MONEY LAUNDERING &
THE FINANCING OF TERRORISM

GUIDELINES FOR FINANCIAL INSTITUTIONS

Update

[ISSUED 21 March 2012]

Director of the ONDCP and
The Supervisory Authority under the
Money Laundering (Prevention) Act 1996
O.N.D.C.P. Headquarters
Camp Blizard
Antigua, West Indies
Telephone: 562-3255, (268) 462-5934
Fax: (268) 460-8818
email: ondcp@candw.ag

INTRODUCTION

These guidelines are issued pursuant to the powers of the Supervisory Authority under sections 11(vii) and 11(xiii) of the Money Laundering (Prevention) Act 1996 as amended, and the Director of ONDCP under section 43 of the Prevention of Terrorism Act 2005 as amended.

The Money Laundering and Financing of Terrorism Guidelines (MLFTG) are amended by reformating and in certain parts restating the contents of the Appendicies to the MLFTG and reissuing them as attached hereto immediately following the page headed "Updater Pages" of this Update. They supercede previous guidance wherever there may be a conflict.

These guidelines expand and consolidate the Appendicies of the Guidelines and introduce typology guidance to financial institutions in relation to Non-Profit Organizations. This guidance is incomplete on its own and should be read together with Parts I and II of the MLFTG on money laundering and on the financing of terrorism and the updates thereto.

21 March 2012

Lt. Col. Edward Croft
Director of ONDCP and
Supervisory Authority under the
Money Laundering (Prevention) Act 1996

UPDATER PAGES

APPENDIX A — Typologies and Red Flags

TYPES OF POTENTIALLY SUSPICIOUS ACTIVITIES AND TRANSACTIONS

1. **Money Laundering using cash transactions**

   (a) unusually larger cash deposits made by an individual or company whose ostensible business activities would normally be generated by cheques and other instruments;

   (b) 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;

   (c) customers who deposit 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;

   (d) 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.);

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

   (f) customers who seek to exchange large quantities of low denomination notes for those of higher denomination;

   (g) frequent exchange of cash into other currencies;

   (h) branches that have a great deal more cash transactions than usual (Head Office statistics detect aberrations in cash transactions);

   (i) customers whose deposits contain counterfeit notes or forged instruments;

   (j) customers transferring large sums of money to or from overseas locations with instruments for payment in cash; and

   (k) large cash deposits using night safe facilities, thereby avoiding direct contact with bank staff.

2. **Money Laundering using bank accounts**

   (a) 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 nominees;

   (b) customers who have numerous ac-

Appendix A

counts and pay in amounts of cash to each of them in circumstances in which the total of credits would be a large amount;

(c) 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);

(d) reluctance to provide normal information when opening an account, providing minimal or fictitious information or, when applying to open an account, providing information that is difficult or expensive for the institution to verify;

(e) customers who appear to have accounts with several institutions within the same locality, especially when the bank is aware of a regular consolidation process from such accounts prior to a request for onward transmission of the funds;

(f) matching of payments out with credits paid in cash on the same or previous day;

(g) paying in large third party cheques endorsed in favour of the customer;

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

(i) customers who together, and simultaneously, use separate tellers to conduct large cash transactions or foreign exchange transactions;

(j) greater use of safe deposit facilities and increased activity by individuals; the use of sealed packets deposited and withdrawn;

(k) companies' representatives avoiding contact with the branch;

(l) 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;

(m) 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;

(n) insufficient use of normal banking facilities (e.g. avoidance of high interest rate facilities for large balances); and

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

(p) customers who request that account statements and other correspondence be kept at the financial institution for collection or from whom correspondence is returned "note known at this address" etc.

3. Money Laundering using investment related transactions

(a) purchasing of securities to be held by the institution in safe custody, where this does not appear appropriate given the customer's apparent standing;

(b) request by customers for investment management or administration services (either foreign currency or securities) where the source of the funds is unclear or not consistent with the customer's apparent standing;

(c) large or unusual settlements of securities in cash form; and

Appendix A

(d) buying and selling of a security with no discernible purpose or in circumstances which appear unusual.

4. Money Laundering by offshore international activity

(a) customer introduced by an overseas branch, affiliate or other bank based in countries where production of drugs or drug trafficking may be prevalent;

(b) use of letters 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;

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

(d) unexplained electronic fund transfers by customers, foreign currency drafts or other negotiable instruments to be issued:

(e) frequent requests for travelers cheques or foreign currency drafts or other negotiable instruments to be issued; and

(f) frequent paying in of travelers cheques or foreign currency drafts particularly if originating from overseas.

5. Money Laundering involving financial institution employees and agents

(a) changes in employee characteristics, (e.g. lavish lifestyles or avoiding taking holidays);

(b) changes in employee or agent performance, (e.g. the salesman selling products for cash has remarkable or unexpected increase in performance); and

(c) 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.

6. Money Laundering by secured and unsecured lending

(a) customers who repay problem loans unexpectedly;

(b) request to borrow against assets held by the institution or a third party, where the origin of the assets in not known or the assets are inconsistent with the customer's standing; and

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

(d) customers who unexpectedly repay in part or full a mortgage or other loan in a way inconsistent with their earning capacity or asset base.

7. Sales and dealing staff

A. New Business

Although long-standing customers may be laundering money through an investment business it is more likely to be a new customer who may use one or more accounts for a short period only and may use false names and fictitious companies.

Investment may be direct with a local institution or indirect via an intermediary who "doesn't ask too many awkward questions", especially (but not only) in a jurisdiction where money laundering is not legislated against or where the rules are not rigorously enforced.

The following situations will usually give rise to the need for additional enquiries:

(i) a personal client for whom verification of identity proves unusually difficult and who is reluctant to provide

Appendix A

details;

(ii) a corporate/trust client where there are difficulties and delays in obtaining copies of the accounts or other documents of incorporation:

(iii) a client with no discernible reason for using the firm's service, e.g. clients with distant addresses who could find the same services nearer their home base; clients whose requirements are not in the normal pattern of the firm's business which could be more easily serviced elsewhere; and

(iv) any transaction in which the counterparty to the transaction is unknown

B. Intermediaries

There are many clearly legitimate reasons for a client's use of an intermediary. However, the use of intermediaries does introduce further parties into the transaction thus increasing opacity and, depending on the designation of the account, preserving anonymity. Likewise there are a number of legitimate reasons for dealing via intermediaries on a "numbered account" basis; however, this is also a useful tactic which may be used by the money launderer to delay, obscure or avoid detection.

Any apparently unnecessary use of an intermediary in the transaction should give rise to further enquiry.

C. Dealing patterns & Abnormal transactions

The aim of the money launderer is to introduce as many layers as possible. This means that the money will pass through a number of sources and through a number of different persons or entities. Long-standing and apparently legitimate customer accounts may be used to launder money innocently, as a favour, or due to the exercise of undue pressure.

Examples of unusual dealing patterns and abnormal transactions may be as follows:

1. Dealing patterns

(i) A large number of security transactions across a number of jurisdictions;

(ii) Transactions not in keeping with the investor's normal activity, the financial markets in which the investor is active and the business which the investor operates;

(iii) Buying and selling of a security with no discernible purpose or in circumstances which appear unusual, e.g. churning at the client's request;

(iv) Low grade securities purchased in an overseas jurisdiction, sold locally and high grade securities purchased with the proceeds; and

(v) Bearer securities held outside a recognized custodial system.

2. Abnormal transactions

(i) a number of transactions by the same counter-party in small amounts of the same security, each purchased for cash and then sold in one transaction, the proceeds being credited to an account different from the original account;

(ii) any transaction in which the nature, size or frequency appears unusual, e.g. early termination of packaged-products at a loss due to front end loading; early cancellation, especially where cash had been tendered or the refund cheque is to a third party;

(iii) transfer of investments to apparently unrelated third parties;

(iv) transactions not in keeping with normal practice in the market to which they relate, e.g. with reference to market size and frequency, or at off-market prices; and

(v) other transactions linked to the transaction in question which could

Appendix A

be designed to disguise money and divert it into other forms or to other destinations or beneficiaries.

8. Settlements

A. Payment

Money launderers will often have substantial amounts of cash to dispose of and will use a variety of sources. Cash settlement through an independent financial adviser or broker may not in itself be suspicious; however, large or unusual settlements of securities deals in cash and settlements in cash to a large securities house will usually provide cause for further enquiry. Examples of unusual payment settlement may be as follows:

(i) a number of transactions by the same counter-party in small amounts of the same security, each purchased for cash and then sold in one transaction;

(ii) large transaction settlement by cash; and

(iii) payment by way of cheque or money order transfer where there is a variation between the account holder/signatory and the customer.

B. Registration and delivery

Settlement by registration of securities in the name of an unverified third party should always prompt further enquiry.

Bearer securities, held outside a recognized custodial system, are extremely portable and anonymous instruments which may serve the purpose of the money launderer well. Their presentation in settlement or as collateral should therefore always prompt further enquiry as should the following:

(i) settlement to be made by way of bearer securities from outside a recognized clearing system; and

(ii) allotment letters for new issues in the name of persons other than the client.

C. Disposition

As previously stated, the aim of money launderers is to take “dirty” cash and turn it into “clean” spendable money or to pay for further shipments of drugs, etc. Many of those at the root of the underlying crime will be seeking to remove the money from the jurisdiction in which the cash has been received, with a view to its being received by those criminal elements for whom it is ultimately destined in a manner which cannot easily be traced.

The following situations should therefore give rise to further enquiries:

(i) payment to a third party without any apparent connection with the investor;

(ii) settlement either by registration or delivery of securities to be made to an unverified third party; and

(iii) abnormal settlement instructions, including payment to apparently unconnected parties.

9. Company Formation and Management

A. Suspicious circumstances relating to the customer’s behaviour:

(i) the purchase of companies which have no obvious commercial purpose;

(ii) sales invoice totals exceeding known value of goods;

(iii) customers who appear uninterested in legitimate tax avoidance schemes;

(iv) the customer pays over the odds or sells at an undervaluation;

(v) the customer makes unusually large cash payments in relation to business activities which would normally be paid by cheques, banker’s drafts

Appendix A

etc;

(vi) customers transferring large sums of money to or from overseas locations with instructions for payment in cash;

(vii) customers who have numerous bank accounts and pay amounts of cash into all those accounts which, if taken in total, amount to a large overall sum; and

(viii) paying into bank accounts large third party cheques endorsed in favour of the customers.

B. Potentially suspicious secrecy might involve:

(i) excessive or unnecessary use of nominees;

(ii) unnecessary granting of power of attorney;

(iii) performing "execution only" transactions;

(iv) using a client account rather than paying for things directly;

(v) use of mailing address;

(vi) unwillingness to disclose the source of funds; and

(vii) unwillingness to disclose identity of ultimate beneficial owners.

C. Suspicious circumstances in groups of companies:

(i) subsidiaries which have no apparent purpose;

(ii) companies which continuously make substantial losses;

(iii) complex group structures without cause;

(iv) uneconomic group structures for tax purposes;

(v) frequent changes in shareholders and directors;

(vi) unexplained transfers of significant sums through several bank accounts; and

(vii) use of bank accounts in several currencies without reason.

10. Casinos and internet gaming business

(a) customer who request that payouts be sent to third parties, particularly, in jursidictions other than their juridiction of domicile;

(b) customers who deposit significant sums into their player accounts and then withdraw the money without having undertaken much gaming activity;

(c) customers who engage in structuring;

(d) where a customer is paid on a losing wager.

Notes:

1. None of the above factors on their own necessarily mean that a customer or other person is involved in money laundering or terrorist financing. However, it may be that a combination of some of these factors could raise suspicions.

2. What does or does not give rise to a suspicion will depend on the particular circumstances.

Developing an Early-Warning System for Suspicious NPOs[1]

Identifying red flags

Financial institutions are required by section 34(4) of the Prevention of Terrorism Act 2005 to report suspicious transactions relating to the financing of terrorism[2]. Terrorism financing tends to manifest itself either as money laundering or in other more subtle financial activities. This needs to be kept in mind when monitoring the accounts and transactions

Appendix A

of Non-Profit Organizations (NPOs)[3], which are legal entities or organizations that primarily engage in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of "good works". It is therefore important for financial institutions dealing with NPO customers to be able to spot red flags or indicators that suggest the possibility or potential for transactions to be terrorism related.

Red flags are particular behaviours and atypical situations that present themselves in transactions of customers and users of financial institutions that could be linked to illegal activities.

Red flags related to Non-Profit Organizations and their activities include the following:

(1) NPOs whose corporate purpose do not pertain to the place in which they carry out their activities;

(2) NPOs that despite being tax exempt do not take advantage of that benefit;

(3) The transfer of money between local and foreign NPOs that because of the quantity, destination, or corporate purpose do not fit the characteristics of the NPO from which it came;

(4) NPOs that suddenly show a significant increase in volume or amount of incomes;

(5) NPOs that after remaining financially inactive for some time make transactions for sums significantly higher than usual;

(6) NPOs that keep their financial products funded for very long periods of time;

(7) Financial products under the name of the NPO that present a high volume of cash transactions;

(8) NPOs that despite developing projects for high sums of money do not have either the employees or the capacity to execute those projects;

(9) NPOs that open financial products with hardly verifiable personal and/or commercial references, or whose partners or legal representatives are never in the country;

(10) NPOs which use a name that suggest a relationship with another recognized NPO or is similar to another NPO in order to deceive potential donors or clients;

(11) NPOs that often make changes in their shareholders, legal representatives, and/or administrators;

(12) NPO employees or executives who claim to work for the organization but do not have legal permits to work in that country;

(13) NPOs that are lawfully constituted but manage their financial resources through the personal bank accounts of their executives or employees, thus avoiding opening financial products on behalf of the NPO as such.

The compliance officers of financial institutions should develop a thorough familiarity with these red flags and communicate them during training and ordinary interaction to other members of staff.

Footnotes

[1] Based on OAS recommendations

[2] S.34(4) of the PTA requires a financial institution to report every transaction, attempted transaction or proposed transaction where there are reasonable grounds to suspect the transaction, attempted transaction or proposed transaction is related to terrorism, is conducted on behalf of a terrorist or terrorist organization or on behalf of a financier of terrorism.

[3] Some NPOs are referred to as Friendly Societies.

APPENDIX B — Summary of AML/CFT Laws

Appendix B

APPENDIX C — Financial Institutions under the MLPA

Financial activities subject to the requirements of the Money Laundering (Prevention) Act are set out in the First Schedule to the Act and are as follows:

1. "Banking business" and " financial business" as defined in the Banking Act and the Financial Institutions (Non-Banking) Act;

2. "International offshore Banking business" as defined in the International Business Corporation Act;

3. Venture risk capital;

4. Money transmission services;

5. Issuing and administering means of payments (e.g. credit cards, travellers' cheques and bankers' drafts);

6. Guarantees and commitments;

7. Trading for own account or for account of customers in:—

(a) money market instruments (e.g., cheques, bills, certificates of deposits, commercial paper, etc.);

(b) foreign exchange;

(c) financial and commodity-based derivative instruments (e.g., futures, options, interest rate and foreign exchange instruments etc.);

(d) transferable or negotiable instruments;

8. Money broking;

9. Money lending and pawning;

10. Money exchange (e.g., *casa de cambio*);

11. Real property business;

12. Credit unions;

13. Building societies;

14. Trust business;

15 Insurance business;

16. Dealers in precious metals, art and jewellery;

17. Casionos;

18. Internet gambling

19. Sports betting

20. Car Dealerships;

21. Travel agents;

22. Dealers in high value and luxury goods;

23. Company service providers;

24. Attorneys-at-law (who conduct financial activity as a business);

25. Notaries (who conduct financial activity as a business(;

26. Accountants (who conduct financial activity as a business).

APPENDIX D — Forms

Forms relevant to complaince with the requirements of the MLPA and the PTA are the following:

REPORTING FORMS

Form 1 — Suspicious Activity Report

Form 1A — Suspicious Activity Report (Gaming)

Form 1C — Significant Payment Report (Gaming)

Form 3 — Terrorist Property Report

NOTICE FORMS

Appendix D

FORM 1

Suspicious Activity Report

COMPLETE ENTIRE REPORT
(see Instructions)

*Please complete this form in **black ink** and print in **CAPITAL LETTERS***
Mark appropriate answer boxes with a check (√)

Instructions on how to prepare a suspicious activity or transaction report using this form are enclosed with the form or can be obtained from the ONDCP.

CONFIDENTIAL

This Report is a confidential document and must be treated as such.

Complete ALL items on this form, as soon as possible AFTER the transaction or attempted transaction or activity that is the subject of this report. Items that are not applicable should be left blank.

Reporting of suspicious transactions by financial institutions is required by law under Section 13 of the Money Laundering (Prevention) Act 1996 as amended ("MLPA") and regulation 6(1) of the Money Laundering (Prevention) Regulations 2007. A list of all financial institutions required to file suspicious transaction reports ("STR") is found in the First Schedule to the MLPA.

Tipping off: Financial institutions (including employees, staff, directors, owners or other authorized representatives) shall not notify any person that this SAR has been filed and information relating thereto furnished to the Supervisory Authority. Criminal offence is committed contrary to section 13(5) of the MLPA for failure to comply with this obligation.

Send the completed form to:
THE SUPERVISORY AUTHORITY
ONDCP Headquarters
P.O. Box W 827, Camp Blizard, Antigua
Tel: (268) 562-3255 **email: supervisoryauthority@ondcp.gov.ag**

Privacy Statement

The provisions of Section 13 of the MLPA and Regulations 6 of the MLPR are designed to help detect money laundering and uncover transactions invovling the proceeds of crime. Information reported to the Supervisory Authority at the ONDCP is kept confidential. However, the Supervisory Authority is legally authorised to share the information with another law enforcement authority where the disclosure is essential to the detection, investigation or prosecution of an offence. Financial institutions, are protected by Section 13(4)of the MLPA from criminal, civil or administrative liability for complying with the legal requirement to file reports of transactions that constitute or could be related to money laundering.

Penalties exist for failure to lodge or supply full and correct information as required.

For assistance please call the Senior Financial Intelligence Officer of the ONDCP at **(268) 562-3255**

Timing of Report

Reporting is required by Section 13(2) of the MLPA to be done promptly. Reports of suspicious transactions or activities must be made as soon as practicable, but no later than 30 days after the suspicious activity/transaction is discovered.
Please note the time when the suspicious transaction/activity occurred, the time when you start to fill out this form and the time when you complete this form. You may be asked about how long it took to prepare and file this report.

A SAR must be in writing. Contact with law enforcement authorities does not eliminate or satisfy the section 13(2) requirement of the MLPA to make an SAR.

1 ☐ *Check the box if this report is made to correct or update a prior report. Where a correction is being filed, the entire form must be completed again and changes indicated in the appropriate item.*

PART A - IDENTITY OF SUBJECT(S) CONDUCTING THE SUSPICIOUS ACTIVITY OR TRANSACTION

2 ☐ Subject information unavailable

3 ☐ Multiple subjects involved

SUBJECT INFORMATION

4 Name of individual or entity

(a) Surname or name of entity: .....

.....

(b) First name:.....

(c) Middle name:.....

(d) alias (if any):.....

(e) trading as:.....

5 Address

(a) Street.....

(b) City:.....

(c) State/province:.....

(d) Postcode:.....

(e) Country:.....

6 Date of birth (dd/mm/yyyy).....

7 Country of registration

.....

8 Occupation/Type of business

.....

9 (a) Telephone number (home):.....
(b) Telephone number (business):.....

10 (a) Forms of identity verification
☐ (i) passport - no. .....
☐ (ii) driver's licence - no. .....
☐ (iii) voter registration card - no. .....
☐ (iv) identity card - no. .....
☐ (v) certificate of incorporation - no. .....
☐ (vi) other:.....
(b) Authority that issued document(s):.....
.....

11 Subject's relationship to the reporting financial institution

☐ (a) Customer	☐ (g) Broker
☐ (b) Accountant	☐ (h) Director
☐ (c) Agent	☐ (i) Employee
☐ (d) Appraiser	☐ (j) Officer
☐ (e) Attorney	☐ (k) Shareholder
☐ (f) Borrower	☐ (l) Other:.....

12 Is the subject working with or for the institution?
☐ (a) Yes
☐ No
Subject is
☐ (b) still employed
☐ (c) suspended
☐ (d) terminated
☐ (e) resigned

13 Date of suspension, termination or resignation: .....

Appendix D

PART B - DETAILS OF THE TRANSACTION OR ACTIVITY

14 Type of financial services involved in suspicious transaction.....

15 Date or date range of suspicious transaction or activity
From..... to .....

16 E.C. Dollar amount of transaction(s)

E	C	D	$			,				,				.	0	0

17 If foreign currency is involved in the transaction(s) specify the currency and the amount

Currency			Amount												
						,				,				.	0	0
						,				,				.	0	0
						,				,				.	0	0
						,				,				.	0	0

18 Type and quantity of instrument(s) involved
(1) .....
(2) .....
(3) .....

19 Transaction number(s).....

20 Accounts affected:

(1) Account number:.....
(2) Account number::.....
(3) Account number::.....
(4) Account number::.....

21 If account closed, date closed

(1) date .....
(2) date .....
(3) date .....
(4) date .....

PART C - SUMMARY CHARACTERIZATION OF SUSPI ACTIVITY

22 Category of Suspicious Activity. Check the box(e which best identify the suspicious activity: (A numb of typologies is attached to the end of the instructio preparing this form.)

- ☐ (a) Structuring (or layering)
- ☐ (b) Money laundering
- ☐ (c) Cheque Fraud
- ☐ (d) Computer Intrusion
- ☐ (e) Counterfeit Cheque
- ☐ (f) Counterfeit Instrument
- ☐ (g) Credit Card Fraud
- ☐ (h) Debit Card Fraud
- ☐ (i) Embezzlement
- ☐ (j) False invoicing
- ☐ (k) Identity Theft
- ☐ (l) Investment Fraud
- ☐ (m) Mysterious Disapperance
- ☐ (n) Refusal/failure to complete CDD requireme
- ☐ (o) Refusal/failure to update CDD information
- ☐ (p) Terrorist Financing
- ☐ (q) Wire Transfer Fraud
- ☐ (r) The suspicious activity resembles typology No. .....
- ☐ (s) Other:.....

23 Character of suspicious activity

- ☐ (a) unusual transaction
- ☐ (b) complex transaction
- ☐ (c) large transaction
- ☐ (d) unusual pattern of transactions with no appa economic purpose
- ☐ (e) insignificant but periodic transactions with n ent economic purpose
- ☐ (f) unusual use of monetary instrument
- ☐ (g) other:.....

Appendix D

PART D - DESCRIPTION AND EXPLANATION OF SUSPICIOUS TRANSACTION /ACTIVITY

24 Give the reasons why you consider the transaction or activity reported in Part B to be suspicious. (If t insufficient space, continue the narrative on a separate sheet of paper.)

This section of the report is **critical**. The care with which it is written may make the difference in whether the described condu possible criminal nature are clearly understood. Provide below a chronological and complete account of the activity, including unusual, irregular or suspicious about the transaction, using the following checklist as you prepare your account.

a. **Describe** the conduct that raised suspicion, why it was suspicious and the date(s) discovered.
b. **Explain** whether the transaction(s) was completed or only attempted.
c. **Describe** supporting documentation (e.g., transaction records, new account information, correspondence.) **Retain the originals.**
d. **Explain** who benefited, financially or otherwise, from the transaction, how much, and how.
e. **Retain** any admission or explanation of the transaction provided by the suspect or any other person and indicate to whom and when it was given.
f. **Retain** any evidence of an attempt to deceive the financial institution as to the actual nature of the transaction or amount of the transaction the subject sought to carry out.
g. **Indicate** where a possible violation of law took place, if possible.
h. **Indicate** whether the activity is an isolated incident or relates to another transaction(s). Note whether this is an updated report and if so, provide the date of the original SAR regarding this activity.
i. I**ndicate** whether currency and/or monetary instruments were involved. If so, provide the amount and/or description of the instrument (for example, bank draft, letter of credit, money order, stocks, bonds, traveler's cheques, wire transfers sent or received, cash, etc.) and country of origin.
j. **Describe** any funds transfers, including any in or out ident numbers, parties involved, dates, amounts, and financial ir involved.
k. **Indicate** for a foreign national any available information or passport(s), and/or identification card(s). Include date, cou issue, issuing authority, and nationality.
l. **Describe** subject(s) position if employed by or affiliated wi financial institution.
m. **Indicate** the type of institution filing this report, if this is no
n. **Indicate** if a law enforcement agency other than the OND been contacted, list the name of the agency and the name person contacted, their title, their telephone number, and v were contacted.
o. **Recommend** any further action that you consider might as enforcement authorities
p. **Indicate** whether any information has been excluded from if so, state reasons.
q. **Indicate** any account number(s) that may be involved or a
r. **If correcting or amending** a prior report, complete the for entirety and note the items that contain the changes .

Take Note: SARs are confidential and must be handled accord

Appendix D

PART E - DETAILS OF REPORTING FINANCIAL INSTITUTION

26 Type of financial institution reporting

.....

27 Name of financial institution

.....

28 Address of financial institution

Street.....

City:.....

State/province:.....

Postcode:.....

Country:.....

email:.....

29 Location of branch where transaction or activity or the attempt took place (if different from item 26 above)

Street.....

City:.....

State/province:.....

Postcode:.....

Country:.....

30 ☐ Check box if the suspicious activity took place in more than one branch or location and indicate this information in Part D.

31 Details of Compliance Officer or authorised person who can be contacted for assistance in this matter

Name.....

Position:.....

Office Address:.....

Telephone:.....

Fax:.....

email:.....

PART F - STATEMENT OF REPORTING FINANCIAL INST

32 This statement is made by the financial institutic named in Part E pursuant to the requirement of Se 13(2) of the MLPA to report suspicious transactions based on the information provided in Part D.

I declare the information contained in this repo correct to the best of my knowledge, informatic belief.

Date report prepared (dd/mm/yyyy):

SIGN HERE

Signature of Compliance Officer or authorised

OFFICIAL USE ONLY

Report number

Case Officer

Comments

Appendix D

FORM 1A

Suspicious Activity Report

(Internet Gaming)

Form Revised — 31 October 2008

To: The Supervisory Authority
ONDCP Headquarters
Camp Blizard, Antigua

COMPLETE ENTIRE REPORT
(see Instructions)

*Please complete this form in **black ink** and print in **CAPITAL LETTERS***
Mark appropriate answer boxes with a check (√)

Instructions on how to prepare a suspicious activity report using this form are enclosed with the form or can be obtained from the ONDCP.

CONFIDENTIAL

This Report is a confidential document and must be treated accordingly.

Internet Gambling Companies are listed as financial institutions in the First Schedule to the Money Laundering (Prevention) Act 1996 (as amended) ("MLPA"). Reporting to the Supervisroy Authority of fraudulent or suspicious transactions which may involve money laundering or an activity similar to money laundering is required of of financial institutions, including internet gambling companies by Section 13 of the MLPA and Regulation 223 of the Interactive Gaming and Interactive Wagering Regulations 2007 (IGIWR). Such reports must be made using this form (either Form 1A or its electronic version Form 1A-e).

Tipping off: Financial institutions (including employees, staff, directors, owners or other authorized representatives) shall not notify any person that this SAR has been filed and information relating thereto requested by or furnished to the Supervisory Authority. Criminal offence is committed contrary to section 13(5) of the MLPA for failure to comply with this obligation.

Submit the completed form to:
THE SUPERVISORY AUTHORITY
ONDCP Headquarters
P.O. Box W 827, Camp Blizard, Antigua
Tel: (268) 562-3255 **email: ondcp@ondcp.gov.ag**
Help: (268) 562-3255 **Fax: (268) 460-8818**

Privacy Statement

The provisions of Section 13 of the MLPA and Regulations 223 of the IGIWR are designed to help detect money laundering and uncover the proceeds of crime. Information reported to the Supervisory Authority at the ONDCP is kept confidential. However, the Supervisory Authority is legally authorised to share the information with another law enforcement authority where the disclosure is essential to the detection, investigation or prosecution of an offence. As financial institutions, Gaming Companies and their employees are required by Regulation 223 to file suspicious activity reports and authorised by Regulation 158(c) of the IGIWR to disclose information required to enforce the Regulations, and are protected by Section 13(4)of the MLPA from criminal, civil or administrative liability for complying with the legal requirement to file reports of transactions that constitute or could be related to money laundering.

Penalties exist for failure to supply full and correct information as required.

For assistance please call the Manager of the Financial Intelligence Unit of the ONDCP at **(268) 562-3255**

Important Note

Reporting is required to be done promptly. Under Regulation 223 of the IGIWR reports of suspicious transactions or activities that may involve money laundering must be made within 24 hours or as soon as practicable after the activity being reported.

Please note the time when the suspicious transaction/activity or payment occurred and the time when you start to complete this form. You may be asked how long you took to complete it.

1 ☐ *Check the box if this report is made to correct or update a prior report. Where a correction is being filed, the entire form must be completed again and changes indicated in Part D.*

PART A - IDENTITY OF SUBJECT(S) CONDUCTING THE SUSPICIOUS ACTIVITY OR TRANSACTION

2 ☐ Subject information unavailable

3 ☐ Multiple subjects involved

SUBJECT INFORMATION

4 (a) Name of individual or entity:

Surname: .....

First name: .....

Middle name: .....

(b) alias (if any): .....

(c) trading as: .....

5 Address (cannot be a P.O. Box)

Street: .....

City: .....

State/province: .....

Postcode: .....

Country: .....

6 Date of birth: ..... (dd/mm/yyyy)

7 (a) Forms of identity verification

☐ (i) passport - no.: .....
☐ (ii) driver's licence - no.: .....
☐ (iii) voter registration card - no.: .....
☐ (iv) identity card - no.: .....
☐ (v) certificate of incorporation - no.: .....
☐ (vi) other: .....

(b) Authority that issued document(s): .....

.....

8 Subject's relationship to the reporting financial institution

☐ (a) Customer/Player
☐ (b) Accountant
☐ (c) Agent
☐ (d) Appraiser
☐ (e) Attorney
☐ (f) Director
☐ (g) Employee
☐ (h) Officer
☐ (i) Shareholder
☐ (j) Other:.....

9 Player account number (if any) .....

10 Is the subject working with or for the reporting institution?

☐ (a) Yes
☐ No

The Subject is

☐ (b) still employed
☐ (c) suspended
☐ (d) terminated
☐ (e) resigned

11 Date of suspension, termination or resignation: ..... (dd/mm/yyyy)

Appendix D

PART B - DETAILS OF THE TRANSACTION OR ACTIVITY

12 Date or date range of suspicious transaction(s) or activity
From ..... (dd/mm/yyyy) to ..... (dd/mm/yyyy)

13a Type of gaming/wagering activity (game, sports event etc.) invovled:
and/or .....

13b Type of transaction involved (eg. deposit, wager, payment etc.):
.....

14 URL of website involved
.....

15 Currency and the amount involved in transaction(s). If more than one currency is involved list each currency and its amount.(For conversion rates check)

Currency	Amount
USD	, , , . 0 0
	, , , . 0 0
	, , , . 0 0

16 Total value of transaction(s) in U.S. Dollars

USD	, , , . 0 0

17 Type and quantity of instrument(s) involved

	Type	Quantity
(1)	.....	.....
(2)	.....	.....
(3)	.....	.....

18 Transaction number(s)
.....
.....

19 Accounts affected
(1) Account number: .....
(2) Account number: .....
(3) Account number: .....

20 If account(s) were closed, date closed
(1) date .....
(2) date .....
(3) date .....
(4) date .....

PART C - SUMMARY CHARACTERIZATION OF SUSPIC ACTIVITY

21 Category of Suspicious Activity. Check the box(which best identifies the suspicious activity tha stitutes or could be related to money launderin needed, a numbered list of typologies is attach end of the instructions for preparing this form.)

- ☐ (a) Structuring
- ☐ (b) Money laundering
- ☐ (c) Cheque Fraud
- ☐ (d) Computer Intrusion
- ☐ (e) Counterfeit Cheque
- ☐ (f) Counterfeit Instrument
- ☐ (g) Credit Card Fraud
- ☐ (h) Debit Card Fraud
- ☐ (i) Embezzlement
- ☐ (j) Identity Theft
- ☐ (k) Mysterious Disapperance
- ☐ (l) Refusal/failure to complete CDD requi
- ☐ (m) Refusal/failure to update CDD informa
- ☐ (n) Terrorist Financing
- ☐ (o) Wire Transfer Fraud
- ☐ (p) The suspicious activity resembles typ

No.....

- ☐ (q) Other:.....

22 Character of suspicious activity

- ☐ (a) unusual transaction
- ☐ (b) complex transaction
- ☐ (c) large transaction
- ☐ (d) unusual pattern of transactions with n ent economic purpose
- ☐ (e) insignificant but periodic transactions apparent economic purpose
- ☐ (f) unusual use of monetary instrument
- ☐ (g) other:

.....

Appendix D

PART D - DESCRIPTION AND EXPLANATION OF SUSPICIOUS TRANSACTION /ACTIVITY

23* Give the reasons why you consider the transaction(s) or activity reported in Parts B and C to be suspicious. (If there is insufficient space, continue the narrative on a separate sheet of paper.)

This section of the report is **critical**. The care with which it is written may make the difference in whether the described conduct and its possible criminal nature are clearly understood. Provide below a chronological and complete account of the activity, including what is unusual, irregular or suspicious about the transaction, using the following checklist as you prepare your account.

a. **Describe** the conduct that raised suspicion, why it was suspicious and the date(s) it occurred.
b. **Indicate** any account number(s) that may be involved or affected.
c. **Explain** whether the transaction(s) was completed or only attempted.
d. **Describe** supporting documentation (e.g., transaction records, new account information, correspondence.) **Retain the originals.**
e. **Explain** who benefited, financially or otherwise, from the transaction, how much, and how.
f. **Retain** any admission or explanation of the transaction provided by the suspect or any other person and indicate to whom and when it was given.
g. **Retain** any evidence of an attempt to deceive the financial institution as to the actual nature of the transaction or amount of the transaction the subject sought to carry out.
h. **Indicate** where a possible violation of law took place, if possible.
i. **Indicate** whether the activity is an isolated incident or relates to another transaction(s).
j. I**ndicate** whether currency and/or monetary instruments were involved. If so, provide the amount and/or description of the instrument (for example, bank draft, money order, wire transfer sent or received, cash, etc.) and country of origin.
k. **Describe** any funds transfers, including any in or out identification numbers, parties involved, dates, amounts, and financial institutions involved.
l. **Indicate** for a foreign national any available information on subject's passport(s), and/or identification documents(s). Include date, country, and city of issue, issuing authority, and nationality.
m. **Describe** subject(s) position if employed by or affiliated with reporting the financial institution.
n. **Indicate** if a law enforcement agency other than the ONDCP has been contacted, list the name of the agency and the name of any person contacted, their title, their telephone number, and when they were contacted.
o. **Recommend** any further action that you consider might assist law enforcement authorities
p. **Indicate** whether any information has been excluded from this report; if so, state reasons.
q. **If correcting or amending** a prior report, complete the form in its entirety and point out the items that contain the changes .
r. **If updating** a prior report provide the date of the original SAR regarding the activity.

Take Note: SARs are confidential and must be handled accordingly.

24 Is additional information attached to this report?

☐ **No** ☐ **Yes** If yes, please specify: .....

.....

Appendix D

PART E - DETAILS OF REPORTING COMPANY

25 Name of Licence Holder (company filing report)

.....

26 Address of Licence Holder

Street: .....

City: .....

State/province: .....

Postcode: .....

Country: .....

27 Address of office issuing the report

Street: .....

City: .....

State/province: .....

Postcode: .....

Country: .....

28 Physical address of office/facility from which the transaction or activity was processed or detected (if different from 27 above)

Street: .....

City: .....

State/province: .....

Postcode: .....

Country: .....

29 Details of Money Laundering Compliance Office authorised person submitting the report

Name: .....

Position: .....

Office Address:

Street: .....

City: .....

State/province: .....

Postcode: .....

Country: .....

Telephone: .....

Fax: .....

email: .....

PART F- STATEMENT OF THE LICENCE HOLD

30 This report is made by or on behalf of the Licen
er named in 23 above pursuant to the requirement
fraudulent or suspicious transactions that may invo
money laundering under Regulation 223 of the IGI\
Section 13 of the MLPA, and is based on the groun
out in Part D.

**I declare the information contained in this repo
correct to the best of my knowledge, informatio
belief.**

Date .....
(dd/mm/yyyy)

SIGN HERE .....

Signature of Compliance Officer or authorise

OFFICIAL USE ONLY

Report number

Case Officer

Comments

Appendix A

FORM 1C

Significant Payment Report
(over US$25,000)
Internet Gaming

Form revised 31 October 2008

To: The Supervisory Authority
ONDCP Headquarters
Camp Blizard, Antigua

COMPLETE ENTIRE REPORT
(see Instructions)

*Please complete this form in **black ink** and print in **CAPITAL LETTERS***
Mark appropriate answer boxes with a check (√)

Instructions on how to prepare a significant payment report using this form are enclosed with the form or can be obtained from the ONDCP.

CONFIDENTIAL

This Report is a confidential document and must be treated accordingly.

Reporting to the Supervisory Authority by internet gambling companies of payments made to players from the player's account exceeding the threshold of US$25,000 is required by regulation 148(d) of the Interactive Gaming and Interactive Wagering Regulations 2007 (IGIWR). Such reports must be made using this form (Form 1C or its electronic version Form 1C-e). For purposes of this form, such reports may be referred to as "significant payment reports".

Complete and submit this form within 48 hours of the payment being made.

If there is reason to suspect that the payment being reported may involve money laundering activity, then in addition, a separate suspicious activity report must be made on the appropriate form (Form 1A).

Submit the completed form to:
THE SUPERVISORY AUTHORITY
ONDCP Headquarters
P.O. Box W 827, Camp Blizard, Antigua
Tel: (268) 562-3255 **email: supervisoryauthority@ondcp.gov.ag**
Help: (268) 562-3261 **Fax: (268) 460-8818**

Privacy Statement

The provisions of Regulation 148(d) of the IGIWR are designed to help detect money laundering activity and uncover the proceeds of crime. Information reported to the Supervisory Authority at the ONDCP is kept confidential. However, the Supervisory Authority is legally authorised to share the information with another law enforcement authority where the disclosure is essential to the detection, investigation or prosecution of an offence. As financial institutions, Gaming Companies and their employees are authorised by Regulation 158(c) of the IGIWR to disclose information required to enforce the Regulations.

Penalties exist for failure to comply with the regulatory requirement.

For assistance please call the Manager of the Financial Intelligence Unit of the ONDCP at **(268) 562-3255**

Important Note

Reporting is required to be done promptly. Under Regulation 148(d) reports of payments exceeding US$25,000 must be made within 48 hours of the payment.
Please note the time when the payment occurred and the time when you complete this

PART A - IDENTITY OF PERSON TO WHOM PAYMENT WAS MADE

1 Player account number .....

2 (a) Name of Player

Surname: .....

First name: .....

Middle name: .....

(b) alias (if any): .....

3 Player account address (cannot be a P.O. Box only)

Street: .....

City: .....

State/province: .....

Postcode: .....

Country: .....

4 Date of birth .....
(dd/mm/yyyy)

PART B - DETAILS OF THE PAYMENT

5 Name of gaming activity that resulted in payout

.....

6 Date of payment .....
(dd/mm/yyyy)

7 Method of payment (eg. wire to credit card account, cheque to Player's account address)

.....

8 Amount paid out by reporting licence holder: If more than one currency is involved in the transaction(s) list each currency and its amount

Currency	Amount
USD	, , , . 0 0
	, , , . 0 0
	, , , . 0 0
	, , , . 0 0

9 Total value of transaction(s) in U.S. Dollars

USD	, , , . 0 0

PART C - COMMENTS

10 Comment on anything noteworthy or unusual about the nature and circumstances concerning how the money was won or obtained or the payout made as reported in Part B

Appendix A

PART D - DETAILS OF REPORTING GAMING COMPANY

11 Name of Licence Holder (company making report)

.....

12 Address of Licence Holder

Street: .....

City: .....

State/province: .....

Postcode: .....

Country: .....

13 Physical address of office/facility from which the payout was made or the transaction or activity processed (if different from 12 above)

Street: .....

City: .....

State/province: .....

Postcode: .....

Country: .....

14 Details of Compliance Officer or authorised person submitting the report

Name: .....

Position: .....

Office Address:

Street: .....

City: .....

State/province: .....

Postcode: .....

Country: .....

Telephone: .....

Fax: .....

email: .....

PART E - STATEMENT OF REPORTING FINANCIAL INSTITUTION

15 This report is made by or on behalf of the Licence Holder named in item 11 above pursuant to the requirement to report all payments to a player from the player's account exceeding U.S.$25,000 under Regulation 148(d) of the IGIWR.

I declare the information contained in this report to be correct to the best of my knowledge, information and belief.

Date (dd/mm/yyyy) .....

SIGN HERE .....

Signature of Compliance Officer or authorised person

OFFICIAL USE ONLY

Report number

Case Officer

Comments

Appendix A

FORM 3

Terrorist Property Report
(Section 34 of the Prevention of Terrorism Act 2005)

Submit the completed form to the Director, ONDCP Headquarters, P.O. Box W827, Camp Blizard, Antigua

If you are a financial institution or person that has property in your possession or control that you believe is owned or controlled by or on behalf of a designated terrorist or terrorist organisation or are making a quarterly statutory report on whether or not you possess or control such property, you should use this form to make a report of the property to the Director of the ONDCP. A designated terrorist or terrorist organisation is one that has been so designated by publication of the entitiy's name and details in the Gazette by the Attorney General pursuant to Section 3 of the Prevention of Terrorism Act 2005. "financial institution" means a commercial bank, or any other institution which makes loans advances or investments or accepts deposits of money from the public.

Please type or print and select boxes and buttons as appropriate.

PART A – Reporting Financial Institution

1. Name .....
2. Street Address .....
3. City/Town ..... 4. State/Province ..... 5. Post code .....
6. Country .....
7. Type of financial institution .....
8. Telephone ..... 9. Fax .....
10. Email .....

PART B – Reporting Period

11. ☐ This report is for the following period:
    - ☐ a. January to March
    - ☐ b. April to June
    - ☐ c. July to September
    - ☐ d. October to December

    Year ☐

☐ This is a spontaneous report as required by the Act, made upon discovering funds or property suspected of being related to a specified entity.

PART C – Checks Made of Specified Entities

12. The financial institution named in Part A has over the reporting period made itself aware of the names and identification details of specified entities (terrorists and terrorist organizations) published in the source(s) ticked below and compared them to the identities of its customers:

☐ **(a) The Gazette of the Government of Antigua and Barbuda —**

- ☐ **Prevention of Terrorism (Security Council Resolution) Orders and amendments**
- ☐ **Prevention of Terrorism (Specified Entities Account and Property Freezing) Orders and amendments**

☐ **(b) The United Nations Security Council Sanctions List(s) —**

- ☐ **website sanctions lists relating to Resolution 1267(1999) and 1989(2011)**
- ☐ **website sanctions lists relating to other UN Sanctions Resolution(s) (specify):**

☐ **(c) Other source(s) (specify):**

Appendix A

PART D – Results of Checks

13. The following are the results of the checks made in Part C (tick/select all appropriate boxes and buttons):

- ☐ (1) A match with the identity of a specified entity was found in the customer database.
  - ☐ (a) A suspicious activity report was filed in relation to the customer or entity.
  - ☐ (b) A suspicious activity report is being prepared and will be filed in relation to the customer or entity on the Suspicious Activity Report form issued by the ONDCP.
- ☐ (2) A suspicious transaction was detected indicating possible links to a specified entity or terrorism financing.
  - ☐ (a) A suspicious activity report was filed in relation to the customer or entity.
  - ☐ (b) A suspicious activity report is being prepared and will be filed in relation to the customer or entity on the Suspicious Activity Report form issued by the ONDCP.
- ☐ (3) Property or funds suspected of belonging to or being held on behalf of or related to a specified entity was discovered.
  - ☐ (a) A suspicious activity report was filed in relation to the customer or entity.
  - ☐ (b) A suspicious activity report is being prepared and will be filed in relation to the customer or entity on the Suspicious Activity Report form issued by the ONDCP.
- ☐ (4) Property or funds of a specified entity discovered in a previous reporting period continued to be held.
  - ☐ (a) A suspicious activity report was filed in relation to the customer or entity.
  - ☐ (b) A suspicious activity report is being prepared and will be filed in relation to the customer or entity on the Suspicious Activity Report form issued by the ONDCP.
- ☐ (5) No match was found with the identify of any specified entity in the customer database.
- ☐ (6) No suspicious transaction was detected that appeared to indicate possible links to a specified entity or terrorism financing.
- ☐ (7) No property or funds was discovered that was suspected of belonging to or being held on behalf of or related to a specified entity.
- ☐ (8) No property or funds was known to be in the possession or control of the reporting institution which belonged to or was held on behalf of any specified entity .

PART E – Details of Funds/Property Related to Specified Entity

14. a. Name of specified entity (terrorist or terrorist organization) to whom the funds or property relates directly or indirectly (eg. direct or indirect ownership or control)

Appendix A

b. The following funds and/or other property related to the specified entity have been identified.

I declare the information given herein is true and correct to the best of my knowledge and belief.

Date of report: .....
dd-mmmm-yyyy

Name of reporting officer: .....

Position of reporting officer: .....

Signature
(Sign here)

X