



8-2005

## Community Bank Anti-Money Laundering Compliance

Peter G. Jahner

[How does access to this work benefit you? Let us know!](#)

Follow this and additional works at: <https://commons.und.edu/theses>

---

### Recommended Citation

Jahner, Peter G., "Community Bank Anti-Money Laundering Compliance" (2005). *Theses and Dissertations*. 4886.

<https://commons.und.edu/theses/4886>

This Independent Study is brought to you for free and open access by the Theses, Dissertations, and Senior Projects at UND Scholarly Commons. It has been accepted for inclusion in Theses and Dissertations by an authorized administrator of UND Scholarly Commons. For more information, please contact [und.common@library.und.edu](mailto:und.common@library.und.edu).

**COMMUNITY BANK ANTI-MONEY LAUNDERING COMPLIANCE**

By:

Peter Gerald Jahner  
University of North Dakota  
Grand Forks, ND

An Independent Study  
In Partial Fulfillment of the Requirements for the Degree of  
Master of Business Administration

Submitted to:

James P. Haskins, Ph. D.  
Assistant Professor  
Department of Finance  
College of Business and Public Administration  
University of North Dakota  
Grand Forks, ND

Fall 2005

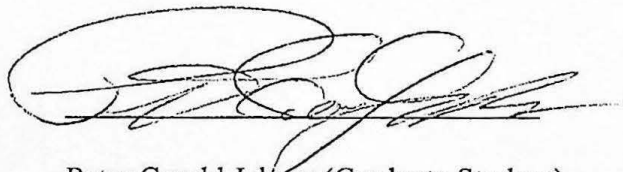
## PERMISSION

Title: Community Bank Anti-Money Laundering Compliance

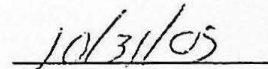
Department: Finance

Degree: Master of Business Administration

In presenting this independent study in partial fulfillment of the requirements for a graduate degree for the University of North Dakota, I agree that the library of this University shall make it freely available for inspection. I further agree that permission for extensive copying for scholarly purposes may be granted by the professor who supervised my independent study work or, in his absence, by the chairperson of the department or the dean of the Graduate School. It is understood that any copying or publication or other use of this independent study or part thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to the University of North Dakota in any scholarly use which may be made of any material in my independent study.



Peter Gerald Jahner (Graduate Student)



Date

## APPROVAL

I hereby authorize Peter G. Jahner to incorporate all or any of Kirkwood Bank & Trust Co.'s Bank Secrecy Act and U.S. PATRIOT Act policies and procedures into his independent study. The independent study is to be submitted in partial fulfillment of his requirements for the Degree of Master of Business Administration from the University of North Dakota. It is understood that no confidential customer data from Kirkwood Bank & Trust Co. will be allowed to be incorporated into the study.



Gerald P. Willer  
President, Kirkwood Bank & Trust Co.

10-31-05

Date



## APPROVAL

I hereby authorize Peter G. Jahner to incorporate the following proprietary information of Eide Bailly, LLP into his independent study:

- 1.) Bank Secrecy Act Transaction Log
- 2.) Incoming Wire Transfer Order
- 3.) Outgoing Wire Transfer Order
- 4.) Customer Identification Program
- 5.) Office of Foreign Asset Control Policy and attachments

The independent study is to be submitted in partial fulfillment of his requirements for the Degree of Master of Business Administration from the University of North Dakota. It is understood that Eide Bailly, LLP makes no representation as to the accuracy or effectiveness of these documents with the exception to Kirkwood Bank & Trust Co.

Cindy Senff

Cindy Senff  
Senior Compliance Consultant  
Eide Bailly, LLP

10/31/05

Date

## TABLE OF CONTENTS

|  |    |
|--|----|
| Introduction   | 7  |
| Part I. Bank Secrecy Act   | 8  |
| Purchases of Negotiable Instruments  | 9  |
| Wire Transfers in Excess of \$3,000  | 10 |
| Wire Transfer Responsibilities of Originator's Banks                               | 11 |
| Travel Rule Requirement  | 12 |
| Wire Transfer Responsibilities of Beneficiary's Banks                              | 13 |
| Wire Transfer Responsibilities of Intermediary Banks                               | 14 |
| Record Maintenance for Extensions of Credit  | 14 |
| Record Maintenance of Taxpayer Identification Numbers                              | 14 |
| Currency Transaction Reporting   | 15 |
| Multiple Transactions  | 15 |
| CTR Filing Requirements  | 16 |
| Exemptions from CTR Reporting  | 16 |
| Ineligible Businesses  | 18 |
| Exemption Filings and Renewals   | 19 |
| Report of International Transportation of Currency or<br>Monetary Instruments      | 20 |
| Suspicious Activity Reporting  | 21 |
| SAR Filing Time Frame  | 22 |
| SAR Report Confidentiality   | 22 |
| SAR Administration   | 22 |
| Minimum Requirements of A BSA Compliance Program                                   | 23 |
| Part II. U.S. PATRIOT Act  | 26 |
| Customer Information Program for Banks   | 26 |
| Customer Information Required for Opening an Account                               | 28 |
| Exceptions to Customer Information Required for<br>Opening an Account              | 29 |
| CIP Verification Procedures  | 30 |
| Comparison with Government Lists   | 32 |
| Customer Notification  | 33 |
| Special Information Procedures to Deter Money<br>Laundering and Terrorist Activity | 33 |
| When to Contact FinCEN   | 35 |
| Designation of Contact Person  | 35 |
| FinCEN Information Safeguards  | 36 |
| Internal Bank Procedures for FinCEN Information Requests                           | 36 |
| Endnotes   | 38 |
| Bibliography   | 42 |

## INTRODUCTION

In response to the terrorist attacks of September 11, 2001, bank regulators have dramatically increased their oversight over the banking industry to ensure compliance with pre-existing and recently enacted anti-money laundering (AML) regulations. In a joint letter dated April 18, 2005 to the American Bankers Association, the Federal banking agencies and the Financial Crimes Enforcement Network (FinCEN) indicated that banks are being scrutinized as never before in maintaining compliance with AML regulations.<sup>1</sup> Small banks (total assets of less than \$250 million) have struggled with the increased scrutiny by regulators. Between October and December of 2004, seven small banks were given "cease and desist" orders for their failure to comply with AML regulations.<sup>2</sup> As a result, financial institutions appealed to the federal regulatory agencies for consistent uniform examination procedures. The regulatory agencies responded by rolling out a 300-plus page statement of policy for AML compliance on June 30, 2005.<sup>3</sup> Carol A. Van Cleef, a partner in the banking and regulatory affairs practices in the Washington Office of Bryan Cave, indicates that "it will be a challenge for many institutions to live up to what has been put in that manual, if the agencies follow through on what they published. If they hold banks to all these standards, there are many banks that cannot afford a compliance program that will be completely satisfactory."<sup>4</sup>

The purpose of this independent study is to provide small banks with a manual that will assist them in complying with AML regulations, specifically, the Financial Recordkeeping and Reporting of Currency and Foreign Transactions Act of 1970 (Bank Secrecy Act) or (BSA) and the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (PATRIOT Act). However, the contents of the manual alone will not provide the results needed to have a successful ALM program. It is necessary to utilize it in conjunction with appropriate management oversight, training, and resources in order to obtain the desired results. In addition, the manual must be tailored to each individual financial institution based upon their size, location, type(s) of business, and customer base. It is also necessary for the manual to be continually updated by management to account for any



amendments to the AML regulations. The information in this manual reflects information researched from August of 2005 to December of 2005. The manual's content should be applicable for the various types of state and national bank charters.

The AML compliance manual is divided into two sections, the BSA and the PATRIOT Act. Each section will begin with a brief history of the regulation followed by a discussion of each compliance provision. Efforts were made to make the discussion of the regulations user friendly, as colleagues often indicate to me that the regulation verbiage is difficult to understand. I will provide recommendations and practical tools that can be used to comply with the regulations. Recommendations made in this independent study will be based upon my research, past regulatory background as a Federal Deposit Insurance Corporation (FDIC) bank examiner, as well as my experience as a BSA officer for a small community bank located in Bismarck, North Dakota (N.D.). Given the tight compliance budget constraints for small banks, the manual was developed to produce the most cost effective method for AML compliance.

### **BANK SECRECY ACT (BSA)**

The purpose of the BSA is to require United States (U.S.) financial institutions to maintain appropriate records and file certain reports involving currency transactions and a financial institution's customer relationships.<sup>5</sup> The BSA requires the identification of the source, volume, and movement of currency and other monetary instruments transported or transmitted into or out of the U.S., or deposited into financial institutions.<sup>6</sup> The BSA is intended to protect the U.S. financial system from the abuses of financial crimes which include money laundering, terrorist financing, drug trafficking, and other illicit financial transactions. These abuses can have a profound impact on the social and economic well being of the citizens of the U.S.<sup>7</sup>

The BSA consists of two parts: Title I - Financial Recordkeeping and Title II - Reports of Currency and Foreign Transactions. Title I authorizes the Department of Treasury to issue regulations, which require financial institutions to maintain certain records. Title II

directed the Department of Treasury to issue regulations overseeing the reporting of certain transactions by and through financial institutions in excess of \$10,000 into, out of, and within the U.S.<sup>8</sup> The regulations implemented by the Department of Treasury are issued within the provisions of 31 CFR Part 103.<sup>9</sup> CFR is an acronym for code of Federal regulations. Immaterial areas of the BSA, more specifically, CFR 103.34, are not discussed as they pertain to recordkeeping requirements that have been routinely followed by banks since 1973.

## **TITLE 1 – BANK SECRECY ACT - FINANCIAL RECORDKEEPING**

### **Purchases of Negotiable Instruments**

A financial institution may not issue or sell a bank check or draft, cashier's check, money order or traveler's check for \$3,000 or more in currency unless it receives appropriate information required by CFR 103.29. Information must be received for each purchase by any individual, which involves currency in the amounts of \$3,000-\$10,000.<sup>10</sup> If a monetary instrument of these types is purchased with more than \$10,000 in currency, a currency transaction report should be filed. If a purchaser has an account with a financial institution, the following documentation must be retained:

- 1.) The name of the purchaser;
- 2.) The date of the purchase;
- 3.) The type(s) of instrument(s) purchased;
- 4.) The serial number(s) of each of the item(s) purchased; and
- 5.) The amount in dollars of each of the item(s) purchased.<sup>11</sup>

The financial institution must verify the purchaser is a deposit account holder or must verify the individual's identity.<sup>12</sup> If the purchaser does not have an account with the financial institution, the following additional information must also be obtained:

- 1.) The address of the purchaser (PO Box is unacceptable)<sup>13</sup>;
- 2.) The social security number or alien registration of the purchaser;
- 3.) The purchasers date of birth;
- 4.) The type of instrument(s) purchased;



- 5.) The serial number(s) of the instrument(s) purchased; and
- 6.) The amount in dollars of each of the instrument(s) purchased.<sup>14</sup>

The financial institution must verify the purchaser's name and address by examination of a document which is normally accepted in the banking community as a means of identification. All records regarding the purchase of monetary instruments in the amounts between \$3,000 and \$10,000 must be retained by the bank for a period of five years.<sup>15</sup> Training of frontline personnel is critical in order to comply with CFR 103.29. Although not required, computer applications can generate a daily report that will aggregate all deposits and withdrawals by taxpayer identification number for a business day. The program can be utilized to report all cash transactions in excess of \$2,999. The program allows the BSA officer to audit all currency transactions in excess of \$2,999 to ensure that personnel are recognizing applicable transactions. Based upon my experience, Information Technology, Inc. of Lincoln, Nebraska has the capability to provide such a program. Appendix A includes a Bank Secrecy Transaction Log for monetary instruments prepared by the accounting firm of Eide Bailly LLP. The BSA Transaction Log should be provided to all front line personnel who have direct contact with bank customers. The log provides personnel with the requirements needed to comply with CFR 103.29. When completed, the log should be reviewed by the BSA officer for proper completion.

#### **Wire Transfers in Excess of \$3,000**

CFR 103.33 requires recordkeeping requirements for wire transfers in excess of \$3,000. Various recordkeeping rules are required depending on the type of wire transfer transaction. Regardless of whether the bank acts as the originator, intermediary, or beneficiary, the bank must retain either the original or a copy of the required information relating to the payment order.<sup>16</sup> It is important to note that financial institutions cannot perform wire transfer actions unless they obtain the required documentation. Examples of outgoing and incoming wire transfer orders prepared by the accounting firm of Eide Bailly LLP are located in Appendix B. The wire transfer orders include the various

requirements imposed by CFR 103.33. The following regulations need to be complied with for the following different types of wire transfer transactions:

#### **Wire Transfer Responsibilities of Originator's Banks**

- 1.) Bank accepting a payment order as an originating bank from an established customer – the following information is required:
  - a.) The name and address of the originating bank;
  - b.) The amount the payment order;
  - c.) The execution date of the payment order;
  - d.) Any payment instructions received from the originator with the payment order;
  - e.) The identity of the beneficiary's bank;
  - f.) The name and address of the beneficiary;
  - g.) The account number of the beneficiary; and,
  - h.) Any other specific identifier of the beneficiary.<sup>17</sup>
  
- 2.) Bank accepting a payment order as an originating bank from non-established customer (payment order made in person) - Prior to acceptance, the originating bank shall verify the identity of the person placing the order. All non-established customers must be compared against the master list of Specially Designated Nationals and Blocked Persons (SDN list). Refer also to page 32, comparison with government lists for compliance. If accepted, the following information must be obtained:
  - a.) All requirements for an established customer detailed above;
  - b.) Name and address of non-established customer;
  - c.) The type of identification reviewed ( i.e. drivers license);
  - d.) The number of the identification document; and
  - e.) The taxpayer ID number of the individual, or, if none, alien identification number or passport number and country of issuance, or a notation in the record of the lack of such document.<sup>18</sup>

If the originating bank has knowledge that the person placing the order is not the originator, the originator's bank must obtain and retain a record of the originator's taxpayer ID number or, if none, alien identification number or passport number and country of issuance, or a notation in the record of the lack of such document.<sup>19</sup>

- 3.) Bank accepting a payment order as an originating bank from non-established customer (payment order not made in person) - the following information is required to be obtained:
  - a.) All requirements for a customer and non-established customer detailed above;
  - b.) Name and address of person placing the payment order;
  - c.) The taxpayer ID number of the individual placing the order on behalf of the originator, or, if none, the alien identification number or passport number and country of issuance, or a notation in the record of the lack of such document; and,
  - d.) A copy of the method of payment.<sup>20</sup>

The information required by the regulation to be retained by the bank acting as an originating bank must be retrievable by reference to the name of the originator. If the originator is a customer of the bank and has an account used for wire transfers, the information must also be retrievable by account number. All required information must be retained for five years.<sup>21</sup>

### **Travel Rule Requirement**

In addition to the bank originating and receiving funds transfers, a bank must also obtain and retain information on payment orders it accepts as either an originator's or intermediary bank. This requirement is commonly known as the travel rule.<sup>22</sup> For each transmittal order that it accepts as transmitter's financial institution, a financial institution must obtain and retain the following documentation:

- 1.) The name and address of the transmitter;
- 2.) The amount of the transmittal order;



- 3.) The execution date of the order;
- 4.) The identity of the recipient's financial institution;
- 5.) Either the name and address or numerical identifier of the transmitter's financial institution;
- 6.) The name and address of the recipient;
- 7.) The account number of the recipient; and,
- 8.) Any payment instructions received from the transmitter with the transmittal order.<sup>23</sup>

#### **Wire Transfer Responsibilities of Beneficiary's Banks**

- 1.) Beneficiaries who are established customers – For each payment order that it accepts as a beneficiary bank, the bank must retain the original or copy of the payment order.<sup>24</sup>
- 2.) Beneficiaries who are non-established customers – For each payment order that it accepts as a beneficiary bank, the bank must verify the identity of the person who receives the proceeds. The bank must obtain the same information on the beneficiary as required above for a non-established customer originating a payment order.<sup>25</sup>
- 3.) Beneficiary who are non-established customers and are not present to receive funds – If funds are distributed via the mail or other method, a copy of the check or other method of payment must be retained. In addition, the name and address of where the payment was sent must be retained.<sup>26</sup>

When receiving funds on behalf of a beneficiary, information must be able to be retrieved by the financial institution by reference to the name of the beneficiary.<sup>27</sup> If the beneficiary is an established customer, the information must be retrievable by account number.<sup>28</sup> The information must be retained for five years.<sup>29</sup>

### **Wire Transfer Responsibilities of Intermediary Banks**

An intermediary is neither the originator or the beneficiary bank. The intermediary bank will receive a payment order from an originating bank and request to forward it to the beneficiary bank. An example of an intermediary bank would be a correspondent bank forwarding a wire transfer request to a foreign country from an originating bank who received the request from a customer. In this case, the intermediary bank must retain a copy of the payment order only.<sup>30</sup> It is important to note that the travel rule discussed above also applies to banks acting as intermediaries.

### **Record Maintenance for Extensions of Credit**

The BSA requires each financial institution to retain a record of each extension of credit (loan) in an amount in excess of \$10,000, unless the extension of credit is secured by real property. Information retained should include the name and address of the person to whom the extension of credit is made, the amount, the nature or purpose, and the date of the extension of credit.<sup>31</sup>

### **Record Maintenance of Taxpayer Identification Numbers**

A bank must obtain a taxpayer identification number for each deposit account opened within 30 days from which the transaction occurred. If more than one name is on the account, an institution must obtain the taxpayer ID number of the person who has a financial interest in the account.<sup>32</sup> For example, a non-individual retirement account set up as a "payable on death" account does not need the taxpayer ID number of the future beneficiary. There are few exemptions for obtaining taxpayer ID numbers, most notably, accounts opened under the name of a federal or state governmental authority.<sup>33</sup> Although situations can arise where a taxpayer ID number may not be available when an account is opened, an internal bank policy of not opening an account without the taxpayer ID number for all account holders is recommended. A policy that requires a taxpayer ID number prior to opening an account will: prevent any future violations of law with this section, allow for proper information to be forwarded to the Internal Revenue Service (IRS), and will assist the BSA officer with reporting requirements. Based upon my past experience with FDIC bank examinations, a financial institution should maintain a list of



all individuals for whom they do not have a taxpayer ID number. In addition, a review of the entire customer data base should be conducted on a semiannual basis to ensure all customer taxpayer ID numbers are retained.

## **TITLE II – REPORTS OF CURRENCY AND FORETGN TRANSACTIONS**

### **Currency Transaction Reporting**

31 CFR Part 103.22 requires financial institutions to file Financial Crimes Enforcement Network (FinCEN) Form 104 for each deposit, withdrawal, exchange of currency or other payment or transfer, by , through or to such financial institution which involves a transaction in currency of more than \$10,000.<sup>34</sup> FinCEN Form 104 is also known as a currency transaction report (CTR). A copy of Form 104 is located in Appendix C with instructions as to how to complete the form. Proper completion of Form 104 is critical. Incorrect completion can subject a financial institution to informal and formal enforcement actions as well as civil money penalties. There is extensive literature available regarding Form 104, and its proper completion.

### **Multiple Transactions**

Multiple currency transactions shall be treated as a single transaction if the financial institution has knowledge that they are by or on behalf of any person and result in either cash in or cash out totaling more than \$10,000 during any one business day.<sup>35</sup> Deposits made at night or over a weekend or holiday shall be treated as if received on the next business day following the deposit.<sup>36</sup> Transactions at all branches of the financial institution must be aggregated when determining whether a multiple transaction occurred.<sup>37</sup> A bank is required to use reasonable efforts to identify all multiple transaction aggregations that exceed \$10,000.<sup>38</sup>

If a financial institution has one or more branches, it is imperative that a BSA computer software program be installed that integrates with the bank's main computer system to satisfy the "reasonable efforts" test. A software program of this type has the capability to generate a daily report that aggregates all deposits and withdrawals by taxpayer identification number for a business day. For example, an individual could deposit

\$5,000 in cash in the morning at the main office and deposit \$6,000 in cash in the afternoon at a branch office. Without the appropriate software, the multiple transaction would not be detected. The program must include deposits and withdrawals that occur at all of the financial institution's branches. Based upon my past experience with FDIC bank examinations, the daily report generated should be tested for accuracy on a periodic basis. Based upon my experience, Information Technology, Inc. of Lincoln, Nebraska has the capability to provide such a program.

### **CTR Filing Requirements**

FinCEN Form 104 must be filed by a financial institution within fifteen days following the day on which the reportable transaction occurred. Institutions using magnetic media to file reports must file within twenty-five days from the date of the transaction.<sup>39</sup> Each report must be retained by the institution for a period of five years from the date of the report.<sup>40</sup> FinCEN provides the bank regulatory agencies with each institutions record of submitting the reports within the prescribed time frames. Regulatory agencies review these reports to determine an institution's compliance with the filing requirements. The bank's BSA policy must include time filing requirements to ensure the CTRs are submitted in a timely manner.

### **Exemptions from CTR Reporting**

CFR 103.22 provides certain exemptions from the reporting of CTRs. The Money Laundering Suppression Act of 1994, which modified the BSA, established a two-phase exemption process: "Phase I" and "Phase II" exemptions.<sup>41</sup> "Phase I" exemptions include:

- 1.) A bank, to the extent of its domestic operations
- 2.) A department or agency of the U.S., of any state, or of any political subdivision of any state;
- 3.) Any entity exercising governmental authority within the U.S. (includes District of Columbia, Territories, and Native American tribal lands);

- 4.) Any entity (to the extent of its domestic operations), other than a bank, whose common stock or analogous equity interests are listed on the New York, American, or NASDAQ stock exchanges. Stock or interests listed under the separate "Nasdaq Small-Cap issues are not exempt from reporting requirements; or,
- 5.) A subsidiary, other than a bank, which is owned at least fifty-one percent, and is controlled, by a listed company.<sup>42</sup>

"Phase II" exemptions include:

- 1.) Non-listed business - A non-listed business includes commercial enterprises that do not have more than fifty percent of the business gross revenues derived from certain ineligible businesses.<sup>43</sup> To the extent of its domestic operations, any business that is a "non-listed business" that meets the following requirements:
  - a.) has maintained a transaction account at the bank for at least 12 months, and;
  - b.) frequently engages in transactions in currency with the bank in excess of ten thousand dollars; and
  - c.) is incorporated or organized under the laws of the U.S. or any state, or is registered as and eligible to do business within the U.S. or any state.<sup>44</sup>

Corporations, partnerships, limited-liability companies, and sole proprietorships are all eligible to be a non-listed business.<sup>45</sup> When determining whether or not a customer meets the definition of a non-listed business, all accounts held at the bank for the customer should be aggregated to determine if an exemption is warranted. It is important to review the purpose of all of the customer's accounts when determining whether they meet the definition of a non-listed business. Individuals who own several different business interests with separate accounts are generally not eligible to be treated as a single account.<sup>46</sup> However, it may be necessary to treat these accounts as one account if the



bank has knowledge that funds are being intermingled amongst various business interests.<sup>47</sup> Multiple businesses operating under one tax payer ID number are to be treated as a single account according to my personal conversation with Marie Morris from the Department of Treasury.<sup>48</sup> In addition, my conversation with Morris revealed that a non-listed business that experiences at least eight reportable transactions in a calendar year would meet the definition of "frequently engages."<sup>49</sup>

- 2.) Payroll Customer - An account set up by a business for payroll purposes only. It includes any exempt person not covered under the exempt person definition. Payroll customers must meet the following requirements to obtain an exempt status:
  - a.) Has maintained a transaction account at the bank for at least 12 months, and;
  - b.) Operates a firm that regularly withdraws more than \$10,000 in order to pay its U.S. employees; and
  - c.) Is incorporated or organized under the laws of the U.S. or any state, or is registered as and eligible to do business within the U.S. or any state.<sup>50</sup>

### **Ineligible Businesses**

The following businesses may not be treated as non-listed businesses due to their inherent ability to facilitate illicit activity:

- 1.) Non-bank financial institutions or their agents. The FDIC indicates that the definition includes telegraph companies and money service businesses (currency exchange, check casher, or issuer of monetary instruments in an amount greater than \$1,000 to any person in one day);<sup>51</sup>
- 2.) Purchasers or sellers of motor vehicles of any kind, vessels, aircraft, farm equipment, or mobile homes;
- 3.) Businesses engaging in the practice of law, accountancy, or medicine;
- 4.) Auctioneers;
- 5.) Businesses that charter or operate ships, buses, or aircraft;

- 6.) Gaming of any kind other than licensed pari-mutuel betting at race tracks;
- 7.) Businesses providing investment advisory services or investment banking services;
- 8.) Businesses that engage in real estate brokerage, pawn brokerage, title insurance and real estate closing, and trade union activities, and;
- 9.) Any other activities that may be specified by FinCen.<sup>52</sup>

### **Exemption Filings and Renewals**

Exemptions are filed with FinCEN by completing form TD F 90-22.53 – Designation of Exempt Person. Located in Appendix D is a copy of form TD F 90-22.53 and instructions for its completion. Exemptions for Phase I exemptions need to be filed only once. Initial Phase II exemptions must be filed within 30 days after the date of the first reportable transaction that the institution is asking to be exempted.<sup>53</sup> As long as they meet the exemption requirements, Phase II customers must be renewed and filed every two years.<sup>54</sup> Form TD F 90-22.53 must be refilled by March 15 of the second calendar year following the year in which the exemption was initially granted.<sup>55</sup> Conversations between FDIC Bank Examiner Miranda Swanson on February 19, 2003 revealed that the exemption renewal filings must be received by FinCEN by March 15.<sup>56</sup>

Documentation justifying each Phase I and Phase II exemption is extremely important and should be retained by the BSA officer. For Phase I exemptions, it is acceptable to document that an entity is listed on an accepted stock market by relying on any of the following: a listing published in a newspaper of general circulation, a commonly accepted or published stock symbol guide, or on any public information obtained through the Securities and Exchange Commission (SEC).<sup>57</sup> In determining whether a listed company subsidiary exists, a bank may rely upon: any reasonably authenticated corporate officer's certificate, any reasonably authenticated photocopy of IRS Form 851 for the appropriate tax year, and a person's Annual Report or Form 10-K, as filed with the SEC.<sup>58</sup>



Based upon experience, documentation for Phase II exemptions can include information from an applicable state agency in which the business is operating in. For example, in N.D., the N.D. Secretary of State has the appropriate information to provide evidence that the business is incorporated or organized under the laws of the U.S. or any state, or is registered as and eligible to do business within the U.S. or any state. Documentation of Phase II exemptions should also include bank records which indicate the opening date of an account, and the past eight reportable transactions.

The regulation also requires an annual review of exemptions. A documented review of the information supporting each designation of exempt person must be completed. I have developed a MS Excel® workbook model which provides the BSA Officer with a tool to review whether Phase II exempted customers have had at least eight reportable transactions in the last calendar year. The report also has the ability of determining potential new exemptions. In addition, the model also provides regulatory agencies and auditors with appropriate dates to ensure that CTRs are being completed within the required time frame. Appendix E provides a printout of a hypothetical report from the model. The model should be updated by the BSA officer on a daily basis. When determining new exemptions as well as biennial renewal exemptions, the report can be sorted by name to determine if the eight transaction minimum has been met.

#### **Report of International Transportation of Currency or Monetary Instruments**

CFR 103.23 requires the filing of FinCEN Form 105, "Report of International Transportation of Currency or Monetary Instruments" when a person is involved with the transportation, mailing, or shipping of currency or monetary instruments in excess of \$10,000 at one time out of or into the U.S. The report must be filed within fifteen days from the receipt of the currency or other monetary instruments.<sup>59</sup> A bank is not required to file the report if the currency or other monetary instrument was mailed through the postal service or by common carrier.<sup>60</sup> A copy of Form 105 is located in Appendix F with instructions as to how to complete the form.

### **Suspicious Activity Reporting**

The BSA requires financial institutions to identify and report known or suspected violations of law or/and suspicious transactions related to possible violations of law.<sup>61</sup>

CFR 103.18 requires every financial institution to file with the Treasury Department, a report of any suspicious transaction relevant to a possible violation of law or regulation.<sup>62</sup>

A copy of the Department of Treasury's suspicious activity report (SAR) as well as instructions for proper completion is located in Appendix G. A transaction requires reporting if: it is conducted or attempted by, at, or through the financial institution; it involves or aggregates at least \$5,000 in funds or other assets; and, the bank 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 federal law or regulation or to avoid any transaction reporting requirement under federal law or regulation;
- (ii) The transaction is designed to evade any requirements of the BSA; 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 bank knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.<sup>63</sup>

If the financial institution is either the victim or believes it is a victim of a criminal violation, and the amount exceeds \$25,000, the bank must file a SAR even if they cannot identify a possible suspect.<sup>64</sup> If the suspicious transaction involves an insider of the bank, a SAR must be filed regardless of the amount. An insider is defined as any financial institution director, officer, employee, agent, or any other institutional affiliated party. An institutional affiliated party can be any person who participates in the affairs of the financial institution. They include: shareholders, consultants, independent contractors, attorneys, appraisers, accountants, etc.<sup>65</sup>

A bank is not required to file a SAR for a robbery or burglary committed or attempted that is reported to appropriate law enforcement authorities, or for lost, missing, counterfeit, or stolen securities with respect to which the bank files a report.<sup>66</sup>

### **SAR Filing Time Frame**

A bank is required to file a SAR no later than 30 calendar days after the date of initial detection by the bank of facts that may constitute a basis for filing. If no suspect was identified on the date of the detection of the incident requiring the filing, a bank may delay filing a SAR 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. In situations involving violations that require immediate attention, such as, for example, ongoing money laundering schemes, the bank shall immediately notify, by telephone, an appropriate law enforcement authority in addition to filing a SAR on a timely basis.<sup>67</sup>

### **SAR Report Confidentiality**

A financial institution, director, officer, employee, or agent of the financial institution, who reports a suspicious transaction, cannot notify any person involved in the transaction that a SAR has been reported.<sup>68</sup> If any person is subpoenaed or otherwise requested to disclose information contained in a SAR, except where such disclosure is requested by FinCEN or an appropriate law enforcement or bank supervisory agency, that person cannot produce the SAR or provide any information that would disclose that a SAR has been prepared or filed. If requested, the financial institution must notify FinCEN of any such request and its response.<sup>69</sup> A financial institution should have legal counsel review any request for a reported SAR.

### **SAR Administration**

Proper training of bank employees is also critical in detecting suspicious activity. A training program should include the discussion of, but not be limited to: potential types of suspicious activities, internal procedures for the reporting of suspicious activity, and SAR preparation. Based upon past experiences with regulatory bank examinations,



training should occur no less than two times per year. The retention period for completed SARs is five years. Bank officials must retain all supporting documentation pertaining to the report.<sup>70</sup> All SARs should be reviewed by the bank's board of directors. However, the board is not required to approve the filings prior to their submission. Official board minutes should not include the individual(s) name(s) of the suspect(s). Financial institutions and their directors, officers, employees, and agents are protected from any liability for reporting SARs. Federal Statute 31 U.S.C. 5318(g) provides safe harbor for good faith reporting to authorities.<sup>71</sup>

Bank officials are not required to terminate the relationship with the customer if a SAR is filed. However, the bank may close the customer's account to avoid being the victim of fraud. The filing of the SAR should not be the reason for closing the account; however, the underlying suspicious activity leading to the SAR can be used as the basis for closing the account. Bank counsel may need to be contacted to ensure that correct steps are taken in closing a suspicious account.<sup>72</sup>

### **Minimum Requirements of a BSA Compliance Program**

Federal regulatory agencies established regulations for the minimum requirements of a BSA program as promulgated by the Department of Treasury at 31 CFR Part 103. The regulations are the same for each financial institution regardless of who their primary regulatory agency is. The minimum requirements of a BSA compliance program discussed below are derived from Part 326 of the FDIC Rules and Regulations. A financial institution must develop and provide for the continued administration of a program reasonably designed to assure and monitor compliance with recordkeeping and reporting requirements of the BSA. The compliance program must be written, approved by the bank's board of directors, and noted in the official board minutes.<sup>73</sup> Based upon experience, the program should be reviewed and approved by the board of directors on an annual basis. Part 326.8 requires the bank to establish a program that at a minimum:

- (1) Provide for a system of internal controls to assure ongoing compliance<sup>74</sup> – Content in this manual is designed to provide a system of internal controls to assure ongoing

compliance with the BSA. A recap of the minimum requirements can be viewed at [www.fdic.gov](http://www.fdic.gov) under the FDIC's DSC Risk Manual of Examination Policies. Internal controls are extremely important in the administration of a strong BSA program. Computer applications can be utilized to provide the BSA officer with appropriate tools to monitor day-to-day compliance. For smaller community bank's there is sufficient data available to monitor without a vendor system according to Laurie Bender, senior special anti-money laundering examiner with the Federal Reserve.<sup>75</sup> She indicates that "as small banks grow, there is a point where clearly the options and the interests and benefits of a vendor system could occur."<sup>76</sup> Computer applications alone will not ensure strong internal controls. Appropriate review of these applications is important. Finally, frequent discussions between the BSA officer and frontline personnel regarding BSA issues will also lead to a successful system of internal controls.

As part of a system for internal controls, federal regulatory agencies are also requiring financial institutions to develop a risk assessment for all major lines, products, and services offered by the financial institution. The risk assessment should focus on the following areas related to the financial institution: size and location, accounts and services offered, methods for opening accounts, customer base, operations, and overall level of risk represented.<sup>77</sup>

(2) Provide for independent testing for compliance to be conducted by bank personnel or an outside party – The independent testing should be completed by a qualified internal audit staff, or outsourced to accountants or consultants with strong qualifications. The results should be reviewed and approved by the bank's board of directors. Quick action should be taken by management to address any deficiencies noted in the testing results. Regulatory agencies recommend the testing to occur on an annual basis; however, it is not required by the regulation. It is not acceptable for an institution's BSA officer or any other person involved with BSA to perform the independent review.<sup>78</sup> Due to the complexity of the regulation, it is strongly recommended that a bank outsource the testing if it does not have a formal internal audit department. In addition, it is recommended that testing occur on an annual basis to allow program errors to be discovered quickly.



Testing must include procedures related to high-risk accounts and activities. Based upon experience, the independent testing should include auditing for compliance with the customer identification program. Testing should be sufficient to verify compliance with the financial institution's anti-money laundering program.<sup>79</sup>

(3) Designate an individual or individuals responsible for coordinating and monitoring day-to-day compliance with BSA – The board of directors must designate a senior official with the authority to monitor the day-to-day compliance. The official should be approved by the board on an annual basis. The BSA officer must have the ability to make and enforce BSA policies.<sup>80</sup> It is imperative that the BSA officer receive the necessary training to allow him or her the ability to fulfill AML requirements.

(4) Provide training for appropriate personnel – BSA training is vital to a successful program. Internal training as well as external training is recommended. Training should be given to all new employees prior to them beginning their duties as an employee. Based upon my past experience with regulatory examinations, training should occur at a minimum of twice a year. The training sessions should be documented as follows: date of training, signatures of attendees, as well as topics discussed. The FDIC recommends that the scope of the training include:

- a.) The bank's BSA policies and procedures;
- b.) Discussion of the definition of money laundering;
- c.) How to identify money laundering;
- d.) Types of suspicious activity and examples;
- e.) Customer identification policies;
- f.) Internal policies for CTR and SAR filings;
- g.) Procedures for implementing new BSA procedures; and,
- h.) OFAC policies and procedures.<sup>81</sup>

Small banks' training programs usually fail to address methods to address illegal activities as well as the need to understand the sources, and the beneficial ownership of

funds in accounts.<sup>82</sup> The central question for bank personnel to determine is whether the account is being used for its intended purpose.<sup>83</sup> An additional area of concern for small banks is staying abreast of BSA changes. Small financial institutions usually have small compliance staffs that have other duties. Training resources are available through state and national banking associations, outside vendors, trade groups, or they can be internally developed.<sup>84</sup>

## **U.S. PATRIOT ACT**

On June 9, 2003, The Department of the Treasury, through the Financial Crimes Enforcement Network (FinCEN), together with the federal financial institution regulatory agencies, jointly enacted a final rule to implement Section 326 of the PATRIOT Act.<sup>85</sup> The PATRIOT Act requirements were added as new provisions of the BSA under Section 103.121. The regulation, at a minimum, requires financial institutions to implement reasonable procedures to verify the identity of any person seeking to open an account; maintain records of the information used to verify the person's identity; and determine whether the person appears on any lists of known or suspected terrorists or terrorist organizations provided to the financial institution by any government agency. These provisions are intended to facilitate the prevention, detection, and prosecution of international money laundering and the financing of terrorism.<sup>86</sup>

In addition to the customer identification regulations required by Section 326, the Department of Treasury implemented Section 314 of the PATRIOT Act that adds sections 103.100 and 103.110 to the BSA regulations.<sup>87</sup> These sections establish procedures that encourage information sharing between governmental authorities and financial institutions, and among financial institutions themselves. Both Section 326 and 314 requirements will be discussed below.

### **Customer Identification Programs for Banks**

CFR 103.121 requires a financial institution's customer identification program (CIP) to meet five main requirements. The regulation requires a bank to establish: a written CIP,

identity verification procedures, recordkeeping requirements, a method to compare information with government lists, and customer notification procedures.<sup>88</sup> The five requirements are discussed below:

Written Customer Identification Program - a financial institution must implement a written Customer Identification Program (CIP) appropriate for its size and type of business. The CIP program must be included within the bank's anti-money laundering program, and be included under the "umbrella" of its overall BSA/AML program.<sup>89</sup>

Appendix H includes an example of a written CIP. The program was prepared by the accounting firm of Eide Bailly, LLP. It is important to note that the program is provided as an example only. The program may or may not address a financial institution's needs depending upon its size, location, type(s) of business done, as well as its customer base.<sup>90</sup>

Identity Verification Procedures - According to CFR 103.121, the bank's CIP must include risk-based procedures for verifying the identity of each customer in a reasonable and practicable manner. The procedures must enable the bank to form a reasonable belief that it knows the true identity of each customer. These procedures must be based on the bank's assessment of the relevant risks associated with: the various types of accounts maintained by the bank, the various methods of opening accounts provided by the bank, the various types of identifying information available, and the bank's size, location, and customer base.<sup>91</sup>

Although the regulation has several definitions of terms detailed in CFR 103.21, it is very important to understand the definitions of the following three terms as they relate to the regulation.

Definition of an Account - means a formal banking relationship established to provide or engage in services, dealings, or other financial transactions including a deposit account, a transaction or asset account, a credit account, or other extension of credit. Account also includes a relationship established to provide a safety deposit box or other safekeeping services, or cash management, custodian, and trust services.<sup>92</sup>



Account does not include:

- 1.) A product or service where a formal banking relationship is not established with a person, such as check-cashing, wire transfer, or sale of a check or money order;
- 2.) An account that the bank acquires through an acquisition, merger, purchase of assets, or assumption of liabilities; or
- 3.) An account opened for the purpose of participating in an employee benefit plan established under the Employee Retirement Income Security Act of 1974.<sup>93</sup>

Definition of a Customer – a customer is a person that opens a new account; and an individual who opens a new account for:

- 1.) an individual who lacks legal capacity, such as a minor; or
2. an entity that is not a legal person, such as a civic club.

A customer does not include a financial institution regulated by a Federal functional regulator or a bank regulated by a state bank regulator, or a person that has an existing account with the bank, provided that the bank has a reasonable belief that it knows the true identity of the person.<sup>94</sup>

Definition of a Person - A U.S. citizen; or a person other than an individual (such as a corporation, partnership or trust) that is established or organized under the laws of a state or the U.S.<sup>95</sup>

### **Customer Information Required for Opening an Account**

The CIP must contain procedures for opening an account that specify the identifying information that will be obtained from each customer. The bank must obtain, at a minimum, the following information from the customer prior to opening an account:

- 1.) Name;
- 2.) Date of birth, for an individual;
- 3.) Address, which shall be:
  - (a) For an individual - a residential or business street address;
  - (b) For an individual who does not have a residential or business street address -an Army Post Office (APO) or Fleet Post Office (FPO) box number, or the residential or



business street address of next of kin or of another contact individual; or

(c) For a person other than an individual (such as a corporation, partnership, or trust) - a principal place of business, local office, or other physical location; and

4.) Identification number, which shall be:

(a) For a U.S. person, a taxpayer identification number; or

(b) For a non-U.S. person, one or more of the following: a taxpayer identification number; passport number and country of issuance; alien identification card number; or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard.<sup>96</sup>

When opening an account for a foreign business or enterprise that does not have an identification number, the bank must request alternative government-issued documentation certifying the existence of the business or enterprise.<sup>97</sup> Appendix H includes example forms of a new customer account application, and a new business account application, which have all of the required information in the regulation.

#### **Exceptions to Customer Information Required for Opening an Account**

Persons applying for a taxpayer identification number - Instead of obtaining a taxpayer identification number from a customer prior to opening the account, the CIP may include procedures for opening an account for a customer that has applied for, but has not received, a taxpayer identification number. In this case, the CIP must include procedures to confirm that the application was filed before the customer opens the account and to obtain the taxpayer identification number within a reasonable period of time after the account is opened.<sup>98</sup> Although there are always instances where exceptions can be made, it is recommended that taxpayer identifications are required prior to opening a new account.

Credit card account - In connection with a customer who opens a credit card account, a bank may obtain the identifying information about a customer by acquiring it from a third-party source prior to extending credit to the customer.<sup>99</sup>

## CIP Verification Procedures

The CIP must contain procedures for verifying the identity of the customer within a reasonable time after the account is opened. The procedures must describe when the bank will use documents, non-documentary methods, or a combination of both methods.<sup>100</sup> Verification of the documents prior to opening the account is recommended.

Verification through documents - For a bank relying on documents, the CIP must contain procedures that indicate which documents the bank will use. Recommended documents include:

- 1.) For an individual, an unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as a driver's license or passport; and
- 2.) For a person other than an individual (such as a corporation, partnership, or trust), documents showing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement, or trust instrument.<sup>101</sup>

Verification through non-documentary methods - For a bank relying on non-documentary methods, the CIP must contain procedures that describe the non-documentary methods the bank will use. These methods may include: contacting a customer; independently verifying the customer's identity by obtaining a credit report or other public database such as check systems or other sources; checking references with other financial institutions; or, obtaining a financial statement<sup>102</sup>.

The bank's non-documentary procedures must address situations where an individual is unable to present an unexpired government-issued identification document that bears a photograph or similar safeguard; the bank is not familiar with the documents presented; the account is opened without obtaining documents; the customer opens the account without appearing in person at the bank; and where the bank is otherwise presented with circumstances that increase the risk that the bank will be unable to verify the true identity of a customer through documents.<sup>103</sup>

Additional verification for certain customers - The CIP must address situations where, based on the bank's risk assessment of a new account opened by a customer that is not an individual, the bank will obtain information about individuals with authority or control over such account, including signatories, in order to verify the customer's identity. This verification method applies only when the bank cannot verify the customer's true identity using the verification methods described above.<sup>104</sup>

Lack of verification - The CIP must include procedures for responding to circumstances in which the bank cannot form a reasonable belief that it knows the true identity of a customer. These procedures should describe:

- 1.) When the bank should not open an account;
- 2.) The terms under which a customer may use an account while the bank attempts to verify the customer's identity;
- 3.) When the bank should close an account, after attempts to verify a customer's identity have failed; and
- 4.) When the bank should file a SAR in accordance with applicable law and regulation.<sup>105</sup>

Recordkeeping - The CIP must include procedures for making and maintaining a record of all information obtained. At a minimum, the record must include:

- 1.) All identifying information about a customer obtained;
- 2.) A description of any document that was relied on, noting the type of document, any identification number contained in the document, the place of issuance and, if any, the date of issuance and expiration date;
- 3.) A description of the methods and the results of any measures undertaken to verify the identity of the customer, and
- 4.) A description of the resolution of any substantive discrepancy discovered when verifying the identifying information obtained.<sup>106</sup>

The CIP may include procedures specifying when a bank will rely on the performance by another financial institution (including an affiliate) for the performance of CIP procedures.<sup>107</sup> An example of CIP reliance is a loan participation purchased from



another financial institution. The requirements for CIP reliance are as follows:

- 1.) Such reliance must be reasonable under the circumstances;
- 2.) The other financial institution is regulated by a Federal functional regulator; and
- 3.) The other financial institution enters into a contract requiring it to certify annually to the bank that it has implemented its anti-money laundering program, and that it will perform (or its agent will perform) the specified requirements of the bank's CIP.<sup>108</sup>

Based upon my experience, situations can arise where it is difficult to verify a customer's identity. However, it is strongly recommended that the account not be opened unless all the required portions of the application are properly completed. A customer verification form is included with the CIP program in Appendix G. Each employee who is responsible for obtaining the proper information should ensure completion of the application and verification. A second employee should complete a final review for any errors that have occurred in obtaining the appropriate information. Once the final review has been completed, the bank's computer system should be updated to designate the customer as "ID verified". The "ID verified" designation will allow all bank employees to know whether or not a customer has been properly identified.

Record Retention - The bank must retain the customer information and verification methods for five years after the date the account is closed or, in the case of credit card accounts, five years after the account is closed or becomes dormant.<sup>109</sup>

### **Comparison with Government Lists**

The CIP must include procedures for determining whether the customer appears on any list of known or suspected terrorists or terrorist organizations issued by any Federal government agency.<sup>110</sup> The procedures must require the bank to make such a determination within a reasonable period of time after the account is opened.<sup>111</sup> A list of known or suspected terrorists or terrorist organizations is established and continually updated by the Office of Foreign Assets Control (OFAC) of the Department of Treasury.

The list of Specially Designated Nationals (SDN list) contains an alphabetical master list of Specially Designated Nationals and Blocked Persons suspected terrorists. The list can be viewed at [www.treas.gov/offices/enforcement/ofac/sdn/](http://www.treas.gov/offices/enforcement/ofac/sdn/). If bank personnel have internet access, the aforementioned OFAC website should be made available to all employees who open new accounts. This will allow all new customers to be compared against the OFAC list prior to opening an account. If bank personnel do not have internet access, a current SDN list must be made available to them.

Federal regulatory agencies also recommend that the bank's entire customer database be scanned against the OFAC list on a periodic basis. According to Dennis Dahl, Field Supervisor for the FDIC, such a scan ensures that existing customers are not included on the OFAC list subsequent to when the customer opened their account at the institution.<sup>112</sup> Dahl recommends that the scan of the customer database be updated anytime there is an update to the OFAC list, but no less than annually.<sup>113</sup> Computer software is widely available to perform this function. Based upon my experience, Information Technology, Inc. of Lincoln, Nebraska has the capability to provide such software. Financial institutions that do not purchase this software should have all employees periodically review the list to ensure a current customer is not on the list. Whether or not an institution purchases the software depends on the bank's size, location, and customer base.

**Customer Notification** - The CIP must include procedures for providing bank customers with adequate notice that the bank is requesting information to verify their identities. Depending upon the manner in which the account is opened, a bank may post a notice in the lobby or on its website, include the notice on its account applications, or use any other form of written or oral notice.<sup>114</sup> A sample notice is located in Appendix G.

#### **Special Information Sharing Procedures to Deter Money Laundering and Terrorist Activity**

Section 314 of the PATRIOT Act added section 103.100 to the BSA regulations.<sup>115</sup> This section establishes procedures that encourage information sharing between governmental authorities and financial institutions. Section 103.100 establishes a mechanism for law

enforcement to communicate names of suspected terrorists and money launderers to financial institutions in return for securing the ability to promptly locate accounts and transactions involving those suspects. When a federal law enforcement agency is seeking information regarding terrorist activity or money laundering, they must request the information from FinCEN. FinCEN, in turn, requests the information from financial institutions. Upon receiving an information request from FinCEN, a financial institution shall expeditiously search its records to determine whether it maintains or has maintained any account for, or has engaged in any transaction with, each individual, entity, or organization named in the request.<sup>116</sup> Generally, a financial institution must respond to FinCEN within a two week period if there is a positive match. However, individual requests can have different deadline dates.<sup>117</sup> A financial institution may contact the Federal law enforcement agency named in the information request provided to the institution by FinCEN with any questions relating to the scope or terms of the request.

On March 1, 2005, FinCEN released the Secure Information Sharing System (SISS) for requesting Section 314(a) information. Typically, financial institutions receive biweekly email notifications about new information that has been posted on the SISS web site for their review. Institutions must register to have access to the site. Registration can be completed at [www.fincen.gov/314a/](http://www.fincen.gov/314a/).<sup>118</sup> For institutions who do not utilize email, FinCEN provides the information via facsimile.<sup>119</sup> The SISS system can only be assessed by the financial institution's designated 314(a) points of contact. If a third-party vendor or product is used to conduct searches, the institution is still required to log on and review the information on the SISS. Any changes to the Section 314(a) point of contact must be made through the quarterly call report.<sup>120</sup>

Unless indicated in the information request, a financial institution shall only be required to search its records for the preceding twelve months for:

- 1.) Deposit account records
- 2.) Funds transfer records
- 3.) Sales of monetary instruments (purchaser only);
- 4.) Loan records;



- 5.) Trust department records;
- 6.) Securities records (purchases, sales, safekeeping, etc.)
- 7.) Commodities, options, and derivatives
- 8.) Safe deposit box rentals (but only if searchable electronically).<sup>121</sup>

Frequently asked questions concerning the 314(a) process can be viewed at [www.fincen.gov/314a/help.php](http://www.fincen.gov/314a/help.php).

### **When to Contact FinCEN**

If a financial institution identifies an account or transaction identified with any individual, entity, or organization named in a request from FinCEN, it shall report to FinCEN, in the manner and in the time frame specified in FinCEN's request, the following information:

- 1.) The name of such individual, entity, or organization;
- 2.) The number of each such account, or in the case of a transaction, the date and type of each such transaction; and
- 3.) Any Social Security number, taxpayer identification number, passport number, date of birth, address, or other similar identifying information provided by the individual, entity, or organization when each such account was opened or each such transaction was conducted.<sup>122</sup>

### **Designation of contact person**

A financial institution must designate one person to be the point of contact at the institution regarding FinCEN requests.<sup>123</sup> Due to the BSA officer's knowledge with the bank's overall anti-money laundering program, it is recommended that the BSA officer be the point of contact for FinCEN requests. When requested by FinCEN, a financial institution shall provide FinCEN with the name, title, mailing address, e-mail address, telephone number, and facsimile number of such person, in such manner as FinCEN may request. A financial institution that has provided FinCEN with contact information must promptly notify FinCEN of any changes to such information.<sup>124</sup>

### **FinCEN Information Safeguards**

FinCEN requests are confidential, and the institution must protect the security of the requests.<sup>125</sup> A financial institution shall not use information provided by FinCEN for any purpose other than:

- 1.) Reporting to FinCEN;
- 2.) Determining whether to establish or maintain an account or to engage in a transaction; or
- 3.) Assisting the financial institution in complying with any requirement of the regulation.<sup>126</sup>

A financial institution shall not disclose to any person, other than FinCEN or the Federal law enforcement agencies, the fact that FinCEN has requested or has obtained information, except to the extent necessary to comply with such an information request.

Each financial institution must maintain adequate procedures to protect the security and confidentiality of requests from FinCEN. Compliance is satisfied if the financial institution adheres to the requirements of section 501 of the Gramm-Leach-Bliley Act (15 U.S.C. 6801), with regard to the protection of its customers' nonpublic personal information.<sup>127</sup>

### **Internal Bank Procedures for FinCEN Information Requests**

A bank should adopt an Office of Foreign Assets Control Policy which outlines the duties required under Section 314 of the PATRIOT Act. The policy should be reviewed and approved by the board on an annual basis. In addition, procedures for OFAC and PATRIOT Act information requests should be incorporated into the policy. An example of an OFAC policy is located in Appendix I. The policy was prepared by the accounting firm of Eide Bailly, LLP. It is important to note that the program is provided as an example only. The program may or may not address a financial institution's needs depending upon its size, location, type(s) of business done, as well as its customer base.<sup>128</sup>

Computer software systems are available to help search a financial institution's data base for Section 314(a) requests. Based upon my experience, Information Technology, Inc. of Lincoln, Nebraska has the capability to provide such a program. The system must be able to search the institution's current customer list as well as all customers of the bank for the last year. For this reason, banks must not remove customers from their computer system after an account is closed until after one year from the closing date. Also, various departments may not be on the bank's main computer system.

Financial institutions should keep a log of all Section 314(a) requests received and any positive matches identified and reported to FinCEN. Documentation that all required searches were performed is important for audit and regulatory purposes. Appendix I includes an OFAC Exception Log and a FinCEN Information Request Log designed to track all requests. Based upon my past experience with bank regulators, unless a bank adequately secures and protects the confidentiality of the reports, any information received by FinCEN should be destroyed after the research is completed. Due to the confidential nature of the information received from FinCEN, only the personnel needed to conduct the search should have access to the information.



## ENDNOTES

- 
- <sup>1</sup> Susan Schmidt Bies, Julie L. Williams, Donna E. Powell, James E. Gilleran, and William J. Fox to the American Bankers Association, 18 April 2005, [www.aba.com](http://www.aba.com).
- <sup>2</sup> Dennis Sullivan, BSA Violations Cause Heads to Roll at Small Banks, *Regulatory Risk Monitor*, 24 January 2005, 1:2.
- <sup>3</sup> Cocheo, Steve, "BSA exam procedures bring uniformity...but at a price", *ABA Banking Journal*, October 2005, 52.
- <sup>4</sup> *Ibid.*, 54, 56.
- <sup>5</sup> "Introduction to the Bank Secrecy Act", Federal Deposit Insurance Corporation DSC Risk Management Manual of Examination Policies, December 2004, 8.1-1.
- <sup>6</sup> "Introduction to FFIEC BSA/AML Materials", Federal Financial Institutions Examination Council, July 2005, 6.
- <sup>7</sup> *Ibid.*, 1.
- <sup>8</sup> "Introduction to the Bank Secrecy Act", Federal Deposit Insurance Corporation DSC Risk Management Manual of Examination Policies, December 2004, 8.1-1.
- <sup>9</sup> *Ibid.*, 1.
- <sup>10</sup> U.S. 31 CFR 103.29, "Purchases of bank checks and drafts, cashier's checks, money orders, and travelers checks", FDIC Rules and Regulations, Miscellaneous Statutes and Regulations, [www.fdic.gov](http://www.fdic.gov)
- <sup>11</sup> *Ibid.*
- <sup>12</sup> *Ibid.*
- <sup>13</sup> "FinCEN Recordkeeping Requirements", Federal Deposit Insurance Corporation DSC Risk Management Manual of Examination Policies, December 2004, 8.1-6.
- <sup>14</sup> U.S. 31 CFR 103.29, "Purchases of bank checks and drafts, cashier's checks, money orders, and travelers checks", FDIC Rules and Regulations, Miscellaneous Statutes and Regulations, [www.fdic.gov](http://www.fdic.gov).
- <sup>15</sup> *Ibid.*
- <sup>16</sup> U.S. 31 CFR 103.33, "Records to be made and retained by financial institutions", FDIC Rules and Regulations, Miscellaneous Statutes and Regulations, [www.fdic.gov](http://www.fdic.gov).
- <sup>17</sup> *Ibid.*
- <sup>18</sup> *Ibid.*
- <sup>19</sup> *Ibid.*
- <sup>20</sup> "Originator's Bank", *Kirchman Regulatory Service*, January 2004, 3.6.7.
- <sup>21</sup> "Retrieveability", FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual, June 23, 2005, 64.
- <sup>22</sup> "The Travel Rule", *Kirchman Regulatory Service*, January 2004, 3.6.9.
- <sup>23</sup> *Ibid.*
- <sup>24</sup> *Ibid.*, 3.6.8.
- <sup>25</sup> *Ibid.*
- <sup>26</sup> U.S. 31 CFR 103.33, "Records to be made and retained by financial institutions", FDIC Rules and Regulations, Miscellaneous Statutes and Regulations, [www.fdic.gov](http://www.fdic.gov).
- <sup>27</sup> Retrieveability", FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual, June 23, 2005, 66.
- <sup>28</sup> *Ibid.*
- <sup>29</sup> *Ibid.*
- <sup>30</sup> "Intermediary Bank", *Kirchman Regulatory Service*, January 2004, 3.6.8.
- <sup>31</sup> U.S. 31 CFR 103.33, "Records to be made and retained by financial institutions", FDIC Rules and Regulations, Miscellaneous Statutes and Regulations, [www.fdic.gov](http://www.fdic.gov).
- <sup>32</sup> U.S. 31 CFR 103.34, "Additional records to be made and retained by banks", FDIC Rules and Regulations, Miscellaneous Statutes and Regulations, [www.fdic.gov](http://www.fdic.gov).
- <sup>33</sup> "Obtaining Tax Identification Numbers for Deposit Accounts", *Kirchman Regulatory Service*, January 2004, 3.8.10.

- <sup>34</sup> U.S. 31 CFR 103.22, "Reports of transactions in currency", FDIC Rules and Regulations, Miscellaneous Statutes and Regulations, [www.fdic.gov](http://www.fdic.gov).
- <sup>35</sup> Ibid.
- <sup>36</sup> Ibid.
- <sup>37</sup> "Currency Transaction Reports and Exemptions", Federal Deposit Insurance Corporation DSC Risk Management Manual of Examination Policies, December 2004, 8.1-1.
- <sup>38</sup> "Currency Transaction Reporting", *Kirchman Regulatory Service*, January 2004, 3.2.
- <sup>39</sup> "CTR Filing Requirements", Federal Deposit Insurance Corporation DSC Risk Management Manual of Examination Policies, December 2004, 8.1-2.
- <sup>40</sup> U.S. 31 CFR 103.27, "Filing of Reports", FDIC Rules and Regulations, Miscellaneous Statutes and Regulations, [www.fdic.gov](http://www.fdic.gov).
- <sup>41</sup> "Core Overview - Currency Transaction Reporting Exemptions", FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual, 23 June 2005, 51.
- <sup>42</sup> Ibid.
- <sup>43</sup> "Exemptions from CTR filing Requirements", Federal Deposit Insurance Corporation DSC Risk Management Manual of Examination Policies, December 2004, 8.1-2.
- <sup>44</sup> Ibid., 8.1-3.
- <sup>45</sup> "Currency Transaction Reporting", *Kirchman Regulatory Service*, January 2004, 3.6.
- <sup>46</sup> "Additional Qualification Criteria for Phase II Exemptions", Federal Deposit Insurance Corporation DSC Risk Management Manual of Examination Policies, December 2004, 8.1-3.
- <sup>47</sup> Ibid., 8.1-3
- <sup>48</sup> Marie Morris, BSA Specialist, Department of Treasury, telephone conversation with author, 27 January 2003.
- <sup>49</sup> Ibid.
- <sup>50</sup> U.S. 31 CFR 103.22, "Reports of Transactions in Currency", FDIC Rules and Regulations, Miscellaneous Statutes and Regulations, [www.fdic.gov](http://www.fdic.gov).
- <sup>51</sup> "Ineligible Businesses", Federal Deposit Insurance Corporation DSC Risk Management Manual of Examination Policies, December 2004, 8.1-3.
- <sup>52</sup> U.S. 31 CFR 103.22, "Reports of Transactions in Currency", FDIC Rules and Regulations, Miscellaneous Statutes and Regulations, [www.fdic.gov](http://www.fdic.gov).
- <sup>53</sup> Ibid.
- <sup>54</sup> "Designation of Exempt Person Filings and Renewals", Federal Deposit Insurance Corporation DSC Risk Management Manual of Examination Policies, December 2004, 8.1-4.
- <sup>55</sup> "Establishment and Review of Exemptions", *Kirchman Regulatory Service*, January 2004, 3.6.1.
- <sup>56</sup> Swanson, Miranda, FDIC Bank Examiner, telephone conversation with author, 19 February 2003.
- <sup>57</sup> U.S. 31 CFR 103.22, "Reports of Transactions in Currency", FDIC Rules and Regulations, Miscellaneous Statutes and Regulations, [www.fdic.gov](http://www.fdic.gov).
- <sup>58</sup> Ibid.
- <sup>59</sup> "Other FinCEN Reports", Federal Deposit Insurance Corporation DSC Risk Management Manual of Examination Policies, December 2004, 8.1-5.
- <sup>60</sup> Ibid.
- <sup>61</sup> "Identification and Reporting of Suspicious Activity", Federal Deposit Insurance Corporation DSC Risk Management Manual of Examination Policies, December 2004, 8.1-23.
- <sup>62</sup> U.S. 31 CFR 103.18, "Reports by banks of suspicious transactions", FDIC Rules and Regulations, Miscellaneous Statutes and Regulations, [www.fdic.gov](http://www.fdic.gov).
- <sup>63</sup> Ibid.
- <sup>64</sup> "Reporting when no suspect is identified - \$25,000 threshold", *Kirchman Regulatory Service*, January 2004, 3.8.1.
- <sup>65</sup> Ibid., 3.8.
- <sup>66</sup> U.S. 31 CFR 103.18, "Reports by banks of suspicious transactions", FDIC Rules and Regulations, Miscellaneous Statutes and Regulations, [www.fdic.gov](http://www.fdic.gov).
- <sup>67</sup> Ibid.
- <sup>68</sup> Ibid.
- <sup>69</sup> Ibid.
- <sup>70</sup> Ibid.

- <sup>110</sup> "Comparison with Government Lists of Known or Suspected Terrorists", Federal Deposit Insurance Corporation DSC Risk Management Manual of Examination Policies, December 2004, 8.1-12.
- <sup>111</sup> Ibid.
- <sup>112</sup> Dahl, Dennis, Field Supervisor letter to Chief Executive Officer of Kirkwood Bank & Trust Co., 8 February 2005.
- <sup>113</sup> Ibid.
- <sup>114</sup> U.S. 31 CFR 103.121, "Customer Identification Programs for banks, savings associations, credit unions, and certain non-Federally regulated banks", FDIC Rules and Regulations, Miscellaneous Statutes and Regulations, [www.fdic.gov](http://www.fdic.gov).
- <sup>115</sup> Zamorski, Michael, Director of the Federal Deposit Insurance Corporation, letter to Chief Executive Officer, 10 December 2002.
- <sup>116</sup> Ibid.
- <sup>117</sup> "Section 314(a) – Mandatory Information Sharing Between the U.S. Government and Financial Institutions", Federal Deposit Insurance Corporation DSC Risk Management Manual of Examination Policies, December 2004, 8.1-14.
- <sup>118</sup> Zamorski, Michael, Director of the Federal Deposit Insurance Corporation, "FinCEN's Secure Information Sharing System Web-Based Process Required By USA PATRIOT Act", 2 May 2005.
- <sup>119</sup> Zamorski, Michael, Director of the Federal Deposit Insurance Corporation, "FinCEN's Secure Information Sharing System, 'Point of Contact Changes with June Call Report'", 1 July 2005.
- <sup>120</sup> Zamorski, Michael, Director of the Federal Deposit Insurance Corporation, "FinCEN's Secure Information Sharing System Web-Based Process Required By USA PATRIOT Act", 2 May 2005.
- <sup>121</sup> "Section 314(a) – Mandatory Information Sharing Between the U.S. Government and Financial Institutions", Federal Deposit Insurance Corporation DSC Risk Management Manual of Examination Policies, December 2004, 8.1-14.
- <sup>122</sup> U.S. 31 CFR 103.100, "Information sharing between Federal law enforcement agencies and financial institutions", FDIC Rules and Regulations, Miscellaneous Statutes and Regulations, [www.fdic.gov](http://www.fdic.gov).
- <sup>123</sup> Ibid.
- <sup>124</sup> Ibid.
- <sup>125</sup> "Section 314(a) – Mandatory Information Sharing Between the U.S. Government and Financial Institutions", Federal Deposit Insurance Corporation DSC Risk Management Manual of Examination Policies, December 2004, 8.1-15.
- <sup>126</sup> U.S. 31 CFR 103.100, "Information sharing between Federal law enforcement agencies and financial institutions", FDIC Rules and Regulations, Miscellaneous Statutes and Regulations, [www.fdic.gov](http://www.fdic.gov).
- <sup>127</sup> Ibid.
- <sup>128</sup> "Customer Identification Program Requirements" Kirchman Regulatory Service, January 2004, 3.8.6



---

## BIBLIOGRAPHY

AML Compliance Alert, "Small Banks Overemphasize CTRs, Overlook Bigger Risks", November 2004, 2

Bies Schmidt, Susan, Julie L. Williams, Donna E. Powell, James E. Gilleran, and William J. Fox to the American Bankers Association, 18 April 2005, [www.aba.com](http://www.aba.com).

Cocheo, Steve, "BSA exam procedures bring uniformity...but at a price", ABA Banking Journal, October 2005, 52.

Community Bank Advisor, "Carrying out the Bank Secrecy Act Requirements", Summer 2005, 3

Dahl, Dennis, Federal Deposit Insurance Corporation to Chief Executive Officer of Kirkwood Bank & Trust Co., February 8, 2005.

FDIC Rules and Regulations, Miscellaneous Statutes and Regulations, 31 CFR 103.18, 103.22, 103.27, 103.29, 103.33, 103.34, 103.100, 103.121, [www.fdic.gov](http://www.fdic.gov).

Federal Deposit Insurance Corporation, Federal Deposit Insurance Corporation DSC Risk Management Manual of Examination Policies, December 2004, 8.1-1, 8.1-2, 8.1-3, 8.1-4, 8.1-5, 8.1-6, 8.1-8, 8.1-12, 8.1-14, 8.1-15, 8.1-23, 8.1-37, 8.1-38.

Federal Deposit Insurance Corporation, "Anti-Money Laundering Measures", by Zamorski, Michael, FIL-135-2002, December 10, 2002.

Federal Deposit Insurance Corporation, "FinCEN's Secure Information Sharing System, Point of Contact Changes with June Call Report", by Zamorski, Michael, July 1, 2005

Federal Deposit Insurance Corporation, "FinCEN's Secure Information Sharing System Web-Based Process Required By USA PATRIOT Act", by Zamorski, Michael, May 2, 2005.

Federal Deposit Insurance Corporation, Part 326.8, "Bank Secrecy Act Compliance", [www.fdic.gov](http://www.fdic.gov).

Federal Financial Institutions Examination Council, Introduction to FFIEC BSA/AML Materials, July 2005, 1, 6.

FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual, June 23, 2005, 51, 64, 66

Ginovsky, John, "Anti-Money Laundering Exams", ABA Bankers News, 12, May 11, 2004, 2.

Kirchman Corporation, Kirchman Regulatory Service, January 2004, 3.2, 3.6.1, 3.6.7-3.6.9, 3.8, 3.8.1, 3.8.4-3.8.6, 3.8.10

Morris, Marie, BSA Specialist, Department of Treasury, Interview by author, January 27, 2003.

Sullivan, Dennis, "BSA Violations Cause Heads to Roll at Small Banks", Regulatory Risk Monitor, January 24, 2005, 1:2

Swanson, Miranda, FDIC Bank Examiner, Interview by author, February 19, 2003.