OCC 2003-27

OCC BULLETIN

Comptroller of the Currency
Administrator of National Banks

Subject: Suspicious Activity Report Description: Revised Form

TO: Chief Executive Officers and Compliance Officers of All National Banks, Department and Division Heads, and All Examining Personnel

Pursuant to 12 CFR 21.11, all national banks, as well as all federal branches and agencies of foreign banks licensed by the Office of the Comptroller of the Currency (OCC), are required to file a Suspicious Activity Report (SAR) when they detect a known or suspected violation of federal law or a suspicious transaction related to a money-laundering activity or a violation of the Bank Secrecy Act. Beginning July 1, 2003, national banks and federal branches and agencies may begin using the revised SAR form attached to this bulletin. Banks and federal branches and agencies may continue using the existing SAR form while their procedures and systems are updated, but must start using the revised form by January 1, 2004. The revised SAR form is available on the Financial Crimes Enforcement Network (FinCEN) Web site (http://www.fincen.gov).

The revised form contains three changes from the previous version:

- Part III - The addition of two boxes to check for terrorist financing and identity theft;
- Part V - The addition of a statement indicating that tips on preparing and filing the SAR form are available on the FinCEN Web site; and
- SAR Instructions - The Safe Harbor provisions have been updated to incorporate USA PATRIOT Act changes.

Preparers should refrain from using the "Other" box if it would be more appropriate to use either the "Terrorist Financing" or "Identity Theft" box. Examples of when use of these boxes would be appropriate are included in the "SAR Activity Review – Tips, Trends and Issues" (February 2003), and additional information concerning terrorist or other criminal financial activity is included in FinCEN's "SAR Bulletin No. 4" (January 2002). Both of these documents are available on the FinCEN Web site.

If a bank has a match with a Specially Designated Global Terrorist (SDGT) or Foreign Terrorist Organization on the Specially Designated Nationals list published by the Office of Foreign Assets Control (OFAC), the bank should review the account and any related activity. If the bank discovers anything suspicious, the bank should file a SAR in accordance with the regulation and the instructions on the form.

Terrorist Financing

FinCEN's SAR Bulletin No. 4 provides various indicators and patterns of activity that could be associated with funds collection related to terrorist financing and the movement of funds related to terrorist financing.[1] Some of the indicators and patterns of activity noted in the bulletin include the following:

- Use of a business account to collect and then funnel funds to a smaller number of foreign beneficiaries, both individual and business, in a country associated with terrorism;
- Use of a business account that would not normally generate the volume of wire transfer activity, into and out of the account, as reported;
- Use of multiple individuals to structure transactions under the reporting threshold to circumvent reporting requirements and then funnel funds to a foreign beneficiary;
- Large currency withdrawals from a business account not normally associated with cash transactions;
- Same-day transactions at the same depository institutions using different tellers;
- Shared addresses, which are also business locations, by persons involved in currency transactions;
- Apparent intent to circumvent wire remittance company's internal requirements for presentation of identification through purchase of money orders in small amounts; or
- Movement of funds through a Financial Action Task Force (FATF) designated non-cooperative country or territory.

Identity Theft

FinCEN's SAR Activity Review notes that it would be appropriate to select the "Identity Theft" box in instances in which a person is suspected of having:

- Used someone else's social security number and personal data in order to obtain a loan in that person's name; or
- Established fraudulent bank accounts using the identities of numerous persons.

In addition, occurrences of identity theft or suspected identity theft may increasingly be the result of bank insider or employee misconduct. Examples of when it would be appropriate to select the "Identity Theft" box include situations where a bank employee or insider has:

- Been assigned to work on one type of account and then accessed unrelated, different types of accounts or account information with no valid or permissible business purpose;
- Copied or transferred customers' personal information to a third party who is not employed by the bank, and not otherwise authorized by the bank or customers to review or possess the information;
- Altered or changed more than one account record to reflect addresses or phone numbers that are unknown to the true customers;
- Processed or ordered more than one replacement credit card or other product, when the credit cards or other products are sent to addresses unknown to the true customers;

[1] The bulletin points out that taken individually, the indicators do not necessarily equate to terrorist or other criminal financial activity. Combinations of indicators should raise the level of concern about potential terrorist financing or other criminal context.

- Linked more than two accounts for unrelated customers who are unknown to each other, and who have not authorized such account linkages; or
- Been arrested, or charged with a crime, when customer personal information, customer account documentation, or customer identification was found in the possession of the bank employee or insider at a location outside of the bank.

Questions about the revised SAR form may be directed to your OCC supervisory office or the Compliance Division at (202) 874-4428. In addition, questions regarding use of the "Terrorist Financing" or "Identity Theft" boxes may be directed to the Enforcement and Compliance Division at (202) 874-4800.

_____

David G. Hammaker
Deputy Comptroller for Compliance

Attachment
[http://www.fincen.gov/reg_bsaforms.html#newsar]

Suspicious Activity Report

July 2003

Previous editions will not be accepted after December 31, 2003

ALWAYS COMPLETE ENTIRE REPORT (see instructions)

FRB:	FR 2230	OMB No. 7100-0212
FDIC:	6710/06	OMB No. 3064-0077
OCC:	8010-9,8010-1	OMB No. 1557-0180
OTS:	1601	OMB No. 1550-0003
NCUA:	2362	OMB No. 3133-0094
TREASURY:	TD F 90-22.47	OMB No. 1506-0001

1 Check box below only if correcting a prior report.
☐ Corrects Prior Report (see instruction #3 under "How to Make a Report")

Part I Reporting Financial Institution Information

2 Name of Financial Institution

3 EIN

4 Address of Financial Institution

5 Primary Federal Regulator
a ☐ Federal Reserve d ☐ OCC
b ☐ FDIC e ☐ OTS
c ☐ NCUA

6 City

7 State

8 Zip Code

9 Address of Branch Office(s) where activity occurred ☐ Multiple Branches (include information in narrative, Part V)

10 City

11 State

12 Zip Code

13 If institution closed, date closed
____ / ____ / _____
MM DD YYYY

14 Account number(s) affected, if any
a _____ Closed? ☐ Yes ☐ No
b _____ Closed? ☐ Yes ☐ No
c _____ Closed? ☐ Yes ☐ No
d _____ Closed? ☐ Yes ☐ No

Part II Suspect Information ☐ Suspect Information Unavailable

15 Last Name or Name of Entity

16 First Name

17 Middle

18 Address

19 SSN, EIN or TIN

20 City

21 State

22 Zip Code

23 Country

24 Phone Number - Residence (include area code)
( )

25 Phone Number - Work (include area code)
( )

26 Occupation/Type of Business

27 Date of Birth
_____ / _____ / _____
MM DD YYYY

28 Admission/Confession?
a ☐ Yes b ☐ No

29 Forms of Identification for Suspect:
a ☐ Driver's License/State ID b ☐ Passport c ☐ Alien Registration d ☐ Other _____
Number _____ Issuing Authority _____

30 Relationship to Financial Institution:
a ☐ Accountant d ☐ Attorney g ☐ Customer j ☐ Officer
b ☐ Agent e ☐ Borrower h ☐ Director k ☐ Shareholder
c ☐ Appraiser f ☐ Broker i ☐ Employee l ☐ Other _____

31 Is the relationship an insider relationship? a ☐ Yes b ☐ No
If Yes specify: c ☐ Still employed at financial institution e ☐ Terminated
d ☐ Suspended f ☐ Resigned

32 Date of Suspension, Termination, Resignation
_____ / _____ / _____
MM DD YYYY

Part III Suspicious Activity Information

33 Date or date range of suspicious activity
From ____ / _____ / _____ To ____ / _____ / _____
MM DD YYYY MM DD YYYY

34 Total dollar amount involved in known or suspicious activity
$ .00

35 Summary characterization of suspicious activity:

- a ☐ Bank Secrecy Act/Structuring/ Money Laundering
- b ☐ Bribery/Gratuity
- c ☐ Check Fraud
- d ☐ Check Kiting
- e ☐ Commercial Loan Fraud
- f ☐ Computer Intrusion
- g ☐ Consumer Loan Fraud
- h ☐ Counterfeit Check
- i ☐ Counterfeit Credit/Debit Card
- j ☐ Counterfeit Instrument (other)
- k ☐ Credit Card Fraud
- l ☐ Debit Card Fraud
- m ☐ Defalcation/Embezzlement
- n ☐ False Statement
- o ☐ Misuse of Position or Self Dealing
- p ☐ Mortgage Loan Fraud
- q ☐ Mysterious Disappearance
- r ☐ Wire Transfer Fraud
- t ☐ Terrorist Financing
- u ☐ Identity Theft
- s ☐ Other _____ (type of activity)

36 Amount of loss prior to recovery (if applicable)
$ .00

37 Dollar amount of recovery (if applicable)
$ .00

38 Has the suspicious activity had a material impact on, or otherwise affected, the financial soundness of the institution?
a ☐ Yes b ☐ No

39 Has the institution's bonding company been notified?
a ☐ Yes b ☐ No

40 Has any law enforcement agency already been advised by telephone, written communication, or otherwise?

- a ☐ DEA
- b ☐ FBI
- c ☐ IRS
- d ☐ Postal Inspection
- e ☐ Secret Service
- f ☐ U.S. Customs
- g ☐ Other Federal
- h ☐ State
- i ☐ Local
- j ☐ Agency Name (for g, h or i) _____

41 Name of person(s) contacted at Law Enforcement Agency

42 Phone Number (include area code)
( )

43 Name of person(s) contacted at Law Enforcement Agency

44 Phone Number (include area code)
( )

Part IV Contact for Assistance

45 Last Name

46 First Name

47 Middle

48 Title/Occupation

49 Phone Number (include area code)
( )

50 Date Prepared
_____ / _____ / _____
MM DD YYYY

51 Agency (if not filed by financial institution)

Part V Suspicious Activity Information Explanation/Description

3

Explanation/description of known or suspected violation of law or suspicious activity.

This section of the report is **critical**. The care with which it is written may make the difference in whether or not the described conduct and its possible criminal nature are clearly understood. Provide below a chronological and **complete** account of the possible violation of law, including what is unusual, irregular or suspicious about the transaction, using the following checklist as you prepare your account. **If necessary, continue the narrative on a duplicate of this page.**

a **Describe** supporting documentation and retain for 5 years.
b **Explain** who benefited, financially or otherwise, from the transaction, how much, and how.
c **Retain** any confession, admission, or explanation of the transaction provided by the suspect and indicate to whom and when it was given.
d **Retain** any confession, admission, or explanation of the transaction provided by any other person and indicate to whom and when it was given.
e **Retain** any evidence of cover-up or evidence of an attempt to deceive federal or state examiners or others.
f **Indicate** where the possible violation took place (e.g., main office, branch, other).
g **Indicate** whether the possible violation is an isolated incident or relates to other transactions.
h **Indicate** whether there is any related litigation; if so, specify.
i **Recommend** any further investigation that might assist law enforcement authorities.
j **Indicate** whether any information has been excluded from this report; if so, why?
k If you are correcting a previously filed report, describe the changes that are being made.

For Bank Secrecy Act/Structuring/Money Laundering reports, include the following additional information:

l **Indicate** 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, domestic or international money order, stocks, bonds, traveler's checks, wire transfers sent or received, cash, etc.).
m **Indicate** any account number that may be involved or affected.

Tips on SAR Form preparation and filing are available in the SAR Activity Review at www.fincen.gov/pub_reports.html

Suspicious Activity Report
Instructions

Safe Harbor Federal law (31 U.S.C. 5318(g)(3)) provides complete protection from civil liability for all reports of suspicious transactions made to appropriate authorities, including supporting documentation, regardless of whether such reports are filed pursuant to this report's instructions or are filed on a voluntary basis. Specifically, the law provides that a financial institution, and its directors, officers, employees and agents, that make a disclosure of any possible violation of law or regulation, including in connection with the preparation of suspicious activity reports, "shall not be liable to any person under any law or regulation of the United States, any constitution, law, or regulation of any State or political subdivision of any State, or under any contract or other legally enforceable agreement (including any arbitration agreement), for such disclosure or for any failure to provide notice of such disclosure to the person who is the subject of such disclosure or any other person identified in the disclosure".

Notification Prohibited Federal law (31 U.S.C. 5318(g)(2)) requires that a financial institution, and its directors, officers, employees and agents who, voluntarily or by means of a suspicious activity report, report suspected or known criminal violations or suspicious activities may not notify any person involved in the transaction that the transaction has been reported.

In situations involving violations requiring immediate attention, such as when a reportable violation is ongoing, the financial institution shall immediately notify, by telephone, appropriate law enforcement and financial institution supervisory authorities in addition to filing a timely suspicious activity report.

WHEN TO MAKE A REPORT:

1. All financial institutions operating in the United States, including insured banks, savings associations, savings association service corporations, credit unions, bank holding companies, nonbank subsidiaries of bank holding companies, Edge and Agreement corporations, and U.S. branches and agencies of foreign banks, are required to make this report following the discovery of:

   a. **Insider abuse involving any amount.** Whenever the financial institution detects any known or suspected Federal criminal violation, or pattern of criminal violations, committed or attempted against the financial institution or involving a transaction or transactions conducted through the financial institution, where the financial institution believes that it was either an actual or potential victim of a criminal violation, or series of criminal violations, or that the financial institution was used to facilitate a criminal transaction, and the financial institution has a substantial basis for identifying one of its directors, officers, employees, agents or other institution-affiliated parties as having committed or aided in the commission of a criminal act regardless of the amount involved in the violation.

   b. **Violations aggregating $5,000 or more where a suspect can be identified.** Whenever the financial institution detects any known or suspected Federal criminal violation, or pattern of criminal violations, committed or attempted against the financial institution or involving a transaction or transactions conducted through the financial institution and involving or aggregating $5,000 or more in funds or other assets, where the financial institution believes that it was either an actual or potential victim of a criminal violation, or series of criminal violations, or that the financial institution was used to facilitate a criminal transaction, and the financial institution has a substantial basis for identifying a possible suspect or group of suspects. If it is determined prior to filing this report that the identified suspect or group of suspects has used an "alias," then information regarding the true identity of the suspect or group of suspects, as well as alias identifiers, such as drivers' licenses or social security numbers, addresses and telephone numbers, must be reported.

   c. **Violations aggregating $25,000 or more regardless of a potential suspect.** Whenever the financial institution detects any known or suspected Federal criminal violation, or pattern of criminal violations, committed or attempted against the financial institution or involving a transaction or transactions conducted through the financial institution and involving or aggregating $25,000 or more in funds or other assets, where the financial institution believes that it was either an actual or potential victim of a criminal violation, or series of criminal violations, or that the financial institution was used to facilitate a criminal transaction, even though there is no substantial basis for identifying a possible suspect or group of suspects.

   d. **Transactions aggregating $5,000 or more that involve potential money laundering or violations of the Bank Secrecy Act.** Any transaction (which for purposes of this subsection means a deposit, withdrawal, transfer between accounts, exchange of currency, loan, extension of credit, purchase or sale of any stock, bond, certificate of deposit, or other monetary instrument or investment security, or any other payment, transfer, or delivery by, through, or to a financial institution, by whatever means effected) conducted or attempted by, at

or through the financial institution and involving or aggregating $5,000 or more in funds or other assets, if the financial institution knows, suspects, or has reason to suspect that:

i. The transaction involves funds derived from illegal activities or is intended or conducted in order to hide or disguise funds or assets derived from illegal activities (including, without limitation, the ownership, nature, source, location, or control of such funds or assets) as part of a plan to violate or evade any law or regulation or to avoid any transaction reporting requirement under Federal law;

ii. The transaction is designed to evade any regulations promulgated under the Bank Secrecy Act; or

iii. The transaction has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the financial institution knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

The Bank Secrecy Act requires all financial institutions to file currency transaction reports (CTRs) in accordance with the Department of the Treasury's implementing regulations (31 CFR Part 103). These regulations require a financial institution to file a CTR whenever a currency transaction exceeds $10,000. If a currency transaction exceeds $10,000 and is suspicious, the institution must file both a CTR (reporting the currency transaction) and a suspicious activity report (reporting the suspicious or criminal aspects of the transaction). If a currency transaction equals or is below $10,000 and is suspicious, the institution should only file a suspicious activity report.

2. **Computer Intrusion.** For purposes of this report, "computer intrusion" is defined as gaining access to a computer system of a financial institution to:

   a. Remove, steal, procure, or otherwise affect funds of the institution or the institution's customers;
   b. Remove, steal, procure or otherwise affect critical information of the institution including customer account information; or
   c. Damage, disable or otherwise affect critical systems of the institution.

   For purposes of this reporting requirement, computer intrusion does not mean attempted intrusions of websites or other non-critical information systems of the institution that provide no access to institution or customer financial or other critical information.

3. A financial institution is required to file a suspicious activity report no later than 30 calendar days after the date of initial detection of facts that may constitute a basis for filing a suspicious activity report. If no suspect was identified on the date of detection of the incident requiring the filing, a financial institution may delay filing a suspicious activity report for an additional 30 calendar days to identify a suspect. In no case shall reporting be delayed more than 60 calendar days after the date of initial detection of a reportable transaction.

4. This suspicious activity report does not need to be filed for those robberies and burglaries that are reported to local authorities, or (except for savings associations and service corporations) for lost, missing, counterfeit, or stolen securities that are reported pursuant to the requirements of 17 CFR 240.17f-1.

HOW TO MAKE A REPORT:

1. Send each completed suspicious activity report to:

   Detroit Computing Center, P.O. Box 33980, Detroit, Ml 48232-0980

2. For items that do not apply or for which information is not available, leave blank.
3. If you are correcting a previously filed report, check the box at the top of the report (line 1). 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 V (Description of Suspicious Activity), line k.
4. **Do not include any supporting documentation with the suspicious activity report.** Identify and retain a copy of the suspicious activity report and all original supporting documentation or business record equivalent for five (5) years from the date of the suspicious activity report. All supporting documentation must be made available to appropriate authorities upon request.
5. If more space is needed to report additional suspects, attach copies of page 1 to provide the additional information. If more space is needed to report additional branch addresses, include this information in the narrative, Part V.
6. Financial institutions are encouraged to provide copies of suspicious activity reports to state and local authorities, where appropriate.