Introduction

The purpose of the Bank Protection Act of 1968 (BPA) is to discourage robberies, burglaries and larcenies committed against financial institutions. The BPA requires the Federal financial institution supervisory agencies to establish minimum standards for the installation, maintenance, and operation of security devices and procedures to discourage these crimes, and to assist in the identification and apprehension of persons who commit them.

To fulfill the statutory mandate, OTS adopted implementing regulations in 1969, contained in 12 CFR Part 568. The regulations, substantially revised in 1991, contain several requirements for savings associations. A savings association's board of directors is responsible for compliance with the regulations. It is the board's responsibility to ensure that a written security program for the association's main office and branches is developed and maintained. In addition, the board must designate a security officer who has the authority, subject to board approval, to develop and administer a written security program.

The regulations establish minimum standards by specifying the contents of a security program and by requiring four specific security devices. Finally, to ensure that an association's security program is substantively reviewed on a timely basis, the regulations require the security officer to report at least annually to the board on the implementation, administration and effectiveness of the security program. Among other things, the report should contain information such as the status of employee training, the number of offenses committed against the association, and the success of prosecution for such offenses.

The timely filing of the required reports to the appropriate regulatory and enforcement agencies is a necessary function after a crime against an association has been committed. The primary form for reporting a crime is the Suspicious Activity Report (SAR), OTS Form 1601 (Exhibit A). The conditions under which this form is filed include any known or suspected criminal activity whether by insiders or those outside the association or service corporation.

Security Program

To comply with the regulations, each association's security program must:

- Establish procedures for opening and closing for business;
- Establish procedures for the safekeeping of all currency, negotiable securities, and other valuables;
- Provide for initial and periodic training of officers and employees in their responsibilities under the security program and in proper employee conduct during and after a burglary, robbery, or larceny;
- Provide for selecting, testing, operating and maintaining appropriate security devices; and
- Establish procedures that will assist in identifying persons that commit a burglary, robbery, or larceny.

The regulations offer additional guidance as to specific procedures that may assist in the identification of persons that commit crimes: procedures may include the use of a camera to record activity in the office, the use of identification devices (e.g., prerecorded serial-numbered bills or chemical and electronic devices), and the retention of a record of any robbery, burglary, or larceny committed against the association.

Security Devices

The regulations require each association to have, at a minimum, the following security devices:

- A means of protecting cash and other assets, such as a vault;
- A lighting system for illuminating the vault during the hours of darkness;

- An alarm system or other appropriate device for promptly notifying law enforcement officials; and
- Tamper-resistant locks on exterior doors and windows that may be opened.

Additional Considerations

The above are the minimum standards for security devices and procedures that should comprise an association's security program. However, the security officer has the discretion under the regulations to determine which additional security devices will best meet the needs of the program. In this way, the security officer can choose the most up-to-date equipment that meets the requirements of a particular association, based on the level of risk. For example, the risk of robbery, etc. will generally be lower for an association in a small, rural environment where the incidence of crime is demonstrably low, and higher for an association in a dense, urban environment with a high incidence of crime. To assist an association in establishing its program, the regulations suggest certain factors to consider in the selection of additional security devices. These include the:

- Incidence of crimes against financial institutions in the area;
- Amount of currency and other valuables exposed to robbery, burglary, or larceny;
- Distance of the office from the nearest law enforcement officers;
- Cost of the security devices;
- Other security measures in effect at the office; and
- Physical characteristics of the office and its surroundings.

Provisions of the security program, including training for all employees, should be carefully monitored by management as well as examiners. Inadequate employee training could easily nullify the most comprehensive and detailed security program. In addition, an association that becomes careless in the area of maintenance may find that its security devices are nonoperative or ineffective simply because equipment is not tested periodically.

Suspicious Activity Report

Effective April 1, 1996, savings associations and their service corporations are required by §563.180 to file a 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.

A SAR is required to be filed for any known or suspected Federal criminal violation, or pattern of criminal violations: (1) involving insider abuse in any amount, (2) aggregating $5,000 or more where a suspect can be identified, or (3) aggregating $25,000 or more regardless of a potential suspect. A SAR is also required to be filed for any transaction aggregating $5,000 or more that involves potential money laundering or violations of the Bank Secrecy Act.

A SAR is filed with the Financial Crimes Enforcement Network of the Department of the Treasury. A savings association or service corporation is required to file a SAR no later than 30 calendar days after the date of initial detection of facts that may constitute a basis for filing a SAR. If no suspect was identified on the date of detection of the incident requiring the filing, a savings association or service corporation may delay filing a SAR for an additional 30 calendar days to identify a suspect, but in no case can the reporting be delayed more than 60 calendar days after the date of initial detection of a reportable transaction. In situations involving violations requiring immediate attention, such as when a reportable violation is ongoing, the savings association or service corporation should immediately notify, by telephone, an appropriate law enforcement authority and the OTS in addition to filing a timely SAR.

A savings association or service corporation is not required to file a SAR under §563.180 for a robbery or burglary committed or attempted that is reported to appropriate law enforcement authorities under the Bank Protection Act.

While the primary responsibility for filing a SAR rests with the association, examiners should ensure that the form has been appropriately filed in all applicable cases. Examiners should prepare a criminal referral form in the following situations:

- When the association has failed to file a SAR (note why it was not filed);
- If the report made by the association is deemed inadequate; or
- When the examiner discovers criminal activity.

A record of filing the form is required to be kept at the association's main office for five years.

The purpose of the report is to provide appropriate law enforcement authorities with complete and accurate information relating to known or suspected criminal activity. All required information should be supplied at the time of the referral unless such information is not known or can only be supplied at a later date subject to the Right to Financial Privacy Act. The provisions of the Right to Financial Privacy Act prohibit examiners from disclosing identifying information concerning the financial records of individuals and partnerships of five or less individuals who are customers of an insured institution to another governmental agency, unless the customer is notified. To avoid having to notify the customer, examiners should delete the customer's name and account number from any records transferred with the completed SAR. The report should indicate the existence of the protected information and documents not included. In the latter case, documents not provided with this form should be segregated and safeguarded in order that they might be subsequently supplied.

Examiners are not required to make any initial finding that such referrals would, if pursued, result in a criminal conviction. That judgment will be made by responsible law enforcement authorities. Any questions regarding whether or not any particular activity would constitute a crime for purposes of making a criminal referral should be resolved through communications with the Regional Office.

Monitoring and Enforcement

OTS Regional staff should review for Bank Protection Act and Criminal Referral Reporting compliance by savings associations under their jurisdiction. Compliance determination by the staff may be derived from monitoring reports of examination, independent audit reports, SARs, and newspaper articles.

When the monitoring reveals significant deficiencies, substantial losses, or repeated incidents, staff may recommend an expansion of scope for this program area at the next regularly scheduled examination. Other corrective actions that the staff may wish to pursue include:

- Require an audit of the functions or accounts affected by the criminal acts and provide a report of action taken in response to the independent or internal audit findings;
- Report the status of the association's recovery of losses filed under its surety bond;
- Refer criminal acts by employees to the appropriate OTS authorities for possible suspension proceedings or removal;
- Direct the board of directors of the association to review and, where applicable, establish procedures to correct the deficiency.

Whenever the security devices or procedures used by a savings association are deficient in meeting the minimum requirements, the association may be required to take necessary corrective action. Pursuant to section 5 of the BPA, an association that violates OTS regulations is subject to a civil penalty not to exceed $100 for each day of the violation.

Examination Objectives

Determine whether the association has a security program and has provided for appropriate security devices and procedures in accordance with minimum regulatory requirements.

Determine whether known or suspected criminal violations have been identified and properly reported.

Examination Procedures

1. Review the association's security program:

   - Ascertain whether its contents are in compliance with the requirements of 12 CFR §568.3(a);
   - Verify that the installation and maintenance of the security devices satisfy the requirements of 12 CFR §568.3(b); and
   - Determine whether the program is revised as appropriate to reflect changes in circumstances, e.g., the addition of a new facility, changes made to a facility, employee turnover, increased cash exposure, the responsiveness of law enforcement agencies, technological advances in security devices, etc.

2. Interview management and staff to ascertain if association personnel have adequate knowledge of policies and sufficient training to implement procedures.

3. Determine whether the security officer reports at least annually to the board of directors on the implementation, administration, and effectiveness of the security program.

4. Review security reports and records to ascertain whether criminal or suspected criminal violations have been reported to the proper authorities. Determine if the Suspicious Activity Report has been prepared where appropriate, and filed on a timely basis.

5. Determine the impact of criminal violations on the association and whether controls have been established to insure against the possibility of further violations.

References

Law

12 USC 1881-1884	Bank Protection Act

Regulations

12 CFR §568	Minimum Security Devices and Procedures
12 CFR §563.180	Suspicious Activity Reports and Other Reports and Statements

List of Exhibits

Exhibit A Form 1601	Suspicious Activity Report

Exhibit A

Suspicious Activity Report

ALWAYS COMPLETE ENTIRE REPORT

1

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

Expires September 30, 1998

1 Check appropriate box:
a ☐ Initial Report b ☐ Corrected Report c ☐ Supplemental Report

Part I Reporting Financial Institution Information

2 Name of Financial Institution

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

4 Address of Financial Institution

5 City | 6 State | 7 Zip Code | 8 EIN or TIN

9 Address of Branch Office(s) where activity occurred

10 Asset size of financial institution
$ .00

11 City | 12 State | 13 Zip Code | 14 If institution closed, date closed (MMDDYY) ____ / ____ / ____

15 Account number(s) affected, if any
a _____
b _____

16 Have any of the institution's accounts related to this matter been closed?
a ☐ Yes b ☐ No If yes, identify _____

Part II Suspect Information

17 Last Name or Name of Entity | 18 First Name | 19 Middle Initial

20 Address | 21 SSN, EIN or TIN (as applicable)

22 City | 23 State | 24 Zip Code | 25 Country | 26 Date of Birth (MMDDYY) ____ / ____ / ____

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

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

29 Occupation

30 Forms of Identification for Suspect:
a ☐ Driver's License b ☐ Passport c ☐ Alien Registration d ☐ Other _____
e Number _____ f Issuing Authority _____

31 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 _____

32 Is insider suspect still affiliated with the financial institution?
a ☐ Yes
b ☐ No
If no, specify { c ☐ Suspended d ☐ Terminated e ☐ Resigned

33 Date of Suspension, Termination, Resignation (MMDDYY) ____ / ____ / ____

34 Admission/Confession
a ☐ Yes b ☐ No

Part III Suspicious Activity Information

2

35 Date of suspicious activity (MMDDYY) ____ / ____ / ____

36 Dollar amount involved in known or suspicious activity
$ .00

37 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 ☐ Consumer Loan Fraud
- g ☐ Counterfeit Check
- h ☐ Counterfeit Credit/Debit Card
- i ☐ Counterfeit Instrument (other)
- j ☐ Credit Card Fraud
- k ☐ Debit Card Fraud
- l ☐ Defalcation/Embezzlement
- m ☐ False Statement
- n ☐ Misuse of Position or Self-Dealing
- o ☐ Mortgage Loan Fraud
- p ☐ Mysterious Disappearance
- q ☐ Wire Transfer Fraud
- r ☐ Other _____

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

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

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

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

42 Has any law enforcement agency already been advised by telephone, written communication, or otherwise? If so, list the agency and local address.
Agency _____

43 Address

44 City

45 State

46 Zip Code

Part IV Witness Information

47 Last Name

48 First Name

49 Middle Initial

50 Address

51 SSN

52 City

53 State

54 Zip Code

55 Date of Birth (MMDDYY) ____ / ____ / ____

56 Title

57 Phone Number (include area code)
( )

58 Interviewed
a ☐ Yes b ☐ No

Part V Preparer Information

59 Last Name

60 First Name

61 Middle Initial

62 Title

63 Phone Number (include area code)
( )

64 Date (MMDDYY) ____ / ____ / ____

Part VI Contact for Assistance (If different than Preparer Information in Part V)

65 Last Name

66 First Name

67 Middle Initial

68 Title

69 Phone Number (include area code)
( )

70 Agency (If applicable)

Part VII 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?

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

k **Indicate** whether currency and/or monetary instruments were involved. If so, provide the amount and/or description.
l **Indicate** any account number that may be involved or affected.

Paperwork Reduction Act Notice: The purpose of this form is to provide an effective and consistent means for financial institutions to notify appropriate law enforcement agencies of known or suspected criminal conduct or suspicious activities that take place at or were perpetrated against financial institutions. This report is required by law, pursuant to authority contained in the following statutes. Board of Governors of the Federal Reserve System: 12 U.S.C. 324, 334, 611a, 1844(b) and (c), 3105(c) (2) and 3106(a). Federal Deposit Insurance Corporation: 12 U.S.C. 93a, 1818, 1881-84, 3401-22. Office of the Comptroller of the Currency: 12 U.S.C. 93a, 1818, 1881-84, 3401-22. Office of Thrift Supervision: 12 U.S.C. 1463 and 1464. National Credit Union Administration: 12 U.S.C. 1766(a), 1786(q). Financial Crimes Enforcement Network: 31 U.S.C. 5318(g). Information collected on this report is confidential (5 U.S.C. 552(b)(7) and 552a(k)(2), and 31 U.S.C. 5318(g)). The Federal financial institutions regulatory agencies and the U.S. Departments of Justice and Treasury may use and share the information. Public reporting and recordkeeping burden for this information collection is estimated to average 36 minutes per response, and includes time to gather and maintain data in the required report, review the instructions, and complete the information collection. Send comments regarding this burden estimate, including suggestions for reducing the burden, to the Office of Management and Budget, Paperwork Reduction Project, Washington, DC 20503 and, depending on your primary Federal regulatory agency, to Secretary, Board of Governors of the Federal Reserve System, Washington, DC 20551; or Assistant Executive Secretary, Federal Deposit Insurance Corporation, Washington, DC 20429; or Legislative and Regulatory Analysis Division, Office of the Comptroller of the Currency, Washington, DC 20219; or Office of Thrift Supervision, Enforcement Office, Washington, DC 20552; or National Credit Union Administration, 1775 Duke Street, Alexandria, VA 22314; or Office of the Director, Financial Crimes Enforcement Network, Department of the Treasury, 2070 Chain Bridge Road, Vienna, VA 22182.

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 suspected or known criminal violations and suspicious activities 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 or any constitution, law, or regulation of any State or political subdivision thereof, for such disclosure or for any failure to notify the person involved in the transaction or any other person of such 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. 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.

3. 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:

   FinCEN, Detroit Computing Center, P.O. Box 33980, Detroit, MI 48232

2. For items that do not apply or for which information is not available, leave blank.

3. Complete each suspicious activity report in its entirety, even when the suspicious activity report is a corrected or supplemental report.

4. Do not include 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 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 complete an item (for example, to report an additional suspect or witness), a copy of the page containing the item should be used to provide the information.

6. Financial institutions are encouraged to provide copies of suspicious activity reports to state and local authorities, where appropriate.