was part of the suspicious activity being reported.

Eg. 27(a) Altec Gaming Inc.; (b) Casino Royale Online.

Item 28 — Address of Licence Holder: In the appropriate blanks enter the (building number and name where appropriate), street address of the reporting institution shown in Item 27. A Post Office Box number by itself is not sufficient; a street address should be given. 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 — Address of office issuing the report: In the appropriate spaces enter the (building number and name where appropriate), street address of the reporting institution shown in Item 27. A Post Office Box number by itself is not sufficient; a street address should be given. 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 30 — Physical address of office/facility from which the transaction or activity was processed or detected (if different from 29 above): If the location where the suspicious transaction or activity took place is different from that provided in Item 28 above enter the following details (otherwise, leave Item 30 blank): in the appropriate spaces the (building number and name where appropriate), the street address of the branch or office where the activity occurred. A Post Office Box number by itself is not sufficient; a street address should be given. 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 in which the address entered for the branch is located.

Item 31 — Details of Money Laundering Compliance Officer or authorized person submitting the report: 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 ordinarily 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 THE LICENCE HOLDER

Item 32 — 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 format described at the beginning of these Guidelines, [DD/MM/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	Structuring involves the carrying out of multiple transactions of small amounts that aggregate to a significant sum of money: 1. To avoid threshold reporting requirements under Regulations ; 2. To avoid customer identity verification requirements under Regulations and Guidelines. 3. To avoid suspicious activity detection and conventional monitoring thresholds and filters. 4. To avoid enhanced scrutiny or additional review frequently triggered by higher transaction amounts and thresholds.
b	Layering	Layering involves multiple transactions which could be conducted across multiple accounts and/or multiple countries in order: 1. To obscure the paper trail and make it more difficult to trace the source of the funds; 2. To avoid attention that large single transactions might attract; 3. To avoid suspicious activity detection and conventional monitoring thresholds and filters. 4. To avoid enhanced scrutiny or additional review frequently triggered by higher transaction amounts and thresholds. 5. to avoid generating a suspicious activity report. For example, sending money using three transactions when one would ordinarily be sufficient. Or sending money through two or more jurisdictions instead of sending it directly to its intended destination.
c	Money laundering	In money laundering: 1. The transaction may involve funds or other property derived from criminal activity or funds used to conduct criminal activity. 2. The transaction may be conducted to receive, transfer or dispose of funds or assets derived from or used in criminal activity. 3. The transaction may be 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 may be flagged by the fact that it 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.
d	Cheque fraud	Use of counterfeit or altered cheques, withdrawal of funds against cheques with forged signatures or endorsements.
e	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.)
f	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.
g	Counterfeit instrument	Manufacture, copy or reproduction or forgery of an instrument with intent to defraud a financial institution.
H	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.
I	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.
J	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;
k	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.
l	Identity theft	Use without authorization of the means of identification of another.
m	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 sometime be indicated by 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 a non-transparent manner or manner inconsistent with the objects of the company. An example of this is a ponzi or pyramid scheme.
n	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.
o	Refusal/failure to complete CDD requirement	Refusal or failure by a customer to provide the identification and verification information required with no satisfactory explanation.
p	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.
q	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.
r	Wire transfer fraud	The transmission of electronic funds with the intent to obtain money or property by fraudulent means or false pretenses.

List of Currency Codes

Country	Currency	Code
Afghanistan	Afghani	**AFN**
Albania	Lek	**ALL**
Algeria	Dinar	**DZD**
America (U.S.)	Dollar	**USD**
Angola	Kwanza	**AOA**
Argentina	Peso	**ARS**
Armenia	Dram	**AMD**
Aruba	Guilder	**AWG**
Australia	Dollar	**AUD**
Azerbaijan	New Manat	**AZN**
Bahamas	Dollar	**BSD**
Bahrain	Dinar	**BHD**
Bangladesh	Taka	**BDT**
Barbados	Dollar	**BBD**
Belarus	Ruble	**BYR**
Belize	Dollar	**BZD**
Bermuda	Dollar	**BMD**
Bolivia	Boliviano	**BOB**
Bosnia and Herzegovina	Convertible Marka	**BAM**
Botswana	Pula	**BWP**
Brazil	Real	**BRL**
Brunei	Dollar	**BND**
Bulgaria	Lev	**BGN**
Burma (See: Myanmar)		
Burundi	Franc	**BIF**
Cambodia	Riel	**KHR**
Canada	Dollar	**CAD**
Cape Verde	Escudo	**CVE**
Cayman Islands	Dollar	**KYD**
Chile	Peso	**CLP**
China	Yuan Renminbi	**CNY**
Colombia	Peso	**COP**
Communaute Financiere Africaine	BEAC Franc	**XAF**
Communaute Financiere Africaine	BCEAO Franc	**XOF**
Comoros	Franc	**KMF**
Comptoirs Français du Pacifique	Franc	**XPF**
Congo	Franc	**CDF**
Costa Rica	Colon	**CRC**
Croatia	Kuna	**HRK**
Cuba	Peso	**CUP**
Check Republic	Koruna	**CZK**
Denmark	Krone	**DKK**
Djibouti	Franc	**DJF**

Country	Currency	Code
Dominican Republic	Peso	**DOP**
Eastern Caribbean	Dollar	**XCD**
Egypt	Pound	**EGP**
El Salvador	Colon	**SVC**
England (See: United Kingdom)		
Eritrea	Nakfa	**ERN**
Estonia	Kroon	**EEK**
Ethiopia	Birr	**ETB**
	Euro	**EUR**
Falkland Islands	Pound	**FKP**
Fiji	Dollar	**FJD**
Gambia	Dalasi	**GMD**
Georgia	Lari	**GEL**
Ghana	Cedi	**GHS**
Gibraltar	Pound	**GIP**
Guatemala	Quetzal	**GTQ**
Guernsey	Pound	**GGP**
Guinea	Franc	**GNF**
Guyana	Dollar	**GYD**
Haiti	Gourde	**HTG**
Honduras	Lempira	**HNL**
Hong Kong	Dollar	**HKD**
Hungary	Forint	**HUF**
Iceland	Krona	**ISK**
India	Rupee	**INR**
Indonesia	Rupiah	**IDR**
Iran	Rial	**IRR**
Iraq	Dinar	**IQR**
Isle of Man	Pound	**IMP**
Israel	Shekel	**ILS**
Jamaica	Dollar	**JMD**
Japan	Yen	**JPY**
Jersey	Pound	**JEP**
Jordan	Dinar	**JOD**
Kazakhstan	Tenge	**KZT**
Kenya	Shilling	**KWA**
Kuwait	Dinar	**KWD**
Kyrgyzstan	Som	**KGS**
Laos	Kip	**LAK**
Latvia	Lat	**LVL**
Lebanon	Pound	**LBP**
Lesotho	Loti	**LSL**
Liberia	Dollar	**LRD**
Libya	Dinar	**LYD**

Country	Currency	Code
Lithuania	Litas	**LTL**
Macau	Pataca	**MOP**
Macedonia	Denar	**MKD**
Madagascar	Aiary	**MGA**
Malawi	Kwacha	**MWK**
Malaysia	Ringgit	**MYR**
Maldives	Rufiyaa	**MVR**
Mauritania	Ouguiya	**MRO**
Mauritius	Rupee	**MUR**
Mexico	Peso	**MXN**
Moldova	Leu	**MDL**
Mongolia	Tughrik	**MNT**
Morocco	Dirham	**MAD**
Mozambique	Metical	**MZN**
Myanmar	Kyat	**MMK**
Namibia	Dollar	**NAD**
Nepal	Rupee	**NPR**
Netherlands Antilles	Guilder	**ANG**
New Zealand	Dollar	**NZD**
Nicaragua	Cordoba	**NIO**
Nigeria	Naira	**NGN**
North Korea	Won	**KPW**
Norway	Krone	**NOK**
Oman	Rial	**OMR**
Pakistan	Rupee	**PKR**
Panama	Balboa	**PAB**
Papua New Guinea	Kina	**PGK**
Paraguay	Guarani	**PYG**
Peru	Nuevo Sol	**PEN**
Philippines	Peso	**PHP**
Poland	Zloty	**PLN**
Qatar	Riyal	**QAR**
Romania	New Leu	**RON**
Russia	Ruble	**Rub**
Rwanda	Franc	**RWF**
Saint Helena	Pound	**SHP**
Samoa	Tala	**WST**
Sâo Tome and Principe	Dobra	**STD**
Saudi Arabia	Riyal	**SAR**
Seborga	Luigino	**SPL**
Serbia	Dinar	**RSD**
Seychelles	Rupee	**SCR**
Sierra Leone	Leone	**SLL**
Singapore	Dollar	**SGD**

Country	Currency	Code
Slovakia	Koruna	**SKK**
Solomon Islands	Dollar	**SBD**
Somalia	Shilling	**SOS**
South Africa	Rand	**ZAR**
South Korea	Won	**KRW**
Sri Lanka	Rupee	**LKR**
Sudan	Pound	**SDG**
Surinam	Dollar	**SRD**
Swaziland	Lilangeni	**SZL**
Sweden	Krona	**SEK**
Switzerland	Franc	**CHF**
Syria	Pound	**SYP**
Taiwan	New Dollar	**TWD**
Tajikistan	Somoni	**TJS**
Tanzania	Shilling	**TZS**
Thailand	Baht	**THB**
Tonga	Pa'anga	**TOP**
Trinidad and Tobago	Dollar	**TTD**
Tunisia	Dinar	**TND**
Turkey	New Lira	**TRY**
Turkmenistan	Manat	**TMM**
Tuvalu	Dollar	**TVD**
Uganda	Shilling	**UGX**
Ukraine	Hryvna	**UAH**
United Arab Emirates	Dirham	**AED**
United Kingdom	Pound	**GBP**
United States	Dollar	**USD**
Uruguay	Peso	**UYU**
Uzbekistan	Som	**UZS**
Vanuatu	Vatu	**VUV**
Venezuela	Bolivar Fuente	**VEF**
Vietnam	Dong	**VND**
Yemen	Rial	**YER**
Zambia	Kwacha	**ZMK**
Zimbabwe	Dollar	**ZWD**

6. TYPOLOGIES — EXAMPLES OF POTENTIALLY SUSPICIOUS TRANSACTIONS

DEPOSIT TAKING INSTITUTIONS

A. Money laundering using Casinos and Internet Gaming Businesses

(1) Customer is paid on a losing bet.

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

(3) Customers who deposit significant sums into their player accounts and then withdraw the money without having engaged in much or any gaming activity.

(4) Customers who purchase a significant quantity of gaming tokens and then cash them in (for a casino cheque) without having engaged in much or any gaming activity.

(5) Employee of a company accesses gaming machines without proper authorization.

(6) Employee of a company accesses critical company computers without authorization, unnecessarily or without a valid reason.

(7) Employee of a company accesses gaming machines using inappropriate or unauthorized procedures or protocols.

(8) Director, owner or employee of a company issues instructions to recalibrate, reset or alter a gaming machine or critical computer without a transparent reason.

(9) Director, owner or employee of a company issues instructions to recalibrate, reset or alter a gaming machine or critical computer requiring that inappropriate procedures or protocols be used.

General indicators of potential money laundering

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

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

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

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

(14) Even dollar amount transactions.

(15) Transactions structured to lose the paper trail.

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

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

(18) Transactions by non-account holders.

B. Money Laundering Using 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. Money Laundering Using Bank 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. Money Laundering by International offshore international activity

(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. Money Laundering Involving Financial 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. Money Laundering by 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.