ANALYZING BANK RECORDS



Association of Certified Fraud Examiners

GLOBAL HEADQUARTERS • THE GREGOR BUILDING
716 WEST AVE • AUSTIN, TX 78701-2727 • USA

I. INTRODUCTION

Course Objective and Overview

This workbook is designed to teach the reader how to analyze bank records. Upon completion of this course, the reader will have learned about the various types of bank records, how to interpret them, the detection methods used to uncover varied illegal activities through bank records, and the formats used to present these activities in graphics and writing.

After this course, the reader should be able to:

- Recognize common entries in bank records.
- Compare methods of analyzing bank records.
- Identify indicators of illegal activity in bank records.
- Recall which graphics are used to portray financial data.
- Determine conclusions and recommendations after analyzing bank records.
- Distinguish the major laws and agencies governing bank records.

There are eight chapters in this course:

1. Introduction
2. Obtaining and Interpreting Bank Records
3. Finding Leads in Bank Records
4. Uncovering Patterns in Bank Records
5. Identifying Indicators of Illegal Activity in Bank Records
6. Using Graphics to Depict Bank Records
7. Applying Critical Thinking to Bank Records
8. Case Study

Also included are three appendices with information on bank record laws and regulations, "know-your-customer" (KYC) information, and reporting forms.

After several of the chapters, there are review questions to test the reader's understanding of the material. There are also exercises after several of the chapters that will give the reader an opportunity to use some of the skills described in the text. By using realistic files, the reader will be able to see how these techniques can be applied in real-life situations. The answers to the review questions and the exercises are at the end of this course.

A note regarding the use of the material: Purchasers may lend or give the workbook to someone else, but only the purchaser may receive CPE credit. Students may also use the materials for training purposes, but they may not duplicate the files or the workbook without the express written consent of the Association of Certified Fraud Examiners. To do so is illegal.

To receive CPE credit for this course, students should follow the instructions on the enclosed scantron form and return it to the ACFE. Alternatively, they may take the exam online. To access the online exam, use the link included in the order confirmation. Students can also access the exam through ACFE.com. Visit ACFE.com/OnlineCPEgrading for additional instructions.

We trust that purchasers will find this course helpful and rewarding. We welcome any feedback, corrections, or suggestions. Please send any comments to research@ACFE.com or to the Research Department, Association of Certified Fraud Examiners, 716 West Avenue, Austin, TX 78701, USA.

Certain portions of this course are derived from *A Guide to the Financial Analysis of Personal and Corporate Bank Records* by Marilyn B. Peterson.[1]

Components of Bank Record Analysis

Bank record analysis is integral to many criminal and civil investigations and inquiries. "Following the money" helps decipher criminal motives and uncover profiteers. Some of the reasons to use bank record analysis include:

- Uncovering criminal profits
- Identifying criminal assets
- Determining the lifestyle of an account holder
- Determining the financial health of an organization
- Discovering the facilitation of money laundering
- Uncovering previously unknown connections between entities

Investigators, auditors, and fraud examiners should understand how to analyze bank records and that it is most successfully done using a thorough process, such as the one described in the following list. This 14-step process was developed using decades of experience with financial records:

- Plan for the collection of the records.
- Obtain and inventory the records.
- Develop a schedule, database, or spreadsheet template for the records.
- Place the records into the template.
- Review the records for investigative leads.
- Review the records for patterns.
- Identify unusual deposits or payments.
- Compare the records to known indicators and schemes.
- Analyze flows among multiple accounts (if present).
- Create graphics if necessary.

[1] Marilyn B. Peterson, *A Guide to the Financial Analysis of Personal and Corporate Bank Records* (Richmond, VA: National White Collar Crime Center, 2002).

- Prepare a summary of the financial activities.
- Develop conclusions from the records.
- Make recommendations based on the records.
- Collate materials and present to management.

Plan for the Collection of the Records

Before analyzing bank records, examiners must develop an investigative plan, which should include determining what financial records should be collected. The investigative plan includes the theory of the case (i.e., what illegal activities might have occurred), a summary of the facts known to date, a list of necessary evidence and where it might be found, and the estimated time the investigation will take before it is completed. Pitfalls that might be present and the probability of success of the investigation should also be noted.

Deciding what records to acquire and what time period to cover is essential. Typically, the fraud examiner should look for documentation of deposits and withdrawals for a specific period. Banks are required by law to keep everything needed to reconstruct transactions in an account for at least five years.[2]

Moreover, examiners must focus the scope of the investigation. If, for example, only major expenditures are of interest, limit the records requested to only those over a specific threshold (e.g., those over $100, $500, or $1,000).

Also, when investigating an individual or company, fraud examiners should focus their efforts on the relevant period. They should obtain the records for a period beginning at least six months before the criminal activity occurred; this will allow them to establish a baseline with which to compare post-criminal activity. But when fraud examiners are only looking at a few transactions, they might limit the time frame to a few weeks before or after the date of the deposits or withdrawals, if appropriate.

Obtain and Inventory the Records

Once examiners have determined which records to collect, they should obtain and inventory them. There are several ways in which fraud examiners can gain access to bank records in the United States, including through a subpoena, a search warrant, or prior consent of the person being investigated.

Most often, the examiner will obtain bank records by subpoena or other court order to produce the relevant documents and records. A *subpoena* is a legal order to produce documents, witnesses, or other things. Subpoenas and other legal processes, such as depositions, interrogations, and document requests, are available if a legal action has been filed.

[2] A synopsis of laws relating to financial records held by depository institutions is found in Appendix A.

A *search warrant* is a court order that grants authorities the right to search premises or property for information pertinent to the case. If a search warrant is required, the examiner must address additional considerations. All warrants must satisfy the requirements of the Fourth Amendment, which protects people from unreasonable searches and seizures by the government. Thus, the warrant must specifically state what types of records are expected to be found and the reason they need to be collected during the service of the warrant.

Bank records can be found at a home or office, or at the office of a hired financial professional such as an accountant or bookkeeper. This approach of obtaining bank records, however, will only gather the bank statements and the checks that were written on the account; it will not give the fraud examiner full information on debit and credit memos, wire transfers, cashier's checks, and so forth.

Examiners may also receive prior consent to obtain the records. But acquisition via the account holder's prior consent will only allow fraud examiners access to bank statements and checks that were written on the account. Prior consent would occur if, for example, an individual, as part of an application or other agreement with a company or agency, agreed to provide their financial information to the company or agency.

Additionally, the fraud examiner should inventory the requested bank records as they are received. The most important reason for making an inventory of bank records is to allow the examiner to know which records, if any, are missing. Making an itemized list also allows the examiner to work with the financial institution to obtain them. Quite often, banks will first provide copies of the account statements and ask fraud examiners to highlight the specific items for which they need copies.

Develop a Schedule, Database, or Spreadsheet Template for the Records

After reviewing the records, the fraud examiner should enter the records into a spreadsheet or database for further analysis. By placing the records into a standardized format, the fraud examiner will be more easily able to compare records, uncover patterns, and extract various representations of the data. Chapter 2, "Obtaining and Interpreting Bank Records," contains an example of typical fields used in a database for bank records.

Place the Records into the Template

Examiners should consider placing the records into a template. If, however, the information is entered by someone else (e.g., an analyst or a clerical support person), fraud examiners should work closely with that individual to ensure that the data is entered accurately.

Review the Records for Investigative Leads

The examiner must also review the records for leads. Chapter 3, "Finding Leads in Bank Records," covers extracting investigative leads from the records. In the interim, it should be noted that one of the keys to a successful bank record analysis is to extract all possible information from the records.

Review the Records for Patterns

Next, the examiner must look for patterns in the data. Chapter 4, "Uncovering Patterns in Bank Records," includes the various types of patterns that can be found in bank records. For instance, some of these patterns can be found in dates, payees, deposits, endorsers, signatories, income sources, types of expenditures, and locations of expenditures.

Identify Unusual Deposits or Payments

The examiner must also identify any unusual deposits or payments. Sources and destinations of funds can be categorized as usual or unusual. Unusual sources and destinations should be mentioned in any thorough data analysis. These are also covered in Chapter 4, "Uncovering Patterns in Bank Records."

Compare the Records to Known Indicators and Schemes

It is also important that the examiner compare the data to common fraud schemes and potential red flags of fraud. Various types of fraud involving bank records have been uncovered in the past, and researchers have identified red flags that indicate an elevated risk of fraud. Some of these schemes and associated red flags are discussed in Chapter 5, "Identifying Indicators of Illegal Activity in Bank Records."

Analyze Flows Among Multiple Accounts if Present

Often, the examiner will review and analyze more than one account at the same time. If a business is suspected of involvement in an illegal activity, the fraud examiner should review the accounts of the individuals involved in the business to see whether they are a potential destination of illegal funds. Likewise, an individual involved in illegal activity might have multiple accounts through which funds are moved to confuse their eventual destination.

Create Graphics if Necessary

It might be necessary for fraud examiners to translate some of their data into graphic figures, so the information is more easily understood by others. Graphics are an excellent way to explain financial data clearly. The types of graphics that can assist in a bank record analysis include pie charts and bar graphs, time-series analysis charts, timelines, and commodity flow charts. Chapter 4, "Uncovering Patterns in Bank Records," demonstrates some of these techniques.

Prepare a Summary of the Financial Activities

Additionally, the examiner should prepare summary statements of income and expenditures by time. Summaries can be numeric or narrative, and the time is usually broken into months, quarters, or years.

Develop Conclusions from the Records

When analyzing bank records, it is important to look at not only what types of transactions have occurred, but also at what they mean. This is done by using deductive and inductive reasoning and logic, and this topic is covered in Chapter 7, "Applying Critical Thinking to Bank Records."

Make Recommendations Based on the Records

Once examiners have derived meaning from the transactions, they should make recommendations for further investigation or action. These matters are also covered in Chapter 7, "Applying Critical Thinking to Bank Records."

Collate Materials and Present to Management

The final step in analyzing bank records is to create a logical report and present it to management or the client.

Overview

The methodology discussed above focuses on providing an in-depth look at the available records, and this self-study is designed, in part, to provide the reader with a logical and consistent technique for dealing with bank records.

Tips

- When searching for assets, the fraud examiner should not limit the search only to records containing large check amounts. A large asset (e.g., car, boat, or vacation home) could have been paid for with cash, and checks for smaller amounts might have been written for expenses pertaining to the large assets (e.g., storage, insurance, or utilities).
- When fraud examiners are attempting to determine a subject's lifestyle, they should review all checks and deposits in the subject's accounts when they have such access. These checks and deposits can be used to reconstruct the subject's living expenses and asset purchases over the desired period.
- With the account holder's permission, anyone can be a signatory on an account. Therefore, fraud examiners should obtain records from all the accounts to which a person is signatory rather than limit their searches to those on which the individual is the sole account holder.
- Bank records include more than checks written on the account. Fraud examiners should obtain and review all other types of documents that can provide insight into an entity's financial business.