Suspicious Activity Reporting

FOR

DUMMIES®

A Wiley Brand

SPECIAL EDITION
Publisher’s Acknowledgements

We’re proud of this book; please send us your comments at http://dummies.custhelp.com.

Some of the people who helped bring this book to market include the following:

**Acquisitions and Editorial**

**Acquiring Editor:** Anam Ahmed
**Manager, Custom Publications:** Christiane Cormier
**Production Editor:** Pamela Vokey

**Composition Services**

**Sr. Production Coordinator:** Kristie Rees
**Layout:** Jennifer Creasey
**Proofreader:** Lauren Mandelbaum

---

**John Wiley & Sons Canada, Ltd.**

**Deborah Barton,** Vice President and Director of Operations
**Jennifer Smith,** Publisher, Professional Development
**Alison Maclean,** Managing Editor

**Publishing and Editorial for Consumer Dummies**

**Kathleen Nebenhaus,** Vice President and Executive Publisher
**David Palmer,** Associate Publisher
**Kristin Ferguson-Wagstaffe,** Product Development Director

**Publishing for Technology Dummies**

**Andy Cummings,** Vice President and Publisher

**Composition Services**

**Debbie Stailey,** Director of Composition Services
## Contents at a Glance

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Part I: Understanding Suspicious Activity</td>
<td>5</td>
</tr>
<tr>
<td>Part II: Reporting Suspicious Activity</td>
<td>11</td>
</tr>
<tr>
<td>Part III: Checking Out the SAR</td>
<td>17</td>
</tr>
<tr>
<td>Part IV: Preparing the SAR Narrative</td>
<td>29</td>
</tr>
<tr>
<td>Part V: Benefiting from Automation</td>
<td>37</td>
</tr>
<tr>
<td>Part VI: Ten Tips for Choosing an Automated System</td>
<td>43</td>
</tr>
</tbody>
</table>
# Table of Contents

## Introduction ................................................................. 1
  About This Book ........................................................... 1
  Foolish Assumptions ...................................................... 2
  How This Book Is Organized ............................................ 2
    Part I: Understanding Suspicious Activity .................. 2
    Part II: Reporting Suspicious Activity ....................... 2
    Part III: Checking Out the SAR ................................. 3
    Part IV: Preparing the SAR Narrative ......................... 3
    Part V: Benefiting from Automation ............................ 3
    Part VI: Ten Tips for Choosing an Automated System ... 3

## Icons Used in This Book ............................................... 3

## Part I: Understanding Suspicious Activity ............... 5
  Preventing Money Laundering ....................................... 5
    Understanding money laundering ................................ 6
    Meeting the regulators ............................................. 7
  Introducing Suspicious Activity .................................. 8
  Detecting Suspicious Activity ..................................... 9
Part II: Reporting Suspicious Activity ................. 11
Meeting Reporting Obligations ............................. 11
Refiling Reports .................................................... 14
Maintaining Confidentiality .................................. 14
Acing Your Exams .................................................... 15

Part III: Checking Out the SAR .......................... 17
Modernizing the SAR .............................................. 17
Tracking Suspicious Activity ................................. 18
Indicating a Corrected Report ............................... 20
Step 1: Filing Institution Contact Information ........... 20
Step 2: Information about Financial Institution
  Where Activity Occurred ....................................... 22
Step 3: Subject Information .................................... 22
Describing the Activity in
  Step 4: Suspicious Activity Information .................. 25

Part IV: Preparing the SAR Narrative .................. 29
Documenting the Five W’s of
  the Suspicious Activity ....................................... 30
  Who’s involved? ................................................. 30
  What happened? ................................................ 31
  When did it happen? ......................................... 32
  Where did it happen? ......................................... 32
  Why is the activity suspicious? .......................... 33
Considering Common Weaknesses ....................... 33
Part V: Benefiting from Automation .......................37
Understanding Why Filing SARs Matters ..............37
Discovering the Advantages of Automation ..........38
Seeing the Step-by-Step Differences .................40

Part VI: Ten Tips for Choosing an
Automated System .............................................43
Delegate Detection .............................................43
Go with the Workflow ...........................................44
Find Flexibility ...............................................44
Automate Your Report Completion Process ........44
Get Connected ...............................................44
Consider Storage ..............................................45
Take a Customer-centric Approach .................45
Get More for Your Money ..................................45
Kick the Tires on Technology (But Don’t
  Forget to Look Under the Hood, Too!) ..........46
Keep It Simple .................................................46
Introduction

Sending regulators clear and detailed reports of suspicious activity arms them with invaluable information in their fight against financial crime. Filing correct Suspicious Activity Reports (SARs) provides them with details that can help make or break their cases against criminals. I created this reference book to help ensure that you produce stellar SARs.

About This Book

In this book, I introduce you to money laundering and discuss your obligations to report activity that you suspect indicates money laundering. I also walk you through completing a SAR, tell you how to avoid some common mistakes, and share the advantages of automating your suspicious activity monitoring and reporting processes.

Note: This book isn’t intended to replace official guides, such as the FFIEC BSA/AML Examination Manual or the detailed instructions on the Suspicious Activity Report. The Financial Crimes Enforcement Network (FinCEN) provides administrative rulings to clarify regulatory issues. If you need more information, you can contact the Bank Secrecy Act (BSA) help desk by phone at 866-346-9478 (option 1) or by e-mail at bsaefilinghelp@fincen.gov.
**Foolish Assumptions**

If you’re reading this book, I assume you work in the financial services industry (most likely at a bank or credit union) and hold a position such as one of these:

✓ A compliance officer responsible for your financial institution’s anti-money-laundering efforts

✓ A fraud investigator

✓ A manager of employees who works in a compliance or fraud-fighting capacity

✓ An employee who makes decisions related to reducing financial crimes, overseeing compliance obligations, or selecting related software

**How This Book Is Organized**

Finding the suspicious activity reporting information you need will be a snap because I present it in six easy-to-digest parts:

**Part I: Understanding Suspicious Activity**

Regulators and compliance departments focus on preventing financial crime, and understanding it makes the task easier. In this part, I introduce you to one of the most common financial crimes — money laundering — and to activities that should make you suspect that bad guys are doing their laundry at your financial institution.

**Part II: Reporting Suspicious Activity**

Alerting regulators to unusual activity at your financial institution helps them to catch the bad guys. In this
Part, I detail your suspicious activity reporting responsibilities.

**Part III: Checking Out the SAR**

In this part, I present the Suspicious Activity Report (SAR) and offer tips so that you can complete SARs and avoid the most common mistakes.

**Part IV: Preparing the SAR Narrative**

Explaining why the activity you’re reporting seems suspicious is critical; after all, regulators aren’t mind readers. In this part, I share ways to ensure you create a helpful narrative.

**Part V: Benefiting from Automation**

Automating your suspicious activity monitoring and reporting processes saves you time and potentially catches more criminals. What’s not to love? In this part, I consider the advantages of switching from a manual process to an automated one.

**Part VI: Ten Tips for Choosing an Automated System**

I love to shop, so it’s only natural that in this part I offer up some shopping tips. Keep them in mind if you decide to purchase software to automate your suspicious activity reporting processes.

**Icons Used in This Book**

Occasionally you’ll notice symbols on the left-hand side of the page that bring your attention to a particular piece of information. Here’s what each one means:
This icon indicates information that’s worth remembering in your fight against financial crime.

This icon highlights something that will make completing SARs a little easier.

This icon signals something that may be dangerous to your well-being or to your career.
Financial institutions (FIs) keep a close eye on suspicious transactions that may involve money laundering so they can prevent it and maintain the integrity of the financial system. In this part, I introduce you to money laundering and to suspicious activities that alert you to potential instances of money laundering.

**Preventing Money Laundering**
Criminals, including drug traffickers, terrorists, arms dealers, and others, use money laundering as a way to fund and expand their illegal activities. But apart from watching the odd mob movie, most people have just a passing understanding of what money laundering involves. So in this section, I introduce the concept of
money laundering and some of the people who are trying to stop it.

Understanding money laundering

Money laundering is an attempt to disguise the source of a sum of money. Everyone does laundry. You know the drill — when you launder your dirty clothes, you put them in the washing machine and, with the exception of the odd sock that goes missing, they come out clean. The same principle applies when the bad guys launder their money. Instead of a washing machine, the bad guys put their dirty money into the financial system (through banks, trust companies, and credit unions) to clean it.

Laundering money to make it appear legitimate involves three steps, which can occur simultaneously or separately:

1. **Placement:** The bad guys put their ill-gotten gains into the financial system. This can be as simple as depositing cash into a bank account. Sometimes they break down a large deposit into several smaller ones in an attempt to avoid detection. For example, Bob the bad guy deposits $5,000 to his personal account at bank branch A, $3,000 to his joint account at bank branch B, and $4,000 through an automated teller machine at bank branch C. Breaking up the deposit like this, with the intention to avoid having to report it to the Department of the Treasury, is called structuring. And it’s illegal.

   **Warning:** Structuring your cash transactions this way can lead to penalties that include up to five years in jail or a fine of up to $250,000.
2. **Layering:** Next, the bad guys try to cover their tracks by carrying out a variety of transactions. Moving the money around makes following the trail back to the original source difficult. For example, Bob the bad guy creates phony companies (called *shell corporations*) and then transfers money between them in an attempt to make the funds appear legitimate.

3. **Integration:** After the money has been deposited into the financial system and its origins have been clouded by a series of transactions, it’s “clean.” Now the bad guys use it to purchase material goods (such as a yacht, a vacation home, or a statue for the front lawn) or invest it in further criminal activities.

**Meeting the regulators**

So, who are the good guys in the war against money laundering? Are they tall, dark, and handsome, with guns on their hips? Not exactly. They may be tall, dark, and handsome, but they wield a slightly different weapon — paper. A branch of the Department of the Treasury, the Financial Crimes Enforcement Network (FinCEN for short), protects the U.S. financial system from money laundering by creating regulations, enforcing compliance, facilitating information sharing, performing analyses, and coordinating with foreign counterparts.

To keep the good guys informed, financial institutions file different types of reports with FinCEN, which uses the reports to try to identify possible instances of money laundering and shares any pertinent information with the appropriate law enforcement agencies. To keep
things simple, I focus on only one of these reports in this book: the Suspicious Activity Report (SAR). (For the inside scoop on another type of report, the Currency Transaction Report, be sure to check out *Currency Transaction Reporting For Dummies.*)

**Introducing Suspicious Activity**

So, how do you figure out if the bad guys launder money through your FI? By keeping tabs on transactions and investigating any activities that seem suspicious. Suspicious transactions come in all different shapes and sizes, but some of the most common things to watch out for include the following:

- Transactions that consistently fall just below reporting or recordkeeping thresholds
- Sudden bursts of activity in low-transaction or dormant accounts
- Bulk transactions
- Complex transactions, which may indicate that the bad guys are layering their activity (refer to the “Understanding money laundering” section for more on layering)
- An unusually large number of wire transfers
- Dealings between businesses that don’t have a natural connection (such as JJ Pizzeria depositing checks from Sal’s Auto Body)
- Transactions that don’t match with expected volumes when compared to peer businesses or customers
### Keeping tabs on questionable activities

Passed in the United States in 1970, the Bank Secrecy Act (BSA) requires financial institutions operating in the United States to file and retain records that may be useful in tracking tax, criminal, and other regulatory activities. Under the BSA, financial institutions must file five different reports:

- The Currency Transaction Report
- The Suspicious Activities Report
- FinCEN Form 105 Report of International Currency or Monetary Instruments (*CMIR*)
- The Department of the Treasury Form 90-22.1 (the Report of Foreign Bank and Financial Accounts)
- The Designation of Exempt Person Form

---

### Detecting Suspicious Activity

FIs become aware of suspicious activity through a variety of means:

- **Inter-office identification:** Frontline staff may notice something out of the ordinary and alert the compliance department.

- **Reviewing core system reports:** This involves manually reviewing transaction reports generated by the core system.

- **Surveillance monitoring:** This involves an automated review of transactions (turn to Part V for more on the advantages of this type of review).
Law enforcement requests: On occasion, law enforcement officers who are pursuing a suspect will ask an FI to review the suspect’s transactions, with the hope of finding more evidence for their case.

Grand jury requests: If your FI receives a grand jury subpoena, review the appropriate customer’s transactions for any evidence of suspicious activity. If you determine you need to file a SAR, do so. However, refer only to the relevant facts that you uncover. Be sure to maintain confidentiality. Don’t disclose that your FI initiated the investigation because of a grand jury request — not even to FinCEN.

When you identify a potentially suspicious activity, put on your detective hat and delve into the details of the case. Figuring out which transactions are suspicious and which are just a little out of the ordinary takes some work, but you can take comfort in the knowledge that your hard work protects your FI and helps regulators crack down on crooks. Thoroughly research a transaction to determine if a logical explanation for the activity exists. After all, an unusually large transaction may just mean your customer won the lottery, or inherited a fortune from Great Aunt Fran.

If you decide that an activity is suspicious and warrants further investigation by authorities, file a SAR with FinCEN (Parts II and III of this book share the full details on SARs). If you decide that the activity isn’t suspicious enough to require the filing of a SAR, document your reasons and store them with the rest of the case details.
Part II

Reporting Suspicious Activity

In This Part
▶ Alerting authorities to suspicious activity
▶ Reporting continuing suspicious activity
▶ Keeping quiet about confidential details
▶ Preparing for an examiners’ review

Maintaining communication between the Financial Crimes Enforcement Network (FinCEN) and financial institutions (FIs) is essential because FinCEN uses the information supplied by FIs to combat crime—everything from money laundering to terrorism. In this part, I detail your reporting responsibilities.

Meeting Reporting Obligations

Regulators can’t investigate suspicious activity if they don’t know about it. Regularly advising them of unusual activity keeps them in the loop. FIs use the Suspicious Activity Report (SAR) to notify FinCEN of the circumstances of any activity that’s out of the ordinary and merits further investigation.
Federal regulations require an FI to file a SAR when

✓ A transaction (or attempted transaction) of more than $5,000 takes place and the FI suspects that money laundering or other illegal activity is involved, the transaction is an attempt to avoid Bank Secrecy Act (BSA) regulations, or the transaction isn’t one this customer would usually engage in

✓ A criminal violation occurs and an insider is suspected

✓ A criminal violation of $5,000 or more occurs and the FI can identify the suspect

✓ A criminal violation of $25,000 occurs, even if the FI can’t identify the suspect

Failing to adhere to BSA regulations exposes you to penalties that include fines of up to $5,000 and/or jail time.

You must file a SAR within 30 days of determining that the activity is suspicious. But don’t panic. I don’t mean 30 days after you first notice the transaction; no need to rush your review. Submit the SAR within 30 days of reviewing it and deciding that something is indeed fishy. In addition, if you have trouble identifying the suspect in the case, you can extend the deadline to 60 days in order to carry out further investigation.

If your situation is urgent, don’t wait until the SAR is complete to alert authorities. Contact law enforcement immediately so they can
begin their investigation, and then file your SAR as you normally would. In Part IV (Step 1) of the SAR, be sure to note the details of your contact with law enforcement.

After you’ve filed a SAR with FinCEN, ensure you save a copy for your records. Keep SAR case information for at least five years. As well as the SAR, retain any documentation that supports your suspicions, such as documentation used to open the customer’s account, transaction records, or e-mail or other correspondence relating to the transaction or investigation.

You can attach a single spreadsheet (referred to as a comma-separated values (CSV) file) as part of the SAR. The CSV is a standard Microsoft file format that stores tabular data in plain-text form. This capability allows you to include data (such as specific financial transactions and funds transfers or other analytics) that is transferable among different programs and is, therefore, more readable and usable in this format than it would be if included in the narrative. Remember that the CSV file doesn’t replace the narrative!

In addition, if you decide that the activity you reviewed isn’t suspicious and doesn’t require filing a SAR, keep your supporting documentation for this decision as well. When examiners audit your FI, they’ll want to see case files for both submitted SARs and transactions you deemed unsuspicious (see “Acing Your Exams,” later in this part).
Refiling Reports

In some cases, suspicious activity continues after you first notice and report it. (For example, Bonnie Badgirl makes weekly cash withdrawals in amounts just under the reporting threshold.) When this happens, notify regulators of the continuing activity by refiling a SAR every 90 days. Use the new SAR to detail whatever suspicious activity has taken place since you filed the last one. (See Part III for tips on refiling.)

Maintaining Confidentiality

Keeping quiet about SARs is essential because revealing the existence of one may alert suspects to the fact that they are under suspicion and can potentially compromise an investigation. Although some facts about transactions can be disclosed, anything that may reveal the existence of a SAR must be treated as confidential. In fact, the unauthorized disclosure of a SAR violates federal law.

Disclosing SAR information may result in civil penalties of up to $100,000 and criminal penalties of up to $250,000, and up to five years in jail. And if the release of information results from inadequate controls in an FI’s anti-money-laundering program, the FI exposes itself to penalties of up to $25,000 per day until it rectifies the problem.

FIs typically address the need for secrecy by limiting access to SAR information to those who “need to
know,” by keeping track of which employees access SARs, and by stressing the importance of confidentiality in their training programs.

You may notice a flaw with this regulation: How can you report suspicious activity if you need to keep it confidential? Don’t worry — regulators recognize the need to balance confidentiality concerns with the benefits of information sharing, so they created a loophole. The U.S.A. Patriot Act, Section 314 (b), offers a safe harbor provision that allows FIs to disclose SARs and SAR-related information to FinCEN or law enforcement. The safe harbor provision also permits an FI to share information with another FI, as long as both are registered participants in the 314 (b) program and file a Notice of Intent to Share with FinCEN.

But other than the exceptions covered by the safe harbor provision, you must keep quiet about any confidential SAR-related information. For example, if you receive a subpoena requesting confidential information, such as from the Securities and Exchange Commission or the Commodity Futures Trading Commission, refuse to provide it. Instead, send the request and a copy of your (negative) response to FinCEN.

**Acing Your Exams**

Periodically, examiners audit your FI to ensure your suspicious activity monitoring, detecting, and reporting meet regulatory standards. Usually, examiners look at your overall process and follow an alert through the process to ensure it’s appropriate.
Knowing what examiners look for can be helpful when structuring your processes and preparing for the review. Auditors want to review the following:

✔️ **How you identify suspicious activity**
  - Do you have a designated person who identifies, researches, and reports unusual activity?
  - Is your staff aware that this person should be the key point of contact for reporting unusual activity?
  - What system do you use to monitor transactions? And does that system filter the transactions well enough to create accurate reports of suspicious activity?

✔️ **How you manage alerts**
  - Do you respond to alerts by reviewing and investigating promptly?
  - Do you have enough staff available to conduct appropriately in-depth investigations?

✔️ **How you deal with suspicious activity**
  - How do you decide whether to file a SAR?
  - When a SAR isn’t filed, do you retain documentation supporting that decision?
  - If suspicious activity continues, what are your procedures for escalating the issue?

✔️ **How you complete your SARs**
  - Do you complete the data fields correctly?
  - Are your narratives sufficiently detailed, and do they clearly explain why you believe the activity is suspicious?
The information provided on a Suspicious Activity Report (SAR) plays a key role in fighting financial crime. Because of the importance of reporting suspicious activity to regulators, in this part I offer some suggestions that will help make filling out your SARs as hassle-free (and error-free) as possible.

**Modernizing the SAR**

In 2011, the Financial Crimes Enforcement Network (FinCEN) started the process of modernizing the SAR, including making important changes to report submission requirements. On the user’s side of things, the
changes were an attempt to make the report more intuitive and user-friendly. From law enforcement’s viewpoint, these changes improve data collection by taking advantage of a modernized information technology system. The updates give law enforcement and regulatory partners a more advanced and sophisticated method of querying report information, which helps to catch the bad guys more quickly.

Much to the chagrin of stamp collectors, FinCEN also bid adieu to snail mail. As of March 31, 2013, FinCEN requires financial institutions to electronically file the new reports through the BSA E-Filing System — it no longer accepts legacy reports after that time.

The new SAR replaces all industry-specific SARs (Form TD F 90-22.47, FinCEN Form 101, FinCEN Form 102, and FinCEN Form 109), which are now known as legacy reports.

**Tracking Suspicious Activity**

Financial institutions (FIs) use SARs to inform regulators of any suspicious activity occurring in their accounts. Regulators and law enforcement officials use the information provided on SARs to track down and build cases against criminals. Luckily for you, most, if not all, of the information required to complete a SAR already exists in your case file. You just need to carefully transfer it to the report.

Check out Figure 3-1 for a look at a typical SAR.
Figure 3-1: The Suspicious Activity Report (SAR).
**Indicating a Corrected Report**

Mistakes happen, even to you and me. When you notice a mistake that pertains to a previously filed SAR, be sure to notify FinCEN by filing an amended SAR. Indicate that this report corrects previously submitted information by checking the Correct/Amend Prior Report check box as part of Item 1, Type of Filing under the Home tab.

**Step 1: Filing Institution Contact Information**

Under the Step 1 tab, you need to complete Part IV – Filing Institution Contact Information. Filling out this part of the report should be a snap; it’s all about you (see Figure 3-2). Complete each of the items with the appropriate information. Here are a few tips for this section:

- When entering your institution’s primary federal regulator in Item 78, if more than one applies, enter the regulator with primary responsibility for enforcing compliance with the BSA.
- Use your institution’s legal name in Item 79, Filer Name. You can enter the trade name later in Item 90, Alternate Name.
- When entering your Tax Identification Number in Item 80, TIN, don’t use hyphens or periods.
- The city name entered in Item 86, City, must match the city name used by the U.S. Postal Service for the state and zip code you enter in Items 87 and 88.
- Items 91 to 95 are used to enter information about law enforcement agencies if they were contacted about this suspicious activity.
Figure 3-2: Suspicious Activity Report, Step 1.
Incorrectly entering an FI’s Tax Identification Number (TIN) in Items 80 and 81 is one of the most common errors for this part of the SAR. Although I mention this earlier in this part, it’s worth repeating: Avoid this mistake by ensuring you include all nine numbers of your TIN and enter only numbers — no hyphens or spaces.

Step 2: Information about Financial Institution Where Activity Occurred

Here is where you tell the authorities where the suspicious activity occurred. One of the best things about this section is that if the activity occurred at the same institution that you entered information about in Part IV (Step 1), you can complete most of this step with the click of a button. Literally.

At the top of Part III (Step 2) is this question: “Would you like to insert all applicable filing institution information into Part III?” Click the blue Yes button to the right of the question. Voilà!

Alright, almost there. You still need to complete the bottom section that indicates the branch of the FI where the activity occurred.

If the activity occurred in more than one branch, you can click the blue + button in the Branch Where Activity Occurred Information section to add more branches to the report.

Step 3: Subject Information

Part I (Step 3) gives you the opportunity to identify the subject. Check out Figure 3-3 for a glimpse.
**Figure 3-3: Suspicious Activity Report, Step 3.**

<table>
<thead>
<tr>
<th>Part 1: Subject Information</th>
<th>1 of 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 Check:</td>
<td></td>
</tr>
<tr>
<td>* 3 Individual's last name</td>
<td></td>
</tr>
<tr>
<td>or entity's legal name</td>
<td></td>
</tr>
<tr>
<td>* 4 First name</td>
<td></td>
</tr>
<tr>
<td>* 5 Middle name or initial</td>
<td></td>
</tr>
<tr>
<td>Suffix</td>
<td></td>
</tr>
<tr>
<td>* 16 Date of birth</td>
<td></td>
</tr>
<tr>
<td>6 Alternate name, e.g.</td>
<td></td>
</tr>
<tr>
<td>AK4, Individual or trade name, DBA - entity</td>
<td></td>
</tr>
<tr>
<td>7 Occupation or type of business</td>
<td></td>
</tr>
<tr>
<td>7a NAICS Code</td>
<td></td>
</tr>
<tr>
<td>* 13 TIN</td>
<td></td>
</tr>
<tr>
<td>18 Phone number</td>
<td></td>
</tr>
<tr>
<td>19 E-mail address</td>
<td></td>
</tr>
<tr>
<td>14 TIN type</td>
<td></td>
</tr>
<tr>
<td>Ext.</td>
<td></td>
</tr>
</tbody>
</table>
Keep the following in mind when completing this section:

✓ If you don’t have any information about the subject, check the If All Critical Subject Information Is Unavailable check box for Item 2 of this part. Doing so ensures that regulators don’t think you simply forgot to complete this part of the report. This should be checked only if you have no information for Items 3, 4, 8, 9, 10, 11, 12, 13, 15, and 16. If you have information for any of these items, don’t check this check box; check the Unknown check box for the relevant items instead.

✓ If you don’t know the subject’s social insurance number, social security number, or Employer Identification number, check the Unknown check box. Don’t input 000000000 or 999999999 as dummy numbers.

✓ If you have a record of the subject’s government-issued identification, be sure to include the ID number. Providing as much detail as possible about this ID makes tracking down a subject easier.

✓ When entering the person’s date of birth in Item 16, remember the date format is MM/DD/YYYY (for example, November 5, 1975, is entered 11/05/1975).

✓ If you need to report more than one suspect involved with the same suspicious activity, complete a separate Part I (Step 3) for each.

✓ If the suspicious activity involves an organization, rather than an individual, check the “if entity” checkbox, place the company name in Item 3, Individual’s Last Name or Entity’s Legal Name and leave Items 4 and 5 blank.
If you know that the suspect also conducts business under another name (often known as *doing business as*, or *DBA*), enter the alternate name in Item 6, Alternate Name. For example, if Jackson Enterprises makes a suspicious cash deposit of pizza sale proceeds under the name of JJ Pizzeria, enter Jackson Enterprises in Item 3 and alert authorities to the existence of JJ Pizzeria in Item 6.

**Describing the Activity in Step 4: Suspicious Activity Information**

Use Part II (Step 4) of the SAR to provide the nitty-gritty details of the suspicious activity, including the type of activity and the dollar value involved (see Figure 3-4).

Completing this part should be straightforward; just take the required information directly from your case file and fill out the appropriate fields. There are sections of this step that show just how universal FinCEN’s updated report is. For example, you can see Item 32 is specific to suspicious activity affecting casinos.

If suspicious activity (that you reported earlier) is continuing, and you are completing a 90-day update report because of this continuing activity, then you must complete Part II (Step 4) to have both information about this report (the past 90 days) and the overall cumulative activity included. The information in Items 26 (dollar amount) and 27 (date range) pertains to only the last 90 days of activity. However, Item 28 should be populated with the cumulative dollar amount if this is a Continuing Activity Report.
### Part II Suspicious Activity Information

- **26** Amount involved in this report
  - [ ] Amount Unknown
  - [ ] No amount involved
  - $_________.00

- **27** Date or date range of suspicious activity for this report
  - From: __________
  - To: __________

- **28** Cumulative amount (only applicable when "Continuing activity report" is checked in Item 1)
  - $_________.00

When completing item 29 through 38, check all that apply:

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>29</td>
<td>Structuring</td>
</tr>
<tr>
<td>a</td>
<td>Alters transaction to avoid BSA recordkeeping requirement</td>
</tr>
<tr>
<td>b</td>
<td>Alters transaction to avoid CTR requirement</td>
</tr>
<tr>
<td>c</td>
<td>Customer cancels transaction to avoid BSA reporting and recordkeeping requirements</td>
</tr>
<tr>
<td>d</td>
<td>Multiple transactions below BSA recordkeeping threshold</td>
</tr>
<tr>
<td>e</td>
<td>Multiple transactions below CTR threshold</td>
</tr>
<tr>
<td>f</td>
<td>Suspicious inquiry by customer regarding BSA reporting or recordkeeping requirements</td>
</tr>
<tr>
<td>z</td>
<td>Other</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>Terrorist Financing</td>
</tr>
<tr>
<td>a</td>
<td>Known or suspected terrorist/terrorist organization</td>
</tr>
<tr>
<td>z</td>
<td>Other</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>31</td>
<td>Fraud (Type)</td>
</tr>
<tr>
<td>a</td>
<td>ACH</td>
</tr>
<tr>
<td>b</td>
<td>Business loan</td>
</tr>
<tr>
<td>c</td>
<td>Check</td>
</tr>
<tr>
<td>d</td>
<td>Consumer loan</td>
</tr>
<tr>
<td>e</td>
<td>Credit/Debit card</td>
</tr>
<tr>
<td>f</td>
<td>Healthcare</td>
</tr>
<tr>
<td>g</td>
<td>Mail</td>
</tr>
<tr>
<td>h</td>
<td>Mass-marketing</td>
</tr>
<tr>
<td>i</td>
<td>Pyramid scheme</td>
</tr>
<tr>
<td>j</td>
<td>Wire</td>
</tr>
<tr>
<td>z</td>
<td>Other</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>32</td>
<td>Casinos</td>
</tr>
<tr>
<td>a</td>
<td>Inquiry about end of business day</td>
</tr>
<tr>
<td>b</td>
<td>Minimal gaming with large transactions</td>
</tr>
<tr>
<td>c</td>
<td>Suspicious intra-casino funds transfers</td>
</tr>
<tr>
<td>d</td>
<td>Suspicious use of counter checks or markers</td>
</tr>
<tr>
<td>z</td>
<td>Other</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>33</td>
<td>Money Laundering</td>
</tr>
<tr>
<td>a</td>
<td>Exchange small bills for large bills or vice versa</td>
</tr>
<tr>
<td>g</td>
<td>Suspicious receipt of government payments/benefits</td>
</tr>
</tbody>
</table>
With the growth of cyber fraud, authorities are adjusting their microscopes to look for any available data relating to suspicious online activity. If the suspicious activity you detected is online, you can include an IP address of the computer involved (if known). Go to Item 44, “IP address (if available)” to enter it. If multiple IP addresses are involved, just click the blue ‘+’ button to add more.

Sometimes suspicious activity requires urgent attention from law enforcement, so you contact them before you have a chance to file a SAR. In this case, fill out Items 91 to 95 in Part IV (Step 1) so that regulators know who to contact regarding the case.

Reporting the suspicious activity to law enforcement doesn’t mean you’re off the SAR hook. You still must file a SAR so that regulators are aware of the activity.
Part IV

Preparing the SAR Narrative

In This Part

▶ Presenting your case
▶ Avoiding common mistakes

Completing the narrative in Part V (Step 5) of the Suspicious Activity Report (SAR) provides you with the opportunity to explain to regulators why you think the activity you’re reporting seems suspicious. The data you enter on the first two pages of the SAR (refer to Part III for details on crossing your t’s and dotting your i’s) isn’t useful to regulators on its own. Understanding the full story is critical if they’re going to catch the bad guys, and the narrative provides your chance to tell that story. In fact, crafting a good narrative helps regulators so much, I devote this entire part just to Part V (Step 5) of the SAR.
Documenting the Five W’s of the Suspicious Activity

Explaining your suspicions in an easily understood narrative is a cinch if you follow the rules you learned in ninth grade composition class. Can’t remember back that far? Let me jog your memory: Make sure your narrative has an introduction, a body, and a conclusion. Create these three parts by addressing the five w’s of the suspicious activity — who, what, when, where, and why.

Who’s involved?

You provide basic information about the subject in Part I (Step 3) of the SAR (you know — name, rank, and serial number), but the narrative offers an opportunity for you to expand on this information. Include all data that you have available, such as

- The subject’s employment details, including occupation, job title, and employer’s name and address
- Additional identification numbers not listed in Part I (Step 3)
- Secondary addresses for the subject, such as a post office box
- Any relationships that exist among multiple subjects
What happened?

Let the regulators know the specifics of what’s happening. What’s the subject’s modus operandi (m.o.)? Tell them what types of instruments the subject uses when conducting the suspicious activity. For example, transactions may involve the following:

- Bank drafts
- Debit or credit cards
- Money orders
- Shell companies
- Structuring
- Wire transfers

The Suspicious Activity Information section of the report — Part II (Step 4) — includes a number of sections that allow you to indicate information about the activity, such as Item 29, Structuring, or Item 40, Instrument Type. Because of this, the narrative section of the updated report is limited to 17,000 characters, much lower than the 39,000 character limit of the legacy report.

Also include details about how the transactions are made. Does the subject use an automated teller machine (ATM), a night deposit box, or Internet banking, or does she make the transactions in person? And even though you identify your account numbers in Part I (Step 3) of the SAR, recap them here and provide any details you have about other financial institutions (FIs) that are involved in the transactions, such as their addresses and account numbers.
If you’re filing a 90-day-update SAR because the suspicious activity hasn’t stopped, you don’t have to retell the entire story. Remember that you indicate under Item 1 (Home tab) that this is a Continuing Activity Report and provide the prior report’s Document Control Number/BSA Identifier. So just reference the previously filed SAR(s) and provide details of the activity that’s happened in the 90 days since you last filed a SAR.

**When did it happen?**

Let the Financial Crimes Enforcement Network (FinCEN) know the date that the suspicious activity took place. If it happened on more than one occasion, list all of the dates and the transaction amounts associated with each date.

Many FIs find it helpful to use spreadsheets to track dates, transactions, and amounts related to suspicious activities. As I mention in Part II of this book, you can now attach a CSV file to SAR submissions to send tabular data in plain-text form.

**Where did it happen?**

Part III (Step 2) of the SAR gives you space to provide information about where the suspicious activity occurred, and you can easily add multiple location information there, if necessary. If a location plays a role in why you think the activity was suspicious, describe why.
Why is the activity suspicious?

Explain, in as much detail as you can, why you think this activity is suspicious. Point out how the activity differs from the customer’s usual activity, or from the expected activity based on the behavior of the customer’s peers.

Considering Common Weaknesses

The information you provide in your narrative affects the success of regulators and law enforcement as they track down the bad guys. Do your part to help them as much as possible by avoiding the most common narrative mistakes. FinCEN reports these top three mistakes:

✓ Leaving the narrative field empty: If you don’t complete the narrative section, investigators won’t know why you consider the activity you’re reporting to be suspicious. Be sure to help investigators by giving them the whole story, not just the data.

✓ Failing to detail all available information: Instead of providing the case information in the narrative field, FIs often refer investigators to supporting documentation, which is prohibited because regulators can’t easily access it. FIs should extract all of the case details from the supporting documentation and set them out in the narrative. Retain the supporting documentation in your own files for five years.

✓ Providing an insufficient narrative: Many FIs fail to adequately explain why they think the activity
is suspicious. Often, they simply restate the data that they provide earlier in the report. Instead, take the opportunity to detail the five w’s of the activity (who, what, when, where, and why) so that investigators have as much ammunition as possible in their fight against financial crimes.

Hover your cursor over the narrative section of the report, and you can see how FinCEN describes what is required. The instructions include the following: “Filers must provide a clear, complete, and concise description of the activity, including what was unusual or irregular that caused suspicion. This description should encompass the data provided in Parts I through III, but should include any other information necessary to explain the nature and circumstances of the suspicious activity.”

---

**Storytelling 101**

While narratives are important, don’t worry — no one expects your account of the suspicious activity to rival an Agatha Christie novel. Simply make sure you clearly present all available information that may help investigators to nab the bad guys. Consider the differences between the following narratives, and you’ll see how much easier you can make life for investigators just by spelling things out clearly and concisely.

**Narrative A**

Bob the bad guy made a number of cash deposits through various methods, including branch ATMs, night deposit slots, and in person. All transactions were below the reporting threshold, and we believe this was intentional so he could avoid reporting the transactions on a Currency Transaction Report.
Narrative B

We suspect that Bob the bad guy is structuring his cash deposits to avoid reporting them to federal authorities. We have investigated, and our case number is 1234567. Bob the bad guy opened his account ABCDEFG with us in April 2011. He used his U.S. passport (#894867) to verify his identity and address (87 Main Street, Our Town, U.S.A.). He indicated that he works as a cook at JJ Pizzeria (1234 South Sesame Street, Our Town, U.S.A.).

On June 8, 2011, he made two separate deposits to his account: $4,000 in person at our main branch and $5,500 through the ATM at our Sesame Street branch (585 Sesame Street, Our Town, U.S.A.). This pattern continued with the following deposits: $9,300 on June 17, $9,750 on June 21, $9,600 on June 24, and $9,800 on June 29. These transactions came to the attention of our compliance officer because they appear to be unusually large deposits for someone who works as a pizza cook and they all fall just below the reporting threshold.

Our compliance officer, Sally Stickler, will continue to monitor the account and will retain all documentation related to this case.

Narrative A provides only a general overview of the potential problem, without substantiating the FI’s suspicions or providing information that can help officials locate the subject. Narrative B offers regulators and law enforcement officials clear reasons for the FI’s concern, useful background information on the subject, and a reference number so that officials can easily obtain clarification or additional information from the FI.
Part V

Benefiting from Automation

In This Part
- Knowing why filing counts
- Getting to know the advantages of automation
- Comparing manual and automated processes

You have to report suspicious activity — there’s no getting around it — but automating your detection and reporting processes makes filing a report as quick and easy as possible. In this part, I remind you of the importance of filing your reports, help you to get familiar with the benefits of automating your suspicious activity monitoring and reporting, and offer a comparison to demonstrate the differences between manual and automated processes.

Understanding Why Filing SARs Matters

Investigating and reporting suspicious activity takes a great deal of your valuable time, but consider it time well spent. After all, incentives for filing quickly and correctly include the following:
✓ **Staying out of jail**: Failing to report suspicious activity can result in fines or imprisonment.

✓ **Impressing your auditors**: Regulators will audit your financial institution (FI). Staying on top of suspicious activity by promptly filing reports and efficiently storing all pertinent evidence makes your audit go much more smoothly. And happy auditors mean a happy FI.

✓ **Getting to play the hero**: Regulators use the information you provide to catch crooks — everyone from terrorists to drug dealers to white-collar criminals. When else do you have a chance to help put away the bad guys so you and your neighbors can sleep better at night?

---

**Discovering the Advantages of Automation**

Reviewing core banking system reports manually to find potentially suspicious activity requires painstaking patience and countless hours. And manually completing and submitting SARs eats up even more time. Streamlining your process by switching to an automated system saves time and reduces the risk of missing suspicious activity through human error. An automated solution offers many advantages:

✓ **Systematic reviews of transaction reports**: Instead of looking for suspicious activity by combing through hundreds of pages of transaction reports, an automated system does it for you. The system analyzes customer activity to produce alerts, advises you of potentially suspicious
activity, provides clear explanations of what prompted an alert, and ranks the alerts according to level of risk.

✓ **Customized alert generation:** With a behavior-based system that analyzes for the out-of-the-ordinary, any alerts you receive are likely to be genuinely suspicious. You spend less time investigating *false positives* (activity that looks suspicious but isn’t).

✓ **Automatic data entry:** If you investigate a transaction flagged by the system and decide that the activity is suspicious and you need to file a SAR, your system draws key information from the case file and puts it directly into the SAR. This leaves more time for you to focus on the all-important narrative section of the report.

✓ **Efficient workflows:** An automated system clearly shows the status of a suspicious activity case and prioritizes cases by due date so you can see, at a glance, what you need to do and when you need to have it done.

✓ **Centralized case management:** Centrally housing all material related to an alert investigation means you no longer need to draw information from a variety of sources. Case status and data are at your fingertips — and at auditors’ fingertips. When an auditor asks to see an example of potentially suspicious activity that you investigated, you can simply give them access to your alerts and they can review the associated notes and evidence, all in one place.

✓ **Easy e-filing:** A secure connection between your FI and FinCEN means you can file reports directly from the software — you no longer have to go through the BSA e-filing system website.
Seeing the Step-by-Step Differences

Using manual processes to detect and report suspicious activity can be time-consuming and labor-intensive. Here, I provide a comparison of manual and automated processes.

Think about the steps involved in manually processing SARs. Many compliance officers must take the following steps:

1. Examines all core banking system reports, looking for suspicious activity.
2. Evaluates any inter-office reports from frontline staff who think a transaction may be suspicious.
3. Sorts transactions from the reports in Steps 1 and 2 into two categories: those that are not suspicious and those that may be.
4. Investigates all transactions that may be suspicious and determines whether a SAR is necessary.
5. Manually creates a case file for transactions that were reviewed.
6. Adds notes to all files that were created in Step 5, indicating if he or she thinks the activity is suspicious and what further action will be taken.
7. Creates SARs for transactions that warrant them.
8. Prints and files a copy of the SAR for the FI’s records.
9. E-files a copy of the report via FinCEN’s e-filing website, where he or she must complete another set of steps.
Reaping the benefits of automation

Washington, D.C.–based Industrial Bank oversees $361 million in assets. Its BSA officer recognized the need for an automated system to streamline her workload and reduce her fear that she wasn’t catching all suspicious activities. Reviewing seven or eight monthly reports, several of which were hundreds of pages long, was time-consuming. The high volume of transactions reported made catching all suspicious activity difficult, especially because the transactions were reviewed in isolation, without a big-picture overview.

Since installing a software solution that applies artificial intelligence to the analysis of financial data, she has much more confidence in her FI’s BSA program. Rather than manually reviewing hundreds of pages of transactions herself, she has the software analyze customers’ behavior and flag any suspicious activity. The software produces alerts that offer an explanation of why the behavior seems suspicious, and she reviews the alerts and the evidence and then decides what steps to take.

The software’s e-filing capability means she no longer has to manually file SARs. Now she just pushes a button, and the reports are on their way into regulators’ hands. She also appreciates the case management component of the software, which keeps all material related to an alert — transactions, evidence, filed reports — in one place. Everything related to the investigation is centrally housed and easily accessed.

With the new system in place, she spends as little as 30 minutes a day reviewing system-generated alerts, a significant reduction from the hours she used to spend reviewing transaction reports. And Industrial Bank catches more suspicious activity. Over the course of 2009, it filed ten SARs. After the new system was installed, it filed ten SARs in less than six months.
On the other hand, with a behavior-based system, your compliance officer can focus on the suspicious activity, and quickly proceed through the following steps:

1. Reviews the system-generated suspicious activity alerts.
2. Evaluates any inter-office reports from frontline staff who think a transaction may be suspicious.
3. Investigates any of the transactions flagged in Steps 1 and 2 to determine if a SAR should be filed.
4. Clicks the button to open a case electronically and enters details of the decisions made.
5. Completes and files any necessary SARs electronically.
Part VI

Ten Tips for Choosing an Automated System

In This Part
▶ Automating your processes
▶ Maximizing your investment
▶ Easing the transition

Part V of this book details the advantages of automating your suspicious activity detection and reporting processes. If you decide automation is right for you, make sure you get the most bang for your buck by considering the following ten tips when shopping for software.

Delegate Detection
Say good-bye to painstaking, eye straining manual transaction reviews. Choose software that reviews the transactions for you and produces risk-rated suspicious activity alerts, complete with evidence of the suspect activity.
Go with the Workflow

Not everyone can be as hyper-organized as, say, Martha Stewart, so select software that provides you with an easy-to-follow workflow and prioritizes your reports by due date. Organized workflows, prioritized to-do lists, and on-time submissions — these are good things.

Find Flexibility

Sometimes you may need to add transactions, subjects, or other details to existing reports. Make sure to find an automated system that’s flexible enough to permit any necessary changes.

Automate Your Report Completion Process

Look, Ma, no hands! Your system should allow for the simple retrieval of customer information so that reports can be completed in a snap. Choose software that pre-populates your SAR (except for the narrative section) using data from the relevant alert or case, eliminating the need to reenter key data. Use the time this saves to create knockout narratives.

Get Connected

Your software should offer a secure connection between your FI and FinCEN (the techies call this a virtual private network, or VPN for short). A VPN allows you to submit reports directly and immediately to FinCEN via the Internet, eliminating the hassles of filing through the BSA e-filing system website, and worries over late filing.
Consider Storage

FinCEN requires you to keep your SAR data for five years from the time of filing. Choose a system that stores this data for you.

Automated systems should have the capacity to maintain all your SARs for the five-year minimum. This means you’ll have everything at your fingertips when the auditors come calling or law enforcement needs your help.

Take a Customer-centric Approach

Find a system that lets you see everything a customer is doing at a glance, without having to draw information from different external sources or look at transactions in isolation. Reviewing a customer’s overall activity gives you a better idea of what he or she is up to and makes identifying suspicious behavior easier.

Get More for Your Money

Seek a software vendor that provides value-added services such as core system integration and end-user training as part of the implementation. Proper training and documentation help you get the most out of your particular solution.
Kick the Tires on Technology (But Don’t Forget to Look Under the Hood, Too!)

Asking your technology vendor lots of questions helps you understand what the solution provides, such as a way for you to deal with things like repeat alerts on the same customer. But you also want to make sure it’s easy to use. So take it for a test drive — a free product trial helps you manage risk and make an informed decision.

Keep It Simple

Let’s face it: Upgrading your system is pointless if your staff can’t figure out how to use it. The whole point is to increase efficiency and effectiveness, which is tough to do if employees spend too much time figuring out the new system. Installing an easy-to-use system reduces employee stress and training costs, and makes everyone happier.
SARs in action.

Go to www.verafin.com/sar-overview to see how Verafin can help improve your SAR process.

Visit www.verafin.com for complimentary:
Videos • White Papers • Case Studies
Educational Webinars • Product Demos
More of the For Dummies e-book series