PacificCPE

COURSE
21752B

Forensic Accounting: Data Investigations

Not every situation calls for a full forensic investigation — and knowing the difference matters. This module examines the conditions that make a Data Sleuth investigation necessary, the key factors that shape how one should be structured, and how to communicate effectively with clients throughout the engagement. You'll gain practical guidance for setting clear expectations, defining the scope of your work, and keeping clients appropriately informed and involved from start to finish.

CREDIT HOURS 2 | FIELD OF STUDY ACCOUNTING | EXAM QUESTIONS 10

Start Course ↓ | Final Exam Copy ↓

LEARNING ASSIGNMENTS AND OBJECTIVES

Assignment

- Study the full course materials included here.
- Complete the review questions after each chapter.
- Answer 10 final exam questions.
- Final exam is scored immediately, 70% or better passes.
- Certificate of completion is available in your account.
- Failed exams can be retaken free of charge.

Course Objectives

- Recall the term that refers to the theft of cash, inventory, equipment, or any other item of value.
- Recognize the author's fraud formula.
- Identify common types of information requested for cases involving an individual dispute.

Copyright Notice

© 2026 Pacific CPE, LP. All rights reserved.

The materials in this course — including the text, illustrations, exhibits, examples, exam questions, and review questions — are the copyrighted property of Pacific CPE, LP. No portion of this course may be reproduced, stored in a retrieval system, distributed, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise) without the prior written permission of Pacific CPE, LP, except for the personal, non-commercial use of the registered learner.

Pacific CPE, LP grants the registered learner a single-seat, non-transferable license to access this course for the purpose of completing the associated continuing professional education credit. Account credentials may not be shared. Group access requires a separate enterprise license.

This course is provided "as is" for educational purposes. While Pacific CPE, LP makes a reasonable effort to ensure the content is current and accurate, the materials should not be relied upon as a substitute for professional advice. Pacific CPE, LP disclaims all liability for any error, omission, or loss arising from the use of, or reliance on, the course content.

Questions about reproduction, licensing, or use of these materials should be directed to support@pacificcpe.com.

Publication Date: July 2026

TABLE OF CONTENTS

CHAPTER 01

The Data Sleuth Necessity 5

1.01 Forensic Accounting Engagements Versus External Financial Statement Audits 6

1.02 The Evolution Of Forensic Accounting 7

1.03 The Case Of The Cash Back Payroll Scheme 9

1.04 Start With The Evidence, Not The Scheme 10

1.05 The Case Of The Gambling Executive Director 11

Test Your Knowledge 15

CHAPTER 02

Data Sleuth Considerations 17

2.01 Investigations Affect Real People 18

2.02 The Fraud Formula 21

2.03 Staying On Task With Purpose In Mind 22

2.04 Figure 4.1 Illustration Of An Investigation Decision Tree. 24

2.05 Recovery Avenues 28

2.06 Table 4.1 Examples Of Bank Statement Transactions Or Images And Corresponding Financial Institution Items. 31

Test Your Knowledge 34

CHAPTER 03

Client Communication And Involvement 40

3.01 The Case Of The Initial Client Meeting 40

3.02 Client Expectations 43
3.03 Data Procurement 45
3.04 Client Involvement During An Investigation 46
3.05 Ongoing Client Communication 49
Test Your Knowledge 50

Final Exam Copy 61
Glossary 54
Index .....

Chapter 1: THE DATA SLEUTH NECESSITY

Chapter Objective

After completing this chapter, you should be able to:

- Recall the term that refers to the theft of cash, inventory, equipment, or any other item of value.

Although the definition of Data Sleuth to describe the work of our team did not originate until more recently, the Data Sleuth Process was developed out of a necessity for me starting a solo firm early in my career. The more I applied a data-focused strategy to cases, no matter the type of organization or scheme alleged, I gained confidence. I knew that if I could identify the best and most reliable sources of evidence determining the legitimacy of a client's allegations from the beginning of an engagement, I could then answer clients' questions early in the process instead of right before a deadline and would be found reputable as an investigator and testifying expert. What began as an effort to prove my legitimacy as an expert resulted in the creation of a professional team that has consistently provided answers to clients' questions in the most complex of cases using the Data Sleuth Process.

Forensic accounting engagements and fraud investigations are not detailed external financial statement audits. They are methodical, process driven, data-focused investigations targeted at answering the most popular client questions of "What happened?" and "How much money did I lose?" External financial statement audits, in general, remain an integral part of many organizations because they provide assurance as to the fairness of the representation of the information presented in financial statements. Additionally, external financial statement audits can contribute to an organization's fraud prevention strategies. However, they are not a replacement for proper internal controls or as a tool to detect fraud.

A widespread increase in the availability of financial data processing technology has provided opportunities to expand the application of forensic accounting procedures, to increase the efficiency of investigations, and to broaden the scope of an investigation beyond just the identified subject. As technology continues to be developed for purposes beyond our imaginations, data, and the information that can be derived and interpreted, may be endless. Although the Data Sleuth Process may have been developed out of necessity because I had nothing to rely upon except data, financial data, financial data analysis, and their uses in investigations are here to stay.

FORENSIC ACCOUNTING ENGAGEMENTS VERSUS EXTERNAL FINANCIAL STATEMENT AUDITS

Frustrated by the number of years a fraud scheme continued while having external financial statement audits is all too common with our clients. In working with the management of organizations that have been victims of occupation fraud, or fraud perpetrated by an employee, we find that they commonly believe external financial statement audits should have detected the scheme. It is not until after their engagement with our firm that they truly realize the distinctions between a forensic accounting engagement and an external financial statement audit. Although the two may seem similar conceptually to someone not in the profession, they both serve distinctly different purposes.

In 2014, while working cases as a solo practitioner, I contracted on audit engagements to gain experience with external financial statement auditing procedures and using data analytics software. It was through these engagements that I began to appreciate the purpose of audits while recognizing stark differences between external financial statement audit procedures and forensic accounting procedures. Many of the procedures assigned to me were routine in testing internal controls and statutory compliance. Testing for internal controls involves an evaluation of the business procedures and corresponding duties assigned to personnel. The auditor evaluates whether there is accountability built into the procedure that would prevent or detect fraud should it occur in the process. Having solely worked investigations for eight years, I did not always understand the purpose of some of the procedures; therefore, I would often ask a supervisor or manager about the purpose of the procedure before beginning the assignment.

External audit procedures can be updated to address areas of concern, but sometimes, procedures are carried over year after year without considering their effectiveness or ongoing purpose. One such procedure was the comparison of a sample group of system exported check register entries and the corresponding paper check stubs. The paper check stubs were generated from the same system as the check register. Ultimately, I was comparing a data source to itself – which in some situations is valuable when testing for the accuracy of an exported report prior to performing data analysis. However, that was not the situation. From a Data Sleuth perspective, an improved procedure would be to compare the sample transactions from the system exported check register to the corresponding checks on the bank statement to ensure that the information in the system represents what actually cleared the bank.

If an organization is concerned about the fraud risk in an organization, an external financial statement audit will not likely detect it for several reasons, but ultimately, because a financial statement audit is not designed to detect fraud. It is simply the wrong tool for the job. The deadlines alone restrict the auditor's ability to examine in detail the individual transactions that make up the balances on the financial statements. The design of an audit includes mandated deadlines requiring an audit to be completed for some organizations in as few as 45 to 60 days. Even as the use of data

analysis has improved the efficiency of audits and allowed for more strategic testing of transactions, there is still a constraint of time.

In providing an opinion on whether financial statements are fairly presented, financial statement fraud may be identified; however, the most common fraud schemes faced by businesses, not-for-profit organizations, governments, tribes, or schools are those of asset misappropriation, and many of the clients we serve do not have internal audit departments. Asset misappropriation refers to the theft of cash, inventory, equipment, or any other asset of value. Asset misappropriation schemes comprise multiple transactions that when combined over the life of the scheme may be material in total. However, over the course of a year, asset misappropriations in transaction value fall below most materiality thresholds established in an audit. Not to mention, many transactions representing the individual occurrences of theft are charged to profit and loss accounts whose balances are closed at the end of each year to retained earnings. Thus, the totality of the amount stolen over time is less obvious – especially in an organization with total revenue necessitating an annual external audit – such as a company that is publicly traded.

Although it may not be the specific intention of an external financial statement audit to detect fraud, it is possible. Additionally, an audit contributes to a fraud prevention program by decreased fraud risk in an organization to the extent that employees believe an auditor could detect their scheme. However, if an employee understands the audit procedures, he may be able to conceal the scheme, making it undetectable by the auditor. If an organization wants to prevent or detect fraud, or investigate fraud that has already happened, an external financial statement audit is not the most effective tool.

THE EVOLUTION OF FORENSIC ACCOUNTING

When I first started working in the private sector, I noticed several perceptions about forensic accounting engagements. The first perception about forensic accounting, from accountants and clients alike, was that forensic accounting engagements were essentially detailed audits with the involving procedures to examine any and all transactions within an organization – or at least in the area of the alleged occurrence of misappropriation of funds. Obviously, this approach created a perception with some clients that to request such an engagement would be cost prohibitive from the start. For other clients, the cost of the investigation itself did not feel justifiable as the client had already suffered a financial loss and knew that not much of the loss could be recovered. Then, there were others who, even though only a fractional part of the loss stolen may be realized, still believed the engagement would provide value because they could learn how the fraud occurred and receive consultation on how to prevent it in the future. The accountants' and clients' perceptions were not entirely wrong.

Familiar with the manual labor process of data entry, it was no surprise that cases in the private sector required the same manual labor process of gathering and entering data that I experienced

when working with law enforcement. A significant difference between public and private sector investigations was a client's budget for the investigation. Although cases I worked on with law enforcement began with the manual data entry of all known bank statements, credit card statements, and the like, such work could be extremely cost prohibitive for private sector clients. Optical character recognition technology (OCR) was being used to search PDF documents but was not yet used to facilitate the importing of financial data into spreadsheets or accounting systems.

Because of the cost of digitizing financial information, private sector investigations seemed to begin by first identifying the scheme a client was alleging about a subject and then the investigator would try to find corresponding data/evidence to determine if the allegation was verifiable. Evidence of the scheme would be collected and documented, and a loss was quantified. This approach reduced the fees that would have been incurred from manual data entry; however, it greatly limited the scope of the investigation.

In order to perform the procedures beginning with an alleged scheme, case planning had to be based on understanding the characteristics of the alleged scheme and comparing the characteristics to the evidence available. An investigation could have several schemes for which this same process was followed. Although this method was successful with clients' cases, I personally did not enjoy the constant internal nagging and concerns. I worried that I might overlook something pertinent to the case, or that had I looked at other evidence, I would have drawn significantly different conclusions. The unsettled feelings led to constant reading, attending trainings, and inquiring of more experienced investigators so I could build up my mental database of schemes and corresponding characteristics. This approach also caused me to enter engagements already suspicious of the client's motives behind hiring a forensic accountant. Was a client singling out an employee because the allegations were true, or was the employer needing a way to fire an individual who was causing problems? This assumed requirement to trust that my clients' intentions were honorable was nearly impossible for me – no matter the client.

By the time I founded Workman Forensics, financial data processing technology was improving, but it was too expensive for my small firm. My desire to return to what I had learned at the Federal Bureau of Investigation (FBI) and to work cases once again from a data focus encouraged me to improve the process of digitizing data. I performed continuous research to find a more technologically advanced, but budget friendly, solution. Several years later, I discovered a technology solution while browsing the exhibition hall at the Association of Certified Fraud Examiners Conference. The improved automation of extracting financial information from PDF documents into a spreadsheet was a game changer for me and my firm.

As I was able to import data more efficiently, I could then switch the investigation starting point from a scheme identification approach to a data-driven approach and still work within a reasonable client budget. For example, rather than just looking into a known payroll scheme of one employee, we could look at the payroll data for all employees and identify outliers. The outliers discovered did

not automatically indicate fraudulent payroll had been discovered, but it was an opportunity for further discussion with the client. Looking at an entire data set instead of something piecemealed or cherry-picked by a client gave me greater satisfaction that the investigation was objective. Finally, it reduced the need to trust a client's intentions; I could simply address their concerns and let the data-driven results speak for themselves.

THE CASE OF THE CASH BACK PAYROLL SCHEME

Vince had been out at the ranch and missed a call from a number he did not recognize. Listening to the voice mail, he heard, "Hi Vince. This is Gina. I work for your company under Jane. I really need to talk to you." Vince immediately redialed Gina's number and set an appointment to talk with her the following day off site. Gina's hands were shaking as she carefully told Vince about a conspiracy in the home office. The conspiracy she described existed between Jane who was the chief executive officer (CEO), the chief financial officer (CFO), and other managers and supervisors. Vince was shocked, blindsided, really. He diligently reviewed his company's financial statements every month. The balance sheets and income statements were consistent, and the CFO had paid every shareholder distribution on time and without any discussion of cash flow issues. He knew Gina was well liked and part of the core team and would not risk that position to tell him something untrue, but he just could not believe it. Vince encouraged Gina to tell him all she had seen and heard so he could chart a course of action.

Jane had positioned herself to be responsible for payroll, even though it was outside the job description of a CEO. She would overpay the core team employees and then place envelopes on team members' desks with a handwritten amount on the front of the envelope. The team members knew that Jane expected them to return to her in the envelope the indicated amount of cash when their paycheck deposited. For example, if Jane overpaid an employee by $1,000, the envelope may have $500 written on the front. That employee was to return $500, and then he was able to keep $500 net of all the taxes that would be due on the extra $1,000.

Later that evening, Vince began to research Gina's allegations. Slowly but surely, he confirmed the worst – a team of trusted employees were stealing money. Vince interviewed the four employees from the list Gina prepared; they all immediately confessed. Then, Vince hired Workman Forensics to help him establish the amount of money missing. Although Gina advised about the employees involved in the scheme, and those interviewed confessed, I asked Vince if we could expand our scope to look at all home office employees – not just those known at the time. We had recently procured data analytics software to pair with our data processing system. I explained that if we ran our analysis on all home office employees at the same time, not only would he know who was involved based on data evidence, but it would be more efficient than generating a loss analysis every time he learned about another involved employee through the grapevine. Vince agreed to this

method and provided us with the timesheet records and payroll reports from the provider for all home office employees.

Comparing the hours in the timesheet data to the hours paid in the payroll reports, we immediately identified 28 employees who had been paid for more hours than they worked. Most of the differences were between 150 hours and 300 hours, and the primary players in the scheme had been overpaid for between 4,000 to 5,000 hours over the five-year relevant period. The loss to the company and Vince was $208,000.

If our investigation focused only on those individuals Gina reported, Vince would have had a loss of $170,000. An additional loss of $38,000 was quantified that could be included by Vince in his recovery efforts moving forward. More significant than this, however, was that the analysis of looking at all home office employees identified that Gina had been overpaid during the period by 500 hours.

START WITH THE EVIDENCE, NOT THE SCHEME

An FBI agent approached my cubical holding a banker's box to ask me if I would process the bank statements contained in the box for an investigation. As the student trainee working under a forensic accountant, entering bank statement information into a spreadsheet was my primary job and responsibility, and I had become extremely proficient in the first year of employment. I accepted the massive box of statements and got to work. As I entered each row of information, I became familiar with the repetitive activity within the accounts. When I saw the case agent the next week, I asked about the case. He obliged and explained the allegations and potential related charges. Within this discussion, I learned that the case involved a pump-and-dump stock scheme. The agent explained that a group of professionals were conspiring to promote penny stocks to victims; whenever the stock price would reach a certain price range, the professionals would sell their shares to make a lot of money. The people they had recruited to invest in the stock, the victims, would lose money. Knowing this information helped me identify patterns or indications in the bank statement data that might lead to recovering assets. My favorite types of transactions to look for while performing the data entry of bank statements were those that led to identifying assets and other related bank accounts for asset forfeiture purposes. Although I was not involved in the asset forfeiture process, I would leave a note for the analysts who were, and they would have a head start on their analysis. Such findings allow for possible forfeiture of the assets purchased with stolen money that, in turn, can be used to repay victims.

At the time, I did not know what kind of evidence was necessary to charge a pump-and-dump stock scheme, but as I continued to enter line after line of data, I kept the case story and charges in mind. One day, I entered a transaction in the amount of $450,000, identified as a wire transfer and the description on the statement included the word "Belize." I had not traveled much in my life by the time I was 20 years old, but my best friend in high school vacationed in Belize for her senior trip, so