FRAUD CASEBOOK

FRAUD CASE STUDIES

Lessons from the Bad Side of Business

Edited by
JOSEPH T. WELLS

ACFE
Association of Certified Fraud Examiners

Fraud Casebook

Fraud Casebook

Lessons from the Bad Side of Business

Edited by Joseph T. Wells

BICENTENNIAL 1807 WILEY 2007 BICENTENNIAL

John Wiley & Sons, Inc.

This book is printed on acid-free paper. ∞

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.

Wiley Bicentennial Logo: Richard J. Pacifico.

Published simultaneously in Canada.

The case studies presented in this book are based on actual cases. Names, dates, locations, and some facts have been changed to protect the privacy of the organizations and individuals involved.

All amounts are in U.S. dollars unless otherwise specified.

Library of Congress Cataloging-in-Publication Data:

Fraud casebook : lessons from the bad side of business / Joseph T. Wells.

p. cm.

Includes index.

ISBN 978-0-470-13468-9 (pbk.)

1. Fraud–Case studies. I. Wells, Joseph T.

HV6691.F737 2007

363.25′963–dc22

2007009247

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

For Barry C. Melancon:
A true giant in the accounting profession

Contents

Preface

Fraud, as you will read in the following pages, is not committed by accounting systems or computers. It is carried out by living, breathing human beings who outwardly seem no different from you and me. Occupational frauds—those offenses that occur in the workplace—are all too common; nearly every company has been a victim or will be in the future.

It would be easy to say that this phenomenon happens because of greedy, dishonest people. But greed is a natural human trait. And all of us lie. So that explanation falls short of predicting who will turn to occupational fraud. More often, as you will see, fraudsters appear to be ordinary individuals who believe that they are caught in extraordinary circumstances. They are frequently upstanding, God-fearing, patriotic citizens who despise crime as much as the rest of us. Moreover, they don't really look at themselves as criminals. But they certainly are.

I have been fascinated with the motives and morals of white-collar criminals for close to 40 years. Preventing, detecting, and investigating fraud has become my life's work. It didn't start out that way, though; I graduated with an accounting degree and became an auditor before being accepted as a special agent of the Federal Bureau of Investigation. Fraud cases, large and small, were my bread and butter. After nearly 10 years, I left to start my own consulting firm specializing in white-collar crime issues. And in the late 1980s, I helped form the Association of Certified Fraud Examiners (ACFE), the world's largest antifraud organization, where I still serve as chairman.

Along the way, I've lectured to thousands of antifraud professionals, traveled to nearly every corner of Earth, taught in the graduate school at the University of Texas at Austin, conducted independent research on the causal factors of fraud, and written extensively on the topic.

This book, my thirteenth, pulls together the experiences of fraud examiners from across the globe, each of whom has provided details about a case he or she has investigated. Although the literary styles are as unique as the people who wrote them, all the chapters drive home a number of universal themes. First, those who commit fraud usually do so without a grand plan; instead, they made bad decisions, one after the other. Second, like water, fraud follows the path of least resistance. That is, these offenses are never more complicated than they need to be in order to accomplish the perpetrator's illicit goals. So you will notice that many of these schemes are the essence of simplicity.

Third, occupational fraud follows definite patterns. We first determined that fact in 1996 with the release of the ACFE's first *Report to the Nation on Occupational Fraud and Abuse,* which consisted of an in-depth study of over 2,000 actual cases furnished to us by certified fraud examiners. The *Report* has been replicated three times since then. We've been able to classify frauds by the methods used to commit them. There are three broad categories—asset misappropriations, corruption, and fraudulent financial statements—and there are numerous subschemes.

Fraud Casebook: Lessons from the Bad Side of Business is organized around these schemes, which has subsequently been dubbed the "Fraud Tree." Part I is devoted to the most common offenses, asset misappropriations. Part II covers corruption; Part III details fraudulent financial statements, the least common but by far the most expensive occupational frauds; and Part IV focuses on a variety of other fraud schemes.

Each case involves four areas. *Why* the fraud was committed is an important human interest story. *How* the fraud was committed gives the accounting and other technical details. *Lessons learned* offers sound advice on what went wrong. And *preventing future occurrences* shows what must be done to keep the same kind of schemes from happening again. You will notice that many of these stories don't have pleasant outcomes; justice was not served and lives were changed forever. My experience in this field has taught me that when fraud occurs, there are no winners. That makes prevention the ultimate goal. And that process begins with educating ourselves.

Lessons from the Bad Side of Business can be utilized by academics wishing to expose their students to the realities of fraud. It can easily be an accompaniment to one of several fraud texts, including my own, *Principles of Fraud Examination*. But practitioners, managers, and business owners will also learn a great deal in these pages. Finally, those with a general interest in occupational fraud will discover that this book is simply a fascinating read.

Thanks go first to the ACFE members who wrote the case studies. They didn't do it for money; the profits are earmarked for the ACFE General Scholarship Fund, which provides grants to deserving college students. Good writers know that there is nothing easy about this craft, and they are therefore commended for their efforts. Authors also are aware of the critical symbiotic relationship that exists with their editing team. John Gill, Kassi Underwood, and Andi McNeal of the ACFE Research Department did an outstanding job in that regard. Finally, I appreciate the assistance of Tim Burgard of John Wiley & Sons, Inc., who wouldn't give up until I agreed to take on this project.

Fraud is a serious problem that goes much beyond monetary losses. It costs jobs, raises, corporate reputations, and individual dignity. *Fraud Casebook: Lessons from the Bad Side of Business* will shed light into the dark corners of government and commerce so that we can hopefully avert, in the future, some of the same mistakes we have made in the past.

Joseph T. Wells, CFE, CPA
Austin, Texas
June 2007

PART ONE

Asset Misappropriation

CHAPTER 1

High Art, Low Value: How A Connoisseur Became A Convict

ELLEN A. FISCHER

If there were a law that required people to trade their names for a single adjective, Lawrence Fairbanks would be *Cosmopolitan*. A tallish, gaunt man of 45, Lawrence held the position of Assistant Vice Chancellor of Communications—the glitziest job in the glitziest department of Aesop University. In the vast sea of academe, Lawrence's ship steered clear of the lecture halls, laboratories, and weekly beer orgies on Fraternity Row. I doubt that Lawrence ever met a professor, much less a student. Instead, he sailed the waters of media and public relations. Lawrence was in charge of making sure that the university's good side was featured in every last magazine, newspaper, and brochure that dropped off the printer.

The position of AVC-Communications fit Lawrence like a second skin. He had been recruited by Aesop from a renowned magazine empire, and it showed. Two decades in the publishing world had secured him the professional trust and personal admiration of the writers, editors, photographers, and graphic artists who produced award-winning publications on behalf of the university.

Moreover, Lawrence wore the cultured charisma of a man well studied in the arts. His knowledge and taste far surpassed the better-known works you might guess on *Jeopardy!* or in a game of Trivial Pursuit. Lawrence was captivated by the black-and-white photography of the early twentieth century. He was versed in original oil paintings and ceramic pieces by important—though not mainstream—artisans in New York, San Francisco, and London. The breadth of Lawrence's interests included antiques—all kinds of antiques, ranging from old books to the earliest cameras, apothecary items, steam trunk luggage, and toys. Lawrence also had a fondness for period furniture of the sort you might find in a museum. Art was Lawrence's life.

Lawrence's high regard among the university communications creative staff was shared by the administrative employees who reported to him. Though fluent in the language of the elite, Lawrence Fairbanks was no snob. He always greeted the accounting clerks, the administrative assistant, and the receptionist by name. At Christmas, he arranged a destination luncheon and tour of the newly opened museum—the one that had a year-long waiting list. Every employee in the department was invited.

Lawrence's glad-handing social ease endeared his university colleagues and impressed the literati and glitterati of the media and art worlds. It also won him a lovely, intelligent wife. Having waited until his late 30s to marry, Lawrence was now the father of six-year-old Ruthie and three-year-old Bobby. It was touching to see how a keen art connoisseur had reserved the outer surface of his office desk as a minigallery for the framed works of his two little crayon masters.

Lawrence's wife, Allison, worked as a midlevel corporate attorney; despite their dual income, which exceeded $250,000 a year, the family home was unpretentious. In a city that sweats opulence, the Fairbanks' home stood unremarkably among other homes of its style in a neighborhood better known for its nearness to prominent cultural venues than its prominent residents. The cozy, single-story clapboard house of pre–World War II construction had three bedrooms and a single bathroom. It was just big enough for four people who, by all appearances, followed the script of the American Dream.

But there was more to Lawrence's life than his wife, his children, and his job—and there was certainly more than met the eye to the way he approached his love of art. Normally, when one speaks of a love of art, one refers to a hobby that provides enjoyment and enrichment. Normally, one's most cherished pieces are shared with family.

Normally.

We often hear that the most public personalities can mask the most private souls. And, while the inner reflections of a private soul are normal, the secret, shame-driven need for certain objects is called "obsession." No one—not even Allison Fairbanks—knew the extent of Lawrence's love for art, nor the lengths to which he would go to acquire it, hide it, and ultimately dupe employer and supplier alike into feeding his passion.

Art nourished Lawrence's troubled heart even as it starved his soul to death.

Art was Lawrence's life.

The Face of Many

Aesop University, the largest campus in a state university system, enjoys an eminence that rivals the Ivy League. Founded in 1871, Aesop grew from a state teacher's college to an institution with a world reputation for scholarship, research, and community service.

Modestly put, the university produces and attracts the "Who's Who" of every imaginable field. Every orange and burgundy sweatshirt in the student bookstore proclaims its logo, *Omnibus Punim,* which is translated to mean "The Face of Many." Aesop's family portrait includes famous actors, Olympic athletes, a Supreme Court Justice, and several Nobel laureates. The Aesop Medical School successfully pioneers new treatments for the most hopeless conditions. Its doctors have ministered to the destitute and distinguished alike.

On any give day, Aesop's total student enrollment reaches 35,000 among its undergraduate, graduate, and professional schools. To keep this educational behemoth running, Aesop employs upwards of 25,000 staff and faculty. And though situated in the highest-rent district of one of the three largest cities in the United States, Aesop's 500-acre campus has earned the *über*-school its very own zip code. Aesop's football team, the Thundering Bison, has secured the celebrity campus a regular spot on the 11 o'clock news. More important, its $3-billion budget has won it a set of permanent box seats in the crosshairs of the state legislature.

The university's in-house business and technology experts have patiently guided this tradition-steeped grandfather of higher education toward the Information Age. With the steady, gentle prodding that got Daddy to trade his turntable for a CD player, Aesop eventually migrated from its old record-keeping system of manila folders and microfilm to the "Give-it-to-me-now!" world of computers.

By the mid-1990s, Aesop's entire purchasing and accounts payable system was computerized. Just enter a log-on ID and password, and an authorized employee is soon staring at any financial transaction processed in any of the university's departments. Push another few buttons, and you'll know which employee entered a purchase request before he or she fired it off to the campus's central Accounts Payable Department. You'll see the serial number of the university check and the day it was cut. You'll even know whether that check was sent out to the vendor through the U.S. mail or whether it was first sent back to the department that requested the payment.

Any business with as many moving parts as Aesop University must make sure that its bills are paid efficiently, but not recklessly. So along with the streamlining of the accounts payable process comes a few built-in security measures. One big safeguard is the university's purchasing policies—in particular, the policy that dictates spending limits.

Aesop's "Low-Value" Purchase Delegation Policy places a ceiling on how much any one campus department can spend with a single vendor on a given day without obtaining formal approval from the Central Purchasing department. Exceeding that limit causes the Materiel Acquisition and Disbursement (MAD) automated system to halt a department's purchase request and reroute it to campus's Central Purchasing unit.

That is, if more than $2,500 worth of business per day—plus a small additional margin for tax and delivery—is going to any one supplier, Central Purchasing will automatically gain control of the purchase. There are all kinds of good reasons, too—for example, making sure that old Aesop, a public university, is given the best deal in the marketplace and that it obeys a long list of state and federal laws.

You can almost see the buyers in Central Purchasing standing there, sneering, arms folded, tapping their feet and wondering what the accounting assistant in the Norwegian Poetry department was thinking when he ordered $2,984.32 worth of Viking translation guides from the Oslo Down company. That type of order immediately results in an e-mail from one of those sneering foot-tappers to the immediate supervisor of the accounting assistant in the Department of Norwegian Poetry.

You might question how a fiscally responsible outfit could extend so much green rope, every day, to a few hundred campus departments. Yet that is exactly the rationale behind the Low Value Purchase Authority—a mouthful of a term that simply means that a $3 billion university is placing up to $2,500-and-change worth of trust in any one department to buy whatever it needs from a single vendor on a given day.

The Low Value Order (LVO) policy allows an organizational giant like Aesop University to function more efficiently by not paralyzing Central Purchasing with routine, nonrecurring purchases. Sure, it involves a measure of risk, but the alternative is a mountain of overdue payments and a premier university with some really bad credit.

Aesop University's purchasing policies and automated safeguards served the institution well. But not for long.

Designing a Fraud

It began with a midmorning phone call from a hoity-toity furniture store—the kind that omits the word "furniture" from its name. A man identifying himself as "Squire's chief financial officer" called the Aesop University Internal Audit department and told our receptionist that he needed to speak to an auditor. He had to report a fraud.

Our receptionist directed the call, just as she did every other one that struck her as odd, to me. I am one of 25 audit professionals in the Aesop Audit department. Since Aesop is the largest of the 12 campuses in our state university system, there is more than enough work to occupy an audit staff of our size.

Ours is a department of specialty units dedicated to particular areas of the campus such as health care or, in my case, a specific discipline like forensics. Although six of us are Certified Fraud Examiners, I am the audit manager of investigations. That is, I am responsible for looking into matters of alleged financial misconduct. Or to be less euphemistic, alleged stealing.

I answered my ringing extension as I always do, with my first and last name. Satisfied that he had an auditor on the line, Mr. CFO repeated his announcement—he was calling to report a fraud. He knew it was fraud because Mr. CFO had previously been an auditor for a "Big 8" accounting firm.

Mr. CFO then informed me that he was holding a photocopy of Invoice Number 5432, bearing Squire's logo. The invoice, in the amount of $2,664, requested payment for "design and illustration services." It also made reference to one of Aesop University's fancy publications, *Bison Quarterly,* a glossy magazine with feature articles on our institution.

Mr. CFO continued. Invoice No. 5432, he said, was accompanied by a recently cut university check in the same amount, payable to Squire. Lawrence Fairbanks, the Assistant Vice Chancellor who oversaw our university's publications unit, had authorized the payment.

Fairbanks's signature was more than legible—it was artistic. Moreover, the billing and shipping addresses were in care of his university office.

"Just a minute," I said to Mr. CFO. "I can look up the invoice on our system." Using our MAD system, it took all of 90 seconds to get the electronic version of Invoice 5432 on my computer screen.

"Okay," I said. "Invoice 5432 certainly looks like a normal type of expense for the Communications Department." But, I wondered aloud to Mr. CFO, why was a furniture store calling me to discuss it?

Then the explosion:

Mr. CFO explained that the hoity-toity store personnel immediately recognized Lawrence Fairbanks as a regular customer, but they didn't know—or care—about his fancy university title.

And, while the invoice copy that accompanied the university check described "design and illustration services" for *Bison Quarterly,* Squire's own copy of that same invoice instead authorized the fabrication of a one-of-a-kind chaise lounge. Prophetically, this chair—or rather, this *chaise*—was named "Ophelia," the psychologically and physically doomed heroine in the Shakespearian tragedy *Hamlet.*

As I silently recalled a verse from our high school production, the Bard was trumped by this chilling quote from Mr. CFO:

"Lady, I don't know squat about magazines. Should I make the chair or not?"

Just the Fax

If there's one thing I know, it's that big guns make big holes, and I sensed that Mr. Lawrence Fairbanks had fired a cannon. I asked Mr. CFO to fax me everything he had that pertained to Invoice 5432. Within moments, I heard the tinkling of the fax phone in our copy room a few yards away from my office.

As I lifted the warm pages from the fax tray, I first inspected Invoice 5432, for $2,664, the version that Lawrence Fairbanks had enclosed with the university's check. It read "design and illustration services for *Bison Quarterly.*" Along came a copy of a low-value purchase order (LVO, for short) in the amount of $2,400. The $264 difference was for sales tax and delivery.

Finally, the fax printed out Squire's version of Invoice 5432. It looked similar to Aesop's copy. The layouts of the invoices were identical. The billing address, "Mr. Lawrence Fairbanks, c/o Aesop University Communications," was the same. Even the boxy, 3-D logos at the top center of the invoices matched.

But the descriptions of the purchases did not.

In the body of the Squire invoice, in place of "design and illustration services," were details for the fabrication of a one-of-a-kind "Ophelia Chaise." It gave precise instructions for the fabric and color—mauve damask, to be exact. It also contained a note that Squire was to contact Lawrence Fairbanks when the chair was ready.

While my first impulse was to carry my handful of trouble straight into the office of the audit director, Frank Adams, I slowly walked back to my own office to eat a banana and contemplate. Was this a one-time indiscretion on the part of a respected university official, or was this a slip-up in an ongoing scheme?

I clicked my mouse on the icon that led me back to MAD, and I input the department code for University Communications. The department had a $4 million annual budget. If I was going to find more examples of the "Squire type," I knew that I would have to drill carefully. I started by typing the four-digit code that the University Communications department used to identify publications expenses on the ledger.

A list of transactions cascaded down my computer screen. As I scrolled through them, I noticed that many of the amounts over the past year or two were under $2,500— many by only a dollar or two. I also noticed a number of "regular" payments in identical amounts, paid to the same vendors over the course of two to six months. The amounts were rarely under $1,000 and never more than $2,499.

I clicked open 20 payments. The online LVO and invoice details were similarly worded: "design and illustration," "stock photos," "reprints of original artwork," or "printing and layout." All made reference to an Aesop magazine, newsletter, or brochure.

Next, I examined the vendors' addresses. One was in San Francisco, another in New York, and still another in Chicago. Publishing ignoramus that I am, it made no sense that so much of the design and illustration work was done out of town. I chose one vendor named Lincoln Photography, partly because it had a San Francisco address and partly because MAD displayed six consecutively numbered invoices under the low-value threshold.

I Googled the address. Not surprisingly, what I got back was not Lincoln Photography, purveyors of stock shots, but Lincoln Galleries, exclusive dealers specializing in early twentieth-century black-and-white photographs snapped by artists who probably tortured themselves to death.

Finally, I broke the news to Frank, the audit director. He listened to my account of the phone conversation with Mr. CFO, the faxed Ophelia Chaise invoice, and the low-value payments to out-of-town art galleries. Frank uttered a one-syllable expletive, and, with that colorful pronouncement, he authorized me to proceed with a full investigation.

The central purpose was clear: to identify the bogus invoices, to quantify the total loss to Aesop, and to collect the evidence to prove it to the university police and the district attorney.

I started by isolating payments that fit a handful of criteria:

- One or more payments to a single vendor
- Under $2,500
- Consecutive or closely numbered invoices
- One-word vendor names
- Vendor address out of town, or out of the United States, or in a major city
- Vendor address in the "artisan" sections of our city

Given that University Communications was an artsy kind of business to begin with, I expected that my initial search for phony transactions would include some that were really A-OK. Yet I wanted to make certain that I wasn't dancing over any rocks that were covering up snakes.

Eventually, I identified 52 vendors and 200 LVO purchases that spanned a three-year period, and I obtained copies of the front and back of each cancelled university check.

You Can Take It to the Bank

As the paper drifted in, I started matching up the endorsements on the backs of the checks with the vendor names on the in-house versions of the invoices. Some of the mismatches were so obvious, it hurt. For example, the check that Aesop issued to "Redhill Publishing" in New York City was endorsed and deposited by "Redhill Antiquarian Books." The payee names on the checks were always close enough to the vendors' true names that they were less likely to notice the "slight" inaccuracy. In the end, vendors are far more concerned that the checks they deposit stay deposited—and you can take an Aesop University check to the bank.

Discretion was not only the better part of valor; it was the only way to keep an investigation of a high-profile character from a famous institution from being publicized prematurely. During these early stages, when we only had one invoice for a fussy purple chair, Frank decided to inform only his boss and campus in-house attorney.

My challenge was to have the vendors respond to my requests to mail and/or fax me copies of the authentic invoices without tipping our hand. Anyone who calls our main office number reaches a recording that announces, "You have reached the Aesop University Audit Department." I came up with a way to minimize the perceived stature of the department by transforming my name from Ellen the Audit Manager into Poor Ellie the Temporary Bookkeeper. Sure, Mata Hari is a more exotic nom de guerre, but Ellie was easy to remember.

I timed each call toward the end of the business day, adjusting for different time zones. That way, whoever answered the vendor's phone would know that Poor Ellie was stuck working late. I began each call by raising my speaking voice half an octave and beginning with the words "Um, hi."

The story was pretty much the same: Poor Ellie was slogging her way through thousands of university payment records. She had to make sure that Aesop's main Accounts Payable department had a copy of each and every invoice that it paid over the past three years. For some reason, the university lost a slew of invoices during that time, and Poor Ellie had to ask the vendors for copies. Poor Ellie had to get the job done—or else.

Pathetic? Sure, but it worked. In came the proof.

Fairbanks's methodology was obvious. He not only had doctored the description of the purchases, but he applied his own artistic flair—and some common desktop publishing tools—to redo the vendors' logos. In some cases, Fairbanks created a new letterhead for the vendor, eliminating telltale verbiage like "dealers in antiques since 1947" that might have alerted the support staff in University Communications and campus Accounts Payable.

Over three years running, Lawrence Fairbanks spent $475,000 of Aesop's money on lithographs, serigraphs, original oils, photographs, antique luggage, books, and cameras. Cartoons, sculptures, and ceramic pots. Strange space-age looking lamps with Swedish names. More fussy chairs. A phrenology head and three taxidermy specimens—all encased in glass; all incredibly dead.

It was time for me to interview Assistant Vice Chancellor Lawrence Fairbanks. Frank and I first met with Fairbanks's boss, Lennie Scott, to give him the background of the case and to solicit his assistance in getting Fairbanks to submit to an interview. Scott was surprised and outraged. Within 30 minutes of our meeting, he sent us a copy of the e-mail in which he instructed Lawrence Fairbanks to come to the Aesop Audit Department at 10 a.m. the following day to discuss some questionable transactions.

Decorating the Trap

Before Fairbanks arrived, I did some interior decorating in our conference room. On our massive, bleached oak conference table, I arranged the files for the 52 vendors in five open cartons, so that the folder tabs with their names were visible. Along the way, we also had gotten a private investigator to take snapshots of the buildings of the 30 or so local galleries and furniture stores that Fairbanks patronized. I opened the photo album to the picture of the Squire storefront and set it at the edge of the conference table, nearest the door.

Fairbanks couldn't miss it.

Lawrence Fairbanks arrived at the Aesop Audit Department reception area at 10 a.m. sharp. Frank and I each shook Fairbanks's hand outside the closed door of the windowless conference room where I had set up shop.

Frank led the way in and sat in one of the chairs across the table from where Fairbanks and I would sit next to each other. As I had learned in several Certified Fraud Examiner training seminars, my sitting beside Fairbanks would allow me develop the rapport that would, with a measure of luck, lead to his unburdening.

Neither Frank nor I expected what Lawrence Fairbanks did next. Upon eyeing the opened photo album and the cartons arranged on the conference table, Fairbanks pivoted on his heels, marched straight out of the room, and, with increasing velocity, through the reception area and out of the suite. I heard no *ding* from the elevator—he had taken the stairs.

Early that afternoon, Frank received a call from the campus attorney whom he had notified earlier about our investigation and our pending interview of Lawrence Fairbanks. Upon leaving the Aesop Audit suite, Fairbanks did not stop until he reached the office of his attorney, Arnold Kruger.

Kruger assured the campus attorney that Lawrence Fairbanks would return to Aesop Audit the very next morning and that he would cooperate fully in an interview. But there was a catch. Apparently, the connoisseur had kept nearly everything that he had purchased and was offering to assist the university in recouping the ill-spent funds by selling off the goods. Kruger was trying to dissuade Aesop's officials from prosecuting Fairbanks in the criminal arena by allowing him to make the university "whole" again.

Then there was the sympathy factor: Kruger explained that Lawrence Fairbanks was a very troubled soul who had been under psychiatric care. He was not a thief; he was sick, and he was prepared to make it all up to the university. The campus attorney told us that he would not recommend that criminal prosecution be avoided. However, he did make an agreement with Kruger that the university would support his client's efforts to mitigate the loss.

The next morning, Lawrence Fairbanks returned to the Aesop Audit conference room. Slouching in a maroon V-neck sweater, a 1960s rock band haircut overshadowing his ashen face, the connoisseur confessed. In carefully measured sentences, Fairbanks recounted how he got away with his first purchase—a $10,000 oil painting that he split into four "low-value" orders for "design and layout" services. In the earlier days, he would take an actual invoice, cut and paste the logo into a less telltale version of the vendor's name onto another sheet of paper, and photocopy the whole thing. Then he discovered it was easier to fabricate the entire invoice using simple word processing graphics. He began to crack a faintly proud smile.

"How did the vendors react to getting checks drawn on Aesop University's bank account and not yours?" I asked.

As I had guessed, the vendors really didn't care, and Fairbanks knew they wouldn't. Aesop is a player in the art world, and Fairbanks's position in the university was prestigious. No one questioned the fact that the checks were coming from Aesop. A few must have assumed that Fairbanks was purchasing art and fancy furniture on the university's behalf.

"Who else in University Communications knew what you were doing?" I asked.

Eyes intense, Fairbanks adamantly replied, "No one!"

Fairbanks explained that, as with most top-level officials, he did not do windows. That is, he had administrative employees processing the invoices—the sanitized versions. He even knew how to skirt the "checks and balances" in his department that provided for a secondary review of each transaction by an accounting supervisor. So long as there was a budget for the "publications" purchases, the busy accounting supervisor, always immersed in details, was not going question him.

And what of Fairbanks's wife?

With downcast eyes, Fairbanks began to sob as he proclaimed how much he loved Allison and dreaded how this was going to shatter her life. She knew nothing of his purchases.

A Thieving Pack Rat

But, how did Fairbanks keep Allison from knowing? Did he bring the merchandise home?

"No." He sighed. "That is my sickness."

Fairbanks unfolded the story of a poor child peering through store windows in a depressed downtown area. It had been his goal to gain the education and social standing that would gain him the finest things that money could buy. Along the way, Fairbanks branched out from the banality of department store goods and into the esoterica of fine art and antiques.

Even more than the acceptance he enjoyed from the art world, Fairbanks was following a noble calling. He was saving old, dark photographs of people who didn't matter anymore, even though their images had become collectors' items. He was preventing old books, antiques, and the strangest objets d'art from being erased from their place of honor in the world. And he was creating new pieces—like the Ophelia Chaise—that would be the antiques of tomorrow.

They mattered; he mattered. And he kept them from harm's way in a public storage facility. Over the past three years, Fairbanks had rented three contiguous storage rooms in one of those "You-Haul-It, You-Store-It" places. Many items, he assured me, were still in their original packing.

Aesop University was not paying for the storage. I checked.

Before our interview concluded, Fairbanks had a question for me. I thought he was going to raise the usual concerns about what would happen next, whether he would go to jail, and so on.

Instead, he startled me by asking, "Tell me—is this the most sophisticated scheme you've ever seen?"

Not vindictively, but honestly, I replied, "No, Lawrence, it isn't."

As Fairbanks ambled out of the Aesop Audit suite, he looked more insulted than contrite.

The police and the district attorney pronounced the case a "slam dunk," and Fairbanks was sentenced to full restitution and a one-year house arrest.

In a sweet, three-bedroom home of prewar construction, Allison, Bobby, and Ruthie Fairbanks were awakened from the American Dream. Allison divorced Lawrence and moved out of state. At the conclusion of his house arrest, Fairbanks moved to the same city, to be near the kids. He now supports himself as a freelance magazine writer on the subject of arts and culture.

Lessons Learned

Our investigation provided incontrovertible proof of Aesop's monetary loss of $475,000, not to mention a detailed confession. However, we all agreed that the process would have been a lot easier had Lawrence Fairbanks set fire to his acquisitions or dumped them in the river.

The investigation in the Audit Department was within our control, but the agreement between Arnold Kruger and the campus attorney was not. We all intuited that the sale of the Fairbanks collection would not abolish the loss or, as Fairbanks optimistically asserted, net Aesop a profit. However, the university now was obliged to take custody of, and account for, all of the merchandise that awaited us in the three storage lockers.

As auditors, Frank and I knew better than to handle it ourselves. We called in experts. On a wet, dreary November morning, clad in blue jeans and old sneakers, I joined two similarly attired curators from the Aesop University art museum. Lawrence Fairbanks met us, keys in hand.

I had come to the storage facility equipped with an Excel spreadsheet that served as an inventory of all of the items from the vendors' actual invoices, including a title, physical description, and, where applicable, the artist's or gallery's serial number.

The curators brought two cameras, kid gloves, bubble wrap, and a university truck to transport the collection to a secure room that had been reserved in the Aesop administration building. The door to the secure room had been outfitted with an emergency installation of a dual-custody lock. One curator had a key; and the offset key was given to the receptionist of the area outside of the secure room. We planned it so that both "unrelated" employees had to be present in order to admit the appraisers and, eventually, the buyers.

Again, as auditors, Frank and I would not take custody of these unwanted assets. Still, we knew that we had to play a major role in protecting Aesop from being accused of breaching the attorneys' agreement—or even compromising the criminal case—if one of the purchased items had been "lost" or damaged.

Lawrence Fairbanks raised the first of the three corrugated metal doors to reveal a fully packed locker. It looked just as he described it—most of the items were still in their original cartons, unopened.

All day long, the curators methodically opened each carton and removed the pieces. We jointly identified the pieces, and as I checked off each item, both of the curators, Lawrence Fairbanks, and I each initialed the line item on the Excel spreadsheet.

The curators placed index cards bearing the inventory number that I had assigned in front of each piece, and they simultaneously photographed the items. We wanted to make certain that, if one camera failed, there would be a second photograph.

The curators then encased each item in bubble wrap, affixed a sticker bearing the same inventory number, and loaded the pieces onto a dolly. When the dolly was full, Lawrence Fairbanks would close down and lock the metal door, and he and one of us would "escort" the dolly to the truck. The driver, an experienced employee of the Aesop Museum, would carefully load the objects into the back, as Fairbanks watched.

We would not allow Fairbanks to leave our presence while either the storage lockers or the truck were unlocked. Finally, when the process was complete, everyone, including the truck driver, signed the inventory listing, which I took back to the Aesop Audit Department. I immediately faxed the listing to all who were present at the storage facility and to Arnold Kruger and the campus attorney.

For several months beyond Lawrence Fairbanks's house arrest, University Communications served its own time with some heavy-duty bookkeeping that resulted from the attorneys' agreement. It was quite a burden as the auction houses dribbled $100,000 worth of sales proceeds, in piecemeal fashion, back to Aesop.

I didn't ask what became of one of the more curious items, "squirrels under glass," after one of the curators mentioned that it is illegal to sell taxidermy specimens in this state.

The biggest lesson in all of this—and one that served us well—was that an investigator will, at some point, lose complete ownership of the case. As auditors, we were not in the position to tell the campus attorney to back off from an agreement with the subject's lawyer—one that almost created more work than the investigation itself.

However, by adopting a flexible posture and applying our expertise in the areas of record keeping, safeguarding, and accountability, we were able to exert our own special brand of control over an unexpected complication.

Recommendations to Prevent Future Occurrences

Separate Accounting Duties and Implement Secondary Purchase Approvals at All Employee Levels

Assistant Vice Chancellor Fairbanks was uniquely positioned to commit major fraud through his position of authority and trust in the Aesop Communications Department. Traditional business controls, such as separation of accounting duties and secondary approvals of purchases, were limited to subordinate staff in the past. High-level officials were practically immune to scrutiny, which enabled Fairbanks to rack up an astronomical bill in fraudulent activity. It is important to separate accounting duties and have secondary approvals of purchases, regardless of an employee's rank.

Monitor for Suspicious Activity

A member of senior finance staff—not a department-level accountant or any of the subordinate departments—should be hired as an independent monitor for the entire organization. The monitor should look for signs of trouble: repeat payments to the same vendor, payments just under the low-value threshold, vendor names and addresses that seem incongruous with the online descriptions of the expenses. The monitor should report anything that appears strange or suspicious.

Redefine Job Descriptions to Maintain Integrity

Human resource experts should review and update the accounting supervisor's written job description. The supervisor should understand that she is as responsible for the integrity of the expenses she approves as she is for the bookkeeping detail.

When the accounting supervisor in Aesop University Communications accidentally took delivery of a large package from the San Francisco–based Lincoln Galleries, she immediately recognized the address from the many invoices she had approved for Lincoln Photography. The supervisor said that she had a "funny feeling" about the package. She was not afraid of angering Lawrence Fairbanks by questioning him about the delivery. To the contrary, the supervisor was more fearful that a serious inquiry might cause unnecessary harm to her boss's reputation.

The accounting supervisor lacked the healthy perspective of an overseer. She was entirely focused on making sure that the individual "publications expenses" were charged to the correct ledger codes and that they fit safely over the bottom line. A specific job description that clearly stated her duties may have prompted the accounting supervisor to inspect the package more closely and put a stop the fraud in a timely manner.

Implement Tip Line

Finally, though not the direct result of this particular case, Aesop University implemented a 24-hour whistleblower hotline that supports anonymous complaints. Had the hotline existed during his acquisition of the Fairbanks collection, Lawrence might only have squirreled away one locker's worth of stuff.

Ellen A. Fischer, CFE, CIA, is the audit manager responsible for all investigations in a large research university. During the past 20 years, she has conducted investigations of complex and high-profile fraud cases toward their successful prosecution. Ms. Fischer enjoys writing about her cases almost as much as she does investigating them.

CHAPTER 2

The Ambitious Payroll Manager

JOHN TONSICK

When Dena Brenner entered a room, people noticed. Her bright blue eyes were framed with blonde, shoulder-length tresses. She wore stylish, expensive clothes that flattered her slender figure. Never too much makeup and just the right amount of jewelry, Dena looked much younger than the 37-year-old mother of three that she was.

Only six years earlier, after finishing her associates degree, Dena went to work in the payroll department of Sure Growth Seed Company, a family-owned business based in Ohio. Three years later, Sure Growth was acquired by a much larger establishment, International Agricultural Seed, commonly known as IAS. Dena quickly attracted the attention of the new owners and was offered a position as corporate payroll manager, requiring her to relocate to the West Coast. She worked at the company's corporate headquarters, the same building occupied by top management. It didn't take long for her to become a favorite of those in the executive suite. Thoughtful, cheery, and flirtatious, Dena was responsive to every administrative whim. The company's CEO held Dena in particularly high regard. He took an active role in protecting her interests and advancing her career. If you were to ask anyone at IAS, they would tell you with certainty that she was on her way to bigger and better things.

Dena's husband, Ron, stood in contrast to his polished and professional wife. Tall and stocky, he was a quiet, plain-spoken man. He'd spent most of his adult life working low-level jobs in the dairy industry. Married for 15 years, Ron and Dena had three beautiful daughters. As is usually the case with fraud, things aren't always what they seem. As much as Dena was loved by her superiors, she was viewed with mistrust by many of her peers and subordinates. Instead of a charming problem-solver, they saw her as arrogant, cold, and condescending. Even worse, they thought, was the way she treated her husband. Unable to find work in the family's new hometown, Ron enrolled in college and became a full-time student. When he wasn't in class, he took care of the girls. He was the family cook, chauffeur, housekeeper, and, most important, errand boy. He meekly complied with Dena's every demand.

By most accounts, Dena was a taskmaster when it came to dealing with Ron. Even the slightest transgression would send her into a withering tirade. Though kinder to her daughters, she treated them the same way as her other possessions. They were cared for, but were viewed more like accessories.

There was one more thing that bothered Dena's coworkers: her lifestyle. Sure, she made a decent salary, but no one could understand how she was able to live so extravagantly. She wore beautiful clothing and jewelry. Dena and her family lived in a spacious five-bedroom house in one of the area's nicest neighborhoods. The Brenner home was richly appointed with tasteful furnishings and artwork. Dena and Ron both drove new cars, and all three girls attended private school. Even more curious were her two horses, to which she seemed more attached than to her own daughters. When anyone dared to ask how she could afford these things, Dena responded quickly with a story of inherited wealth and wise investments.

Sure Growth Seed Company began in 1865. The American Civil War had just ended, and a reunited America was headed back to work. At that time, more than half of all the country's citizens earned their living as farmers, and the company found the perfect moment to begin selling agricultural seed. As America grew and prospered, so did the new business. Becoming an industry innovator, Sure Growth provided high-quality, high-yield seeds that were resistant to drought and pests.

At the dawn of the new millennium, the U.S. agricultural business was bigger than ever; it had also changed dramatically. Family farms played a much smaller role in an industry that was now dominated by large corporations. One was International Agricultural Seed, a global company that had grown through a series of mergers. As IAS followed its plan to become a market leader, Sure Growth was added to its list of acquisitions. With thousands of employees and facilities around the world, IAS was sophisticated. It was an environment conducive to the ambitions of Dena Brenner.

A Suspicious Transfer

Klaus Dieter had been with IAS in Europe for more than a dozen years. A handsome, blond, athletic man in his mid-30s, he acted as if he were born in the executive suite. His English was nearly perfect, with only his name and the slight hint of a German accent divulging his roots. Klaus made it a point of pride to know every aspect of IAS's business, a trait that allowed him to move up the corporate ladder quickly. To most, it was a foregone conclusion that he would head the company someday.

When Klaus arrived at headquarters, Dena had been the payroll manager for nearly three years, and the IAS executive team seemed more enamored with her than ever. By this time she had placed her mark on the department's operations. With support from the CEO and other executives, she moved payroll to the director of human resources. "That's where it belongs," she said confidently. Besides, like the CEO, the human resource director was Dena's good friend and supporter. In addition to changing the reporting relationship, she had a new payroll system installed. Using the complexities of the new system as justification, she replaced all of the department's long-term employees with her own hand-picked staff.

Just as Klaus made it a point to know every aspect of IAS's business, Dena made it a point to endear herself to every executive at the company. Klaus seemed to be the lone holdout. For reasons unknown, and in spite of Dena's best efforts, she just couldn't seem to bring him under her spell. Klaus assumed his new role as treasurer with his usual enthusiasm and love for details. It was his job to make sure that IAS had sufficient financial resources to operate the business and to continue the company's growth; that meant keeping a close eye on cash flow. In only his second month as treasurer, Klaus noted something odd in the numbers. The company payroll was processed every two weeks and, with only minor fluctuations, came in at roughly $4 million. During the last payroll cycle, the number was $4.7 million. Surprised at the large increase, Klaus phoned Dena, who was away on business in Chicago.

"What happened?" he asked.

"I'm not sure," replied Dena, "but I'll find out right away." The next day, she was back in the office and $700,000 had been wired into the company's bank account. "Problem solved," explained Dena. "Just a bank error."

With a plausible explanation and the money's quick and safe return to the company account, most of Klaus's peers would have dismissed the issue and moved on to something else. No doubt Dena's quick resolution would have earned their praise. But that wasn't Klaus's style. Besides, $700,000 was a lot of money. If it was a bank error, shouldn't someone explain how it happened? Something else was bothering Klaus. Dena was always responsive to executive requests, but her abrupt return from Chicago seemed a bit over the top, even for her. Couldn't she have just made some phone calls?

Acting on his suspicion, Klaus phoned my colleague. He explained the situation and asked if it made sense.

"Where did the money come from?" we asked.

"I don't know," replied Klaus.

"Why don't you call the bank to see if you can find out?" we suggested. Within a short time, he got an answer that infuriated him: The money had been wire transferred from Dena Brenner's personal bank account.

Memory Loss

Distressed and angry, Klaus did a little digging on his own. He learned that the $700,000 in question related to three payroll transfers. All three were made to Dena's bank account number but used the name of Yuet Chi, a former IAS employee who'd left the company more than two years ago. Klaus asked our firm to launch an investigation.

The next morning my colleague, Carrie Lane, was shown to the board room at IAS's corporate headquarters. At the center of the room was a massive black marble conference table surrounded by high-backed black leather chairs. The pale gray walls, expensive artwork, and thick gray carpeting seemed to soften the bright sunshine that was streaming through the windows. It was in stark contrast to the moods of those who would soon occupy it.

Dena Brenner walked nervously into the conference room—impeccably dressed, but distraught. She was followed by her boss, Dan Redfern, the Vice President of Human Resources. Carrie made some brief introductions and told Dena that she was trying to sort out what happened with regard to the bank error.

"I'm never doing anything again without getting someone's name in blood," said Dena. The simple bank error she described just the day before sounded a bit more complicated now. "From time to time, Amanda Salazar sends me e-mails requesting special payments for employees," Dena explained. Amanda was an HR manager who, like Dena, worked for Dan. "Since the e-mails came from Amanda, I never questioned them. I've processed lots of them over the years," she said.

"These payments are nearly a month old," replied Carrie. "How were you able to get the bank to reverse them?"

"It was just a matter of finding the right person," explained Dena. When Carrie asked her the name of her contact at the bank, Dena refused to provide it. "I don't think she was supposed to do what she did," she said. "I don't want to get her in trouble."

"Do you recognize the name Yuet Chi?" asked Carrie.

"No," replied Dena.

"These transfers are very large. Aren't they unusual?"

"Not really," Dena said unconvincingly. When shown the bank account number to which the transfers had been made, she claimed she didn't recognize it. Finally, Carrie showed Dena a fax from the bank indicating that the account belonged to Dena and her husband, Ron.

Dena's face turned ashen. After several minutes, she said, "I've returned. . . ." Then her voice trailed off.

"You've returned the money?" asked Carrie.

"No," said Dena. "I didn't take it." After a long pause she said, "I'm feeling uncomfortable. I don't know what will happen to me." Crying now, she asked, "Will I be prosecuted? I would talk if I had a guarantee of no prosecution."

Carrie could make no promises but encouraged her to start from the beginning. "Did you know Yuet Chi?" she asked.

"I just picked him," Dena said solemnly. "I don't remember why, maybe because he was terminated." The first theft had taken place a year earlier. She reactivated Chi's account in the payroll master, changed his bank account number to hers, and transferred $40,000. After the transfer, she changed the account number back to Chi's and deactivated his file. As Dena recounted her thefts, Carrie began to add up the numbers; they totaled $1.2 million.

"I still have it," Dena said softly. "I have all the money. Between my checking and savings accounts, a money market fund, and my children's bank accounts, I have all of the money. I can get it for you today."

"Did you take anything else?" asked Carrie.

"No," said Dena, "I swear on a stack of bibles." She then prepared and signed a written statement admitting to the thefts, agreeing to return the stolen money and to help the company document the transactions.

Dena was escorted to the door by security. A short time later, she returned to the office with a cashier's check payable to the company for $500,000. She agreed to meet with Carrie and me the next day at a fast food restaurant near the office. We both watched intently out the window, awaiting Dena's arrival. Right on time, a shiny new black SUV pulled into the lot. She stepped out of the car dressed in faded blue jeans and a sweat shirt. With no makeup and dark circles under her eyes, she looked as if she'd had a long night. Carrie introduced us.

"I know you've been through a lot in the last 24 hours," I said, "but I have to ask you some more questions. Did you take anything more than you've already told us about?" I asked.

"Absolutely not." she said.

"Now would be a good time to tell us," I said, "because we're going to keep looking." With a quizzical look, Dena asked, "How long do you think it's going to take?" Fighting the urge to smile, I said, "Probably a couple of weeks."

Dena and I met once more at the fast food restaurant. She assured me that I was wasting my time in looking further. She told me that all of the money had been taken in the same way: using the payroll system and the name of Yuet Chi. She told me that no one else at IAS was involved. "Even my husband didn't know until the day I was sent home," she said.

We made a copy of Dena's hard drive and began downloading electronic copies of IAS's payroll registers. Carrie and I interviewed Dena's coworkers and reviewed paper files. The interviews seemed to confirm Dena's assertion that she had worked alone. Our examination of documents did reveal a clue: Each payroll register was missing one page. We later learned that these showed the transfers to Dena's bank account. A search of Dena's hard drive revealed no hints, but we hit the jackpot with the electronic payroll registers. Sorting disbursements by bank account number, we uncovered more than a dozen new transfers to Dena's bank account using the names of three additional terminated employees, totaling $700,000. The next day Carrie and I sat in a quiet corner booth at a coffee shop. Across from us sat Dena and her husband, Ron, whom Carrie and I were meeting for the very first time.

"Dena, we found another $700,000," I said. A distressed Dena looked at me and said, "No. I didn't do it." She then dropped her head and stared silently into her lap.

"I knew you guys were gonna do this!" Ron shouted angrily. "You're going to blame her for stuff she didn't even do!"

I assured Ron that we had no reason to do that. For the next half hour, I repeated my allegations several times, but Dena continued to adamantly deny it. Except for these brief exchanges, there was silence between us. Finally, Ron couldn't stand it any more. "Did you take the money?" he asked his wife.

"Yeah, I took it." Dena said.

"Why didn't you say that half an hour ago?" he shot back angrily.

"I forgot," Dena whispered.

After years of passively doing Dena's bidding, Ron seemed empowered by the situation. "Could you excuse us for a moment?" he asked. "Of course," I said. Ron grabbed Dena by the arm and took her outside. Through the coffee shop window, Carrie and I could see the two of them engaged in a heated conversation. A few minutes later, Ron walked briskly back to the booth with his wife in tow.

"You know about the property in Michigan," he said. We had done a search for assets but had no reason to check in Michigan. "Of course we know about that," I said.

Well, we did now.

"It's worth about $400,000," Ron said. "We paid cash for it. You can have that, too."

The Law Wins

Now that the investigation was complete, IAS turned its attention to recovering its losses. Dena had already returned $1.2 million. Our discovery of the additional thefts meant that she needed to come up with another $700,000. Out of ready cash, she was no longer in the mood to cooperate. IAS filed a civil suit against her seeking recovery of the stolen funds, plus the cost of the investigation. Faced with the expense of litigation and the overwhelming evidence of her guilt, Dena settled the civil suit.

She agreed to repay her remaining debt to IAS by surrendering the property in Michigan, her home, cars, jewelry, furniture, and artwork. As she dispassionately described the assets that she would surrender, tears welled up in her eyes when she got to the horses. "Please make sure they find a good home. They're my pets," she said, sobbing. Dena showed no such emotion when offering up her children's personal belongings.

It wasn't over yet. IAS wanted more than restitution; it wanted Dena to be punished. With pressure from Klaus, the company filed criminal charges and asked me to assist. I prepared several binders of evidence gathered during the investigation and took them to Derek Thompson, head of the district attorney's White Collar Crime Unit. We spent several hours reviewing it. The binders included Dena's signed confession and a detailed description of what she had done and how she had done it. They also included original documents and computer files to support each illicit transfer to her account. "We don't usually get cases that are this well prepared," Derek said. "It could take some time, but I'm ready to get started." Paul Kole, a D.A. investigator, was assigned to work on the case.

Several months passed after our meeting. There had been no arrest and, except for a few inquiries from Paul, not much seemed to be happening. At one point, on a hot summer day with temperatures well over 100 degrees, Dena's neighbors noticed smoke coming from her chimney. Unable to imagine why anyone would light a fire on such a hot day, they summoned the fire department. They arrived to find Dena burning documents in her fireplace. After that, IAS grew increasingly concerned that Dena would escape prosecution. Those fears were soon laid to rest.

Dena and Ron were moving out of the beautiful home that was no longer theirs. Along with the house, most of their possessions had been sold, and they were returning to Ohio with the children. As they placed the last of their meager belongings in a rented trailer, Paul walked up the driveway with a warrant for Dena's arrest. "I won't put the cuffs on you in front of the children," he said, "but you'll have to come with me." Out in the street, Dena was handcuffed and placed into the back of the squad car. Leaving the children behind, Ron walked out and spoke to his wife through the open window. "I'm still going to Ohio with the kids," he said flatly. "I'm also filing for a divorce." Ron turned and walked to the driveway without looking back. Paul drove away with Dena, who was about to spend her first night in jail.

Dena was charged with multiple counts of theft, money laundering, and tax evasion. A conviction on all counts could put her in prison for decades. Derek offered her a deal. In exchange for a guilty plea, he would recommend a sentence of nine years. Dena was stunned. In nine years, her children would be grown. She never expected to see prison, much less a sentence of this length. She declined the deal and asked for a jury trial.

Derek subpoenaed Dena's bank statements and gave them to Paul, who immediately came to me. "John, I wouldn't know where to start with these things. Can you help?" I agreed. Dena had given me photocopies of some of her bank statements, but I had never seen most of them. I noticed numerous large deposits ranging from $4,000 to $50,000. I asked Paul to subpoena the supporting details from the bank. The information provided only deepened Dena's problems.

Part of her job as payroll manager was to prepare and file the company's tax returns. Over the years, she made large overpayments to various state and federal tax authorities. Once the returns were filed and paid, she applied for refunds. Those checks, made payable to IAS, came directly to Dena. She simply endorsed them "Pay to the order of Dena Brenner" and deposited them to her checking account. The misappropriated refunds totaled $350,000.

Derek added the additional thefts to Dena's previous charges, along with multiple counts of forgery and computer fraud. If convicted on all counts and given the maximum sentence for each charge, Dena could spend the rest of her life in prison.

Derek asked me to appear as a witness for the prosecution at Dena's criminal trial. By the time I testified, she had been incarcerated for nearly a year. When she entered the courtroom, I was shocked by her appearance. Dena was wearing a prison-issue navy blue jumpsuit and white tennis shoes. She was shackled at the waist and ankles, causing her to shuffle when she walked. With no makeup and long gray roots in her washed-out blond hair, there was almost no trace of the stylish young woman I first met. After hearing my testimony and reviewing the evidence gathered during our investigation, the jury found Dena guilty of all charges. She was sentenced to 15 years in state prison.

Lessons Learned

The Dena Brenner investigation was successful on many levels, but two aspects stood out. First, IAS realized immediately that it needed help. The company called an outside expert as soon as it suspected a problem and listened to our advice. Internal investigations are often undertaken by individuals who lack the necessary tools, training, and experience. Frequently they do more harm than good. Many times suspects are confronted prematurely, without adequate proof, which allows them to conceal or destroy evidence and alert co-conspirators. Critical evidence is often ignored or handled improperly, rendering it useless in a judicial setting. Because IAS called experienced investigators first, we were able to put together a clear, convincing case of what Dena did and how she did it. This was a critical factor in winning the civil action and the criminal conviction.

Second, the sequence of the investigation provided maximum benefit to the organization. By conducting a thorough inquiry, the company compiled all of the evidence and information necessary to proceed with the civil suit. This helped keep the time and expense to a minimum. Similarly, when filing criminal charges, most of the work was already done for the D.A. It wasn't necessary for the government to tie up scarce resources investigating a complex crime. This brought the case to trial more quickly. It also provided the prosecutors with a road map for presenting the criminal case in a way that easily won a conviction.

Recommendations to Prevent Future Occurrences

The circumstances that allowed Dena Brenner to commit fraud against her employer are all too common. We recommended a number of changes.

Supervisory Review

The payroll master file includes the employee's name, address, Social Security number, rate of pay, and bank account number—the kind of information that changes infrequently or not all. Dena was the only IAS employee with access to this file. She was authorized to make changes without anyone's approval. Not only could she alter data in existing records, she was also free to add or delete employee names. We advised management to review and approve all payroll master file changes. We recommended that changes be reviewed and approved by a supervisor to ensure that all changes have been properly authorized and are made correctly.

The payroll register shows the details for each disbursement to each employee. In an attempt to conceal her thefts, Dena removed the page showing her fraudulent disbursements immediately after the payroll was processed. It didn't matter much anyway, because no one at IAS ever saw it but Dena.

Post Payroll to General Ledger

Another control weakness that helped Dena conceal her fraud involved the payroll system itself, which had the capacity to post transactions to the general ledger electronically after each pay period. Dena feared that this might inadvertently disclose her theft, so she refused to let the posting occur automatically. "There's a bug in the system and I just don't trust it," she told management. Each pay period, Dena would prepare a "manual journal entry," allocating her fraudulent transfers to a huge number of expense accounts in various departments. By splitting them up and spreading them around, Dena made her transactions more difficult to spot by anyone who might be looking.

Frequent Reconciliation of Payroll Account

Before she began making fraudulent transfers, Dena tested the system to see if she would be caught. Rather than use the wire transfers, Dena authorized two fraudulent payroll checks that were never cashed. If someone noticed them, she could simply say that they were errors. But they weren't discovered because the payroll bank account hadn't been properly reconciled for more than two years. At the time Dena's fraud was uncovered, the payroll bank account had more than 500 outstanding checks totaling $700,000, including the two checks used by Dena to test the system. We recommended that the controller's office reconcile the account each month and that it be reviewed and approved by a supervisor.

Segregation of Duties IAS did not have an internal audit department. However, we recommended that someone not involved in processing payroll observe the distribution of paychecks and earnings statements. This recommendation was to help ensure that no more "Yuet Chis" would show up on the list.

Long before she began using the payroll system, Dena stole from her employer by overpaying the taxes and then applying for refunds, which she kept. This was possible because Dena prepared the returns and no one checked them for accuracy. Additionally, tax refund checks were mailed directly to her. So we recommended that payroll be reviewed, approved, and mailed by someone other than the preparer. We also suggested that refund checks be sent directly to a "lockbox" at the bank.

John Tonsick, CFE, CPA, is a forensic accountant and keynote speaker. He provides consulting services in the areas of fraud, internal controls, and expert witnessing. Mr. Tonsick is a graduate of Robert Morris University and has nearly 30 years of experience in preventing, detecting, and investigating white-collar crime.

CHAPTER 3

The Insider

CRAIG R. SINNAMON

Not long after 20-year-old Stefanne Rider was hired at Majestic Bank, she became the most popular teller in the office. Tall and slender with strawberry blond hair and hazel eyes, she had a smile that could light a small town. Stefanne was one of four children raised in blue-collar, rural Morgantown, Pennsylvania, by her mother, Cindy.

Her father, Sam, owned and operated a local furniture store—his pride and joy. When large chain stores moved into the area, his business experienced lean years, but he and Cindy always managed to make ends meet.

After Stefanne graduated from high school at age 18, she was accepted to attend Saint Joseph's University in Philadelphia. She immediately fell in love with the campus and begged her father to let her go. But how would Sam afford to send his daughter to the college of her dreams? The family qualified for some financial assistance, but not nearly enough to afford tuition, room and board, a meal plan, and books. Sam and Cindy mortgaged their modest home of 27 years, and Stefanne took out student loans to cover the remaining costs.

Stefanne reveled in college life. She studied Communications and received full honors her first two years. In September, at the start of her junior year, life was perfect. Then the unthinkable happened.

The remnants of Hurricane Ivan barreled through Morgantown and pummeled the area, dumping more than eight inches of rain in two days. A creek near Sam's store flooded. He fought tooth and nail to combat the rising water, but his efforts were futile. Within a few hours, the storm wiped out the building and all of the furniture inside. Most of all, it devastated Sam. One cost-cutting measure he had employed in order to send Stefanne to college was dropping his expensive flood insurance coverage. Now his business was destroyed, and he had to start over from scratch.

Stefanne returned home from college, placing her dreams on hold so she could contribute to the family. She took a job as a teller at Majestic Bank. The branch manager, Lena Santana, knew Stefanne well. Lena remembered giving her lollipops years ago through the drive-up window when Stefanne accompanied Sam to the bank to make the daily deposit. Stefanne already knew many of the customers in town and possessed the attributes necessary to be successful in her new position.

Majestic Bank is a large, regional bank based in Pittsburgh with approximately $110 billion in assets, over 9,500 employees, and a network of 850 community banking offices spanning from Maine to southern Virginia. It was founded over 17 years ago, starting with four branches in a small western Pennsylvania town. There exists a corporate culture of camaraderie and an entrepreneurial spirit. Employees are referred to as team members.

Majestic invests significant resources into the Loss Prevention and Security (LP&S) function. LP&S is segregated into two primary areas, Loss Prevention and Mitigation, and Fraud Investigations. Loss Prevention/Mitigation employs a large team of highly trained analysts at a central site. Their function is to maintain and review various software applications designed to detect and reduce losses associated with fraud. The Fraud Investigations team consists of a smaller group of professionals, each strategically located throughout the bank's footprint. Many are retired law enforcement detectives. Others, like me, are career bankers. I joined the team after two years in retail banking and seven years as a corporate auditor.

What Did You Do with My Money?

Carolyn Sasser, a career banker and a member of my team, was one of a couple of investigators responsible for investigating all forms of bank fraud cases originating in the greater Philadelphia area. She was in the process of reviewing what appeared to be a routine counterfeit check case on a humid summer afternoon in her tiny office in Rosemont, Pennsylvania. The victim in this case was a customer named Thomas White. He opened an account more than 10 years ago. Thomas, a retired World War II Air Force pilot, stopped by the local Majestic branch in the Chestnut Hill section of Philadelphia to withdraw $100 cash before going to the grocery store. Soon after handing his withdrawal slip to the teller, he was stunned to learn his account was overdrawn.

"How could that be?" he asked. "Didn't my Social Security deposit post to my account last Friday?"

"Yes," the teller replied politely. "But you also wrote three checks to your account last night," she continued.

"That's impossible! I need to speak to Gina immediately," he demanded.

Gina Stevens, the branch manager, had opened his account at the Chestnut Hill branch. She and Mr. White got along famously. But now he was fuming. "What is going on with this bank?" he asked Gina curtly before she could even say hello.

Gina listened intently to Mr. White's problem. To her, it sounded like a case of counterfeit checks. "We will take care of you, Mr. White," she reassured him. Gina completed the necessary paperwork and opened a new account for him. Majestic reimbursed Mr. White in full but he terminated his relationship with the bank a few days later, sighting concerns over security.

Carolyn reviewed the checks contained in his file. The check stock used by the counterfeiters really resonated with Carolyn. "Didn't I recently work on a case with similar-looking fakes?" she asked herself aloud. She then looked at the back of the check and observed a stamp from Kingdom Bank based in New Jersey. "Kingdom Bank?" she wondered. "I've been speaking with their Security Department a lot lately."

After a few minutes of reviewing Mr. White's file, Carolyn realized that this was no ordinary counterfeit check situation. Luckily, she was fanatical about organizing her files. She quickly was able to pull a few cases, and compared them to Mr. White's. All of them were relatively small (under $4,500 loss), so Carolyn had placed them on the back burner while she tended to larger issues. Each victim customer noticed the activity soon after it began. She found three other counterfeit cases with similar attributes—individual checks less than $1,500, same check stock, similar handwriting, all negotiated through Kingdom Bank in New Jersey. Carolyn called Tim Carter, the security officer at Kingdom. "Not only were all of them deposited at our bank," he informed Carolyn, "but they all went through the same ATM machine at one of our branches in Trenton! All four of our customers immediately withdrew all of the money from their accounts using the same ATM."

It was obvious that these seemingly small cases were associated with the same check fraud ring. Carolyn knew that LP&S likely had more problems. She immediately called Mary McFadden, another Majestic Bank fraud investigator in Freehold, New Jersey, to see if she had any similar issues.

Mary took copious notes as Carolyn provided details of her cases.

"Wait a second," Mary said, "What was that last account number?"

It was Mr. White's. "Carolyn," she continued, "that is a passbook savings account. I just received a small counterfeit check case involving checks that posted to a statement savings account. How is it possible that checks can post to *savings* accounts?" she asked. Mary pulled the case file.

"You know what? My victim customer's name is James White. Let me look at the back of the checks . . . yep, Kingdom Bank. You know what else, Carolyn?" Mary continued. "All the victim customers' names are common: Tom White, James White, Mark Williams, Tom Jones, Michael Smith. This doesn't appear to be a dumpster-diving operation. These victims were targeted systematically."

Carolyn agreed, "You're right. I smell an internal fraud. Let's get Kathy and Craig on the line."

Following the Footprints

I had just returned to my office after lunch and was sifting through the mountain of paperwork on my desk when the phone rang. It was my manager, Kathy Backman, the corporate internal fraud manager at Majestic Bank. She manages a team of five analysts and three investigators trained to proactively identify and investigate various types of internal fraud, such as branch cash embezzlements, payroll fraud, and general ledger frauds. I am one of the three internal investigators reporting to Kathy.

"Craig, I need you right away," she said, on a mission.

"What's up?" I asked.

"I'll explain when you get here," she replied.

I scurried to Kathy's office, four doors down from mine. "What's going on?"

"Carolyn and Mary are on the phone with me now," she said. The women explained to me the circumstances that preceded their call.

"Well, it appears a bank employee has compromised your victims' accounts," I stated.

"Craig, research the 'Footprint Report' to determine if the same employee queried the victims' accounts before the counterfeit checks were negotiated," Kathy instructed.

The "Footprint Report" was created by Majestic's IT Department at Kathy's behest a couple of years ago after she suspected an insider was stealing customer account information. She could not prove her theory due to the bank's inability to monitor employee inquiry activity. The "Footprint Report" captures all customer profile/account queries performed by staff directly on the bank's mainframe system. A team member must use his or her unique user ID and password to directly access it. If someone queries a customer profile/account directly on the mainframe system, the "Footprint Report" will capture the activity and the associated user ID.

I reviewed the bank statements associated with the five customer accounts and started my research with two of them that contained minimal account activity. "It should be easy to isolate a common user ID with these two accounts. The customer's infrequent activity should result in fewer account queries," I concluded. I first searched "Footprint Report" for victim Tom White's account. Mr. White's deposit activity consisted only of a monthly direct deposit of his Social Security. He writes some checks to pay his monthly bills and only on occasion withdraws cash over the counter at his local branch. I noticed the first counterfeit check posted to his account on July 9, so I started with a date range search beginning June 1 to July 8. There were a couple of inquiries performed by team members. I cataloged the user IDs and query dates/times on a spreadsheet. I searched the "Footprint Report" for the next victim customer, Mark Williams, and cataloged the queries as I did with Mr. White account. "Bingo!" I said. "We have a hit!" I noticed that the same user ID performed queries on the accounts owned by White and Williams less than two weeks before the counterfeit checks posted.

I searched the system for the owner of this user ID. It was Stefanne Rider at the Morgantown branch. Why would a teller in rural Pennsylvania want details for a customer residing an hour and a half away in Philadelphia? I then reviewed Mr. White's account and noticed that Stefanne asked for his name and account number on June 30 at 12:05 p.m. on the mainframe system. I further observed that Stefanne queried Mr. White's profile and account number on the mainframe system at this time, and also several other rather common names within just a few minutes, some only seconds apart. She appeared to be haphazardly searching for customers.

In no time I was able to trace the three remaining profiles to Stefanne's user ID. Counterfeit checks began to post to each account within two weeks of her inquiries. Coincidentally, all five victims resided and performed their banking in the greater Philadelphia area or New Jersey, hours away from Stefanne's Morgantown branch. It was obvious that she was the point of compromise. I phoned Kathy right away. "I think we have our suspect," I said. We discovered that Stefanne was on vacation visiting family in Ohio for the remainder of the week and was scheduled to return the following Monday.

"Great," said Kathy, "This gives us the opportunity to investigate further and determine the scope of this case. There are probably more victims out there. We can interview Stefanne the day she returns from vacation and maintain the element of surprise so she doesn't have the opportunity to concoct a story behind her activity. However, let's disable her system access immediately, just in case. Solicit the help of the analysts to conduct comprehensive research. We need to identify as many actual and potential victims as soon as possible, so you'll need their help. Report your findings to me by the end of the week," she stated.

"So much for catching up on my paperwork," I said aloud as I journeyed to my office to set up a conference call with the analysts.

Kathy's team and I worked long hours to link Stefanne's inquiries to customer accounts victimized by counterfeit check activity. By the end of the week, we linked her to 18 victims of counterfeit check activity, with total bank losses exceeding $54,000. The fraud had begun only a couple of months before. Victims spanned from Maine to Virginia, and all had common names. Every counterfeit was negotiated at Kingdom Bank and clearly originated from the same check stock. Each one contained very similar handwriting. It was also evident that the "ring" had an insider working at Kingdom, as the identities of many confirmed Majestic victims were used to open accounts at Kingdom. Finally, we knew that many more of our customers had been compromised by Stefanne, as she performed inquiries on countless others. The analysts closely monitored these accounts while regional management and Kathy painstakingly devised the appropriate action plan, including contacting the customers, freezing their accounts, and offering free identity theft protection.

During the investigation, we determined that Stefanne maintained an employee checking account at Majestic. I reviewed her account and identified several nonpayroll cash deposits in amounts ranging from $400 to $1,000. She had deposited over $10,000 just over the past few months. I explained our findings to Kathy, who then reported the results to regional management. Next, we contacted Lena, Stefanne's manager, but did not disclose the nature of our investigation. We needed to obtain some background information prior to the interview. Lena advised us of the unfortunate circumstances that recently befell Stefanne and her family, insisting that she was a top performer, loved by her team and the Morgantown customers.

"If she did anything wrong, I'm sure she'll have a legitimate explanation," Lena insisted. "She's a sweet girl and I would stake my reputation on her."

"What makes you think she did anything wrong?" Kathy asked.

"Well, any time loss prevention calls, it usually means someone is in trouble," Lena replied.

"That's not true," Kathy said. "We simply think Stefanne may have some information to help us with a current investigation. Please ask her to report to the Administration Building first thing Monday morning to meet with Craig."

It was 9:30 a.m. and the start of what would be a productive work week. A trembling Stefanne Rider arrived at our office. When I went to introduce myself, I was startled to see that an older gentleman who identified himself as Sam Rider, her father, accompanied her. He wanted to participate in the interview with his daughter. I told him that the meeting pertained to a private bank matter, and I could not allow him to be present. Sam was clearly agitated, but he acquiesced and waited in the lobby.

As we entered our conference room, I introduced Stefanne to Tracy Blattner, an employee relations representative from Majestic, and directed her to a chair in the middle of the room. The table was previously moved to the side so there would be no obstruction between us. Tracy sat in a chair several feet behind to witness the interview. Stefanne remained visibly nervous, clutching her purse in her lap with her arms crossed, head down, and eyes tentatively peeking at me from under her strawberry blond bangs. She rocked slightly back and forth in her chair as I began asking her some basic background questions about her education, job responsibilities, and family life in an effort to develop a rapport with her. As I learned more about Stefanne, I began to sense the anxiety building in her. She appeared sheepish and spoke almost with a whisper.

Before I was able to begin asking Stefanne questions pertaining to the case, she began to sob. I placed my memo pad to the side, pulled my chair closer to her, and asked, "Is there something you want to talk about? You seem to have the weight of the world on your shoulders, and I'd like to help you in any way I can."

"I don't think there is anything you can do to help me," she responded, tears streaming down her face.

Running on Empty

It took the better part of an hour to settle Stefanne down so that she could speak to me coherently. She eventually confessed to selling customer identities and account numbers to a ring operating out of Philadelphia.

Stefanne had met a young man named Buck while employed as a barmaid at a pub near campus. A regular patron, he had befriended her not long after she began working there. Buck was brash and flirtatious with slicked-back dark hair and a rail-thin build. Although nobody actually knew how he made a living, he appeared to have a lot of money. He drove brand-new import cars, dressed to the nines, and tipped better than any other patron. One night he approached Stefanne after hearing from the bar owner that she was leaving school to tend to a family crisis. He also had learned she accepted a job with Majestic Bank as a full-time teller.

He approached Stefanne. "I'm sorry to hear about your family situation. It sounds pretty bad. I hear you took a job at a bank, huh?" Buck asked.

"I need to help pay the family bills, my own credit card bills, and put food on the table—at least until things get better. I'm devastated that I have to leave school, but I have no choice," Stefanne said.

Buck then made his pitch. "Listen, I think I can help your family and get you back to school in no time, but you need to do something for me," he said. "You take that job with the bank, and I'll give you $200 for every customer account you give me, along with each of their Social Security numbers, addresses, birth dates, phone numbers—any information you can access."

"But isn't that against the law? What in the world are you going to do with it?" she asked.

Buck explained that his friends needed the information to make and cash counterfeit checks, and customer identities to open bank accounts and establish credit lines.

"I don't know," Stefanne said.

Buck interrupted, "You want to help your family, right? You want to return to school, right? If you turn me down, you'll probably never come back to college. Anyway, nobody gets hurt in the end. The bank has millions of dollars and will reimburse the customers."

"But what if we get caught?" Stefanne asked.

"I'll tell you what," Buck said. "After your shift I'll take you to my friend's house and show you how it works. Deal?" he asked persuasively. Stefanne reluctantly agreed.

Her shift ended at 2:30 a.m., and she met Buck outside of her dorm. He drove her to an old, rundown row home somewhere in North Philadelphia. Buck navigated through a complex network of small side streets and dark alleys so Stefanne would not be able to determine the exact location of the property. They entered from behind the row home and proceeded down a dark stairway to the basement. There, they met a man who called himself "Taz." Taz was an older, heavyset African American man who wore a prosthetic leg.

"This is the girl who is going to join our team," Buck said, as he rushed to the basement. Frightened, Stefanne stood at the base of the stairway. Taz grinned and motioned her into the basement. As she made her way toward the men, Stefanne's eyes were drawn to what appeared to be a modern studio equipped with laptop computers, digital cameras, stacks of blank checks and credit cards, and laminating equipment. "This is where it all happens," Taz explained proudly.

The men explained that the information she agreed to provide would be used to create counterfeit checks and fake IDs. Taz provided the fakes to a group of "runners" who would open bank accounts and negotiate the counterfeit checks.

"We'll also tell the runners to apply for loans using the identities you give us," Taz continued. He had a partner who recruited homeless people. "They'll do anything to make a few bucks," he explained. "Stefanne, we'll make more money than you can imagine," Taz promised. "And your job is the easy part. It's the runners who risk getting caught."

It didn't take them long to convince Stefanne to agree to the scheme. She would have done almost anything just to get out of that row house!

Buck returned Stefanne to her dormitory. "I'll call you on your cell in a few weeks and let you know how we're going to do this," he told her.

Two months later, Stefanne was already a favorite teller at the Morgantown branch. One day during her lunch break, her cell phone rang. It was Buck.

"I got $600 and need some customers, Stefanne," he said without even introducing himself. She knew exactly what he meant. "Meet me at Burger King after the bank closes tomorrow and don't target customers that go to your branch. That would be too obvious."

Stefanne returned to her station and quickly decided it would be easiest to query common names on the bank's mainframe system.

Ultimately, Stefanne confessed to stealing the identities of over 55 Majestic depositors. She explained that she would meet Buck once per week and exchange customer screen prints for cash.

"I still can't believe I did this," she whispered to herself as she completed a written statement.

"Did you tell your dad?" I asked.

"I told him this morning after I was asked to come here," she responded. "I wouldn't have involved my dad if Buck didn't call me on my way here. He made it clear that I was not to cooperate with you. I immediately called my dad and told him everything. That's why he came with me this morning. He had no idea what I was doing. He just thought I was making extra commissions by cross-selling bank products. He pleaded with me to cooperate with you. I wasn't sure I would until you started asking me questions."

When the interview was complete and her written statement was secured, Tracy informed Stefanne that her employment with Majestic Bank was terminated. After handing me the keys to her teller cash drawer, I escorted an emotionally drained young woman from the conference room. I watched her approach her father and collapse into his arms.

Stefanne later offered a treasure trove of information to law enforcement. The intelligence she provided resulted in the arrest of several criminals and the breakup of an organized crime ring operating out of Philadelphia. She avoided jail time by cooperating with the prosecution of these criminals, but received five years probation and was ordered to pay $66,000 of restitution to Majestic Bank.

The promising future of this once-exuberant, intelligent young woman changed forever the day she decided to enter into the criminal underground world of identity theft and check fraud—a fact she will be reminded of each and every time she completes a job application.

Lessons Learned

I learned a great deal as a result of this and other identity theft cases involving Majestic Bank customers.

Information Security—Restrict and Monitor

In today's environment, it is critical for every organization to develop and implement enterprise-wide countermeasures to external and insider attacks against their information technology environment. Majestic Bank recognized the risks associated with insider attacks and the need to restrict employee access to sensitive information to only those who require it to perform their job. One countermeasure currently under management consideration is biometric technology. Rather than requiring a customer to provide an easily counterfeited driver's license and secondary form of identification, a customer can authenticate his or her identity with a mere scan of a fingertip.

It is no less critical for organizations to monitor employee access to sensitive company data. For example, Majestic Bank's "Footprint Report" was a relatively new tool that enabled us to identify the single point of compromise. Although it was instrumental in identifying the suspect after the fraud was well under way, we have further enhanced the surveillance of employee system activity. As such, Majestic Bank implemented new business intelligence software to proactively monitor employee access to sensitive company data by capturing anomalous teller inquiry activity, such as:

- Inquiries to the bank's teller processing system with no corresponding customer transactions
- Inquiries on customers residing outside of the teller's predetermined geographic region
- An unusually high volume of inquiries in comparison to historical volumes associated with a given teller
- An unusually high volume of inquiries performed by a teller on a predetermined list of common names, such as "Smith," "Jones," and so on

Employee Assistance Programs

Majestic Bank partners with an organization that offers a wide variety of programs designed to support Majestic team members with just about any life issue, such as financial crises, child care issues, and elder care. Lena Santana failed to recognize the extent of Stefanne's dire situation and direct her to the employee assistance program (EAP). Perhaps Stefanne could have received the help she needed before resorting to nefarious activity.

Customer Retention—Identity Theft Assistance Unit

LP&S and Retail Management had difficulty coordinating proper notification to the identity theft victims. The bank did not have standardized procedures, which created an atmosphere of confusion with respect to roles and responsibilities and did not allow the bank to adequately leverage its resources to respond to customer needs in a timely, organized fashion. LP&S quickly recognized the need to provide victims a single point of contact to facilitate customer retention. As such, LP&S established an Identity Theft Assistance Unit consisting of five highly trained team members charged with the responsibility to respond to the needs of identity theft victims.

LP&S Case Management

Carolyn and Mary utilized years of investigative experience and open dialogue to link multiple fraudulent events (i.e., counterfeit checks) to a single point of compromise. The importance of open communication and dialogue within an organization cannot be overstated. Oftentimes, entities unknowingly maintain a "silo" approach in their day-to-day operations. Majestic Bank's LP&S Department now nurtures a culture of open, honest dialogue among its team members.

Tip Line

Although Stefanne pilfered customer identities stealthily, many insiders fail to exercise such discretion. Majestic Bank provides all team members with an anonymous internal hotline to report unusual or suspicious activity to LP&S. However, only one LP&S team member is currently assigned the responsibility to man the hotline between 8 a.m. and 5 p.m. Because callers often are forced to leave information on a recorded message, many fail to provide sufficient, actionable information. Messages are also sometimes inaudible due to a poor phone line connection. LP&S recommended management consider outsourcing this function to a company that can deliver live, 24/7 coverage by personnel trained to extract detailed information from each caller, while ensuring 100% confidentiality.

Recommendations to Prevent Future Occurrences

Information Security

All companies, including financial institutions, should make it a priority to understand the current threats to their IT infrastructure and consider leveraging technology to defend against attacks from external and internal sources.

Background Checks

Organizations should utilize a comprehensive applicant screening process inclusive of criminal background and credit checks, especially for those positions requiring extensive cash handling and access to sensitive company information, such as customer profiles.

Zero Tolerance Policy

Executive management at Majestic Bank has taken a stance against fraud committed by its team members. They maintain a "Code of Conduct and Ethics" that must be signed by every newly hired team member. In addition, all team members must review the code during each annual performance review and sign a document acknowledging it, which states in plain language the fiduciary duty of everyone to refrain from transactions or behavior that seems even slightly impropriate and report suspected fraud to appropriate personnel. The code also specifically addresses the bank's position regarding fraud, namely "zero tolerance and prosecution of the offenders." This document can serve as a deterrent and sets the appropriate tone from the top.

Customer Education

Majestic Bank uses every communication avenue at its disposal to educate customers on how to protect themselves from identity theft. The bank's Web site contains a prominently displayed section dedicated to these issues. Each branch displays signage warning customers of the threats associated with identity theft. Brochures are also on display in branches and are periodically enclosed with customer statement mailings to educate people about the risks. The call center often plays an audio message alerting customers waiting on hold to the danger and warning signs of identity theft.

The bank advertises and offers a software product that is linked to the three major credit bureaus. This provides customers with instant access to their credit files, automatically monitors changes or inquiries to credit files, and alerts customers to any unauthorized accounts opened in their name.

Employee Training

Financial institutions should conduct ongoing employee training about identity theft. At a minimum, they should develop written policies and procedures governing disclosure of customer information, and use them as a basis to train employees. Employees should be trained to recognize fraudulent attempts to obtain customer information and execute the necessary prevention techniques to protect customer information from internal and external threats, such as shredding documents containing sensitive company or customer information, avoiding unauthorized access to computers, and limiting the amount of information provided over certain communication channels like e-mail and telephone. Majestic Bank's LP&S and Legal departments provide on-site and web-based employee training covering these and many other issues associated with the security of customer information and related privacy regulations.

Craig Sinnamon, CFE, is a regional fraud investigations manager with a large financial institution. He is a graduate of Beaver College (now known as Arcadia University) and has 11 years of auditing and fraud investigations experience in the financial services industry.

CHAPTER 4

Aloha, Hawaii!

DOMINIC A. D'ORAZIO

Marin Jensen seemed to have it all. A self-proclaimed family man, he married a lovely gal named Julia and had two young children. His wife stayed home to manage the active lives of their kids, while Marin appeared to be a model employee at the American Logistics Agency. From the exterior, their lives were picture perfect.

The Jensens' home was nestled away on a quiet tree-lined cul-de-sac in one of the Northeast's more affluent communities. The two-story colonial sits on two acres of beautifully landscaped property that was purchased by the Jensens for almost $400,000. The dead-end street was ideal for the kids, since it does not have a heavy flow of traffic. A state park is located near the neighborhood, which is used for various athletic competitions and has an adjoining farm that resembles what daily lives were like before the advent of the industrial age. Because of the proximity to the state park, one can bike around the neighborhood in the late afternoon and spot deer meandering through the residents' yards.

At first glance, one might surmise that the area consists of the type of folks who spend a great portion of their professional lives climbing the corporate ladder. Indeed, this is not the type of neighborhood one would associate with a middle-management government worker. Of course, it is no crime for a middle-management employee to live in such a neighborhood. Certainly there are other ways to accumulate the type of wealth one would need to afford the property, but if the lifestyle one is living cannot be explained by the income one is earning, questions arise.

Marin's home, though modest compared to some of the more elegant houses that dot this high-income town, contained features common among families who prefer to have amenities close to them. For example, the backyard contained a playground area and an in-ground swimming pool, surrounded by flowers and bushes. These quiet and serene conditions could persuade one to meditate. Like many of their neighbors, the Jensens employed landscapers who mow and edge the lawn, trim the bushes, and maintain the yard.

Marin took pride in coaching his children's sports teams and running the usual family taxi service, transporting his kids to their respective sports and extracurricular activities. While most of today's families own minivans, the Jensens had the original family conveyance: a station wagon.

After working for American Logistics for several years, Marin rose to the position of senior logistics management specialist. He was considered likable, and several program directors wanted to use his services. During one particular year, he split his work time between his main office and two other customers. When a third customer inquired about his services, Marin's supervisor stated he had already used up his available work time for the year. The prospective third customer suggested that if Marin would agree to work for him, he would be willing to pay for the overtime. Marin agreed to put in the time, over and above his normal workweek. Once his work for the third customer was finished, Marin began to struggle financially. He had become accustomed to the extra cash. With his real estate taxes climbing, he had to come up with another way to supplement his salary.

The American Logistics Agency is a part of the federal government, located in the northeast region of the United States. As an integrated entity, it develops, fields, and sustains base command and control, intelligence, surveillance, and reconnaissance systems. American Logistics deals with research and development, management, and distribution of equipment to support soldiers who are fighting overseas. The company employs about 10,000 people worldwide and is also supported by thousands of contractors.

Although American Logistics is located on a site with other federal government entities that covers over 1,000 acres of prime real estate, it is self-sustained, complete with its own fire and police departments, post office, supermarket, gas station, church, child care center, liquor store, thrift shop, credit union, and motor pool. It also contains a range of outdoor amenities: three swimming pools, a physical fitness center, tennis courts, softball fields, a bowling center, a golf course, an athletic complex, and a picnic area.

As typical of any federal government entity, and in addition to its list of researchers, procurement officials, and logistics specialists, American Logistics also employs lawyers, internal auditors, and criminal investigators, along with a resource management office and a personnel office that ensures the agency is properly financed and staffed.

American Logistics is one of the state's largest employers and produces $3.4 billion for the state's economy.

The Copycat

As supervisor to Marin, Arthur Kiley never had any complaints. But one Monday, that changed. After Marin made photocopies of his new travel order, he mistakenly left the document in the machine. Mr. Kiley was the first to notice, and when he looked at the travel order, he observed that the signature block had been cut out of a previously signed order and taped to the new one.

"Marin, may I ask what you're doing with this signature taped to your travel order?" asked Mr. Kiley.

Marin replied that he was simply trying to make the signatures darker because when he faxed them to the ticketing office, the color was muted.

Later that day, Mr. Kiley approached Marin again to inquire about the taped travel order. Still, Marin assured him that he was "just making sure the signature was dark enough to be legible for the ticketing office." Mr. Kiley pressed on, threatening him with an audit of his past reimbursements of travel claims if he didn't come clean.

At the end of the day, Marin had not 'fessed up to any wrongdoing, so Mr. Kiley decided to do a little detective work. It didn't take long for evidence to surface. When he looked inside Marin's trashcan, he found a travel order with the signature cut out of it, copies of pay stubs, and copies of other travel orders where the initial "J" was handwritten by Marin. The "J" pertained to the first name of Mr. Kiley's boss, Mr. James Heyward, who was the authorizing official for Marin's travel orders and subsequent travel voucher claims.

Mr. Kiley contacted Samuel Mezzacante at American Logistics' legal office for guidance. Upon being informed of the possible fraud, Mr. Mezzacante first contacted the criminal investigators. Next, he called my department, the internal review evaluators, and set up a meeting to examine the evidence. Mr. Mezzacante requested our services to review Marin's travel vouchers and to determine how many vouchers were fraudulently filed.

In the meantime, Mr. Kiley had obtained several of Marin's settlement vouchers and tried to compare the dates of supposed travel to what Marin was actually doing on those dates. The settlement vouchers were subsequently turned over to us in the Internal Review Evaluator Department.

We notified the Defense Finance and Accounting Service and requested copies of all vouchers that were paid to Marin. It took several weeks to receive all of the copies. We had asked for vouchers going back five years, which meant the Finance Service had to research within their archives to find them, make copies of the documents, and mail them to us.

The next step was to contact the Bank of Commons, the contractor that managed the Government Travel Card program. All government travelers are required to use the Government Travel Card for all official travel-related expenses such as hotels, car rentals, limousines, airlines, or trains.

Since I had three staff members working on this review, I decided to divide the scope of the project into three timeframes. Each member worked on a one-and-a-half-year timeframe.

Have Committed Fraud, Will Travel

While reviewing Marin's travel vouchers and receipts, we noticed that on trips down to Springfield, Virginia, he stayed at a hotel chain that was not familiar to us. We searched the Internet to find the phone number of the hotel's corporate office. When we contacted them, they confirmed that the hotel was located in four cities in Virginia—but none in Springfield.

In an attempt to give Marin the benefit of the doubt, we contacted Joseph Somers, an evaluator from our corporate office in Virginia, and asked him to go to Springfield to the address listed on the hotel receipt and verify whether any hotel existed at that location. Perhaps Marin had accidentally listed the wrong hotel name. When Joseph tried to go to the address, he could not find it. None of the locals were aware of a hotel with a similar address either. The hotel simply did not exist.

The next day, Joseph called our office and reported his findings. Afterward, we drafted a letter and sent it certified mail to see if there was any chance that Joseph was mistaken. The letter was returned a few weeks later, stamped NSA—No Such Address. Our fears began to take shape. This scheme would require us to research the records and "leave no stone unturned," as our director, Martin Dais, instructed us. In other words, Mr. Dais told us to check every receipt and contact every vendor and to ask for legitimate receipts from the companies involved. We were also to ask the vendors if Marin had stayed in their establishments or used their car rental services as he claimed on his travel vouchers.

On some claims, Marin would use his Government Travel Card to charge for car rentals with one company, while his travel vouchers would show that he used a different one: Alamo Rent-A-Car. In all of those cases, Marin's claim for River Run Rent-A-Car was higher than his actual charge on his Government Travel Card. Also, when we looked at the River Run receipts that were attached to his vouchers, we noticed that the receipts were always in the same position on the letter-size paper, which indicated that Marin had a template in his computer's hard drive and was printing out his receipts as he needed them for "proof" of his various trips. We contacted the corporate headquarters for River Run and asked if Marin had used the agency to rent cars for his business trips. The River Run official told us that Marin was not showing up in their database as ever having rented a car. The official also faxed us an example of a valid receipt. When we compared that receipt to the ones that Marin had printed, we realized that the only difference was a five-digit code that appeared at the bottom of the valid receipt. This code identified either the person handling the transaction or a specific River Run agency office.

When we compared Marin's travel claims to his Government Travel Card charges, we noticed that he had used his Government Travel Card to charge train tickets at the station nearest to the airport. However, on Marin's travel vouchers, he would claim that he took a limousine from his residence to the airport and back. The cost was always under \$75, which would have required him to submit a receipt to our finance office. So an \$11 charge (cost of train ticket) became a claim for \$74 (cost of limousine), a net profit of \$63 for each direction for each trip that Marin claimed.

Another travel voucher showed that he had gone to a location in northeast Pennsylvania. However, his Government Travel Card transactions showed that he was gambling in an Atlantic City, casino located in southeastern New Jersey. We thought it unlikely that Marin was capable of being in two places at the same time.

As we scrutinized the travel vouchers, we realized that each year Marin's claims would grow to a larger amount. Also, when we conducted a review of Government Travel Card transactions, Marin's name came up because he was using the Government Travel Card in restaurants close to his residence. These types of transactions are classified as a misuse of the Travel Card since there was no official purpose for him to eat at the local restaurants. At the end of that particular review, the names of the misusers were turned over to their respective directors who coordinated discipline with the personnel office. When Marin was notified that he was found to have misused the Travel Card, he probably thought he got away with submitting all of the fraudulent vouchers. After receiving administrative disciplinary action, he began upping the ante by claiming parking costs of $18 per night at the hotel that did not exist in Springfield, Virginia.

We noticed a pattern developing while reviewing the travel vouchers. Marin would always leave a few days before his scheduled date of departure or would always stay a few days after his travel had ended. After piecing his travel vouchers together, we noticed that over a three-month stretch, Marin was basically on the road 100 percent of his time. For example, his travel vouchers showed him leaving on a Monday and returning on a Thursday. Then he would leave the next day (Friday) and return Tuesday. Again, he would leave the next day (Wednesday) and return Monday, and so on. I joked to my staff that he might as well not even unpack. Obviously, we questioned whether he was actually on travel status the whole time.

Another claim showed that Marin had traveled to Virginia for a meeting. We contacted the host for that meeting and were told that Marin had called ahead to say that his car broke down. The host had cancelled the meeting and scheduled it for another day. While Marin did not stay in Virginia for his entire travel time, the documentation on his voucher claimed that he stayed there for three days.

In one part of the review, we noticed Marin had scheduled a trip in February—just a few months back. He made reservations through the government ticketing office for a plane ticket that took him to Savannah, Georgia. On the day that he departed for Savannah, he went to the Delta Airlines counter and charged a round-trip flight to Savannah through his Government Travel Card. Then he went to the Continental Airlines counter and had the counter person exchange his government-issued round-trip ticket to Savannah for a one-way personal ticket returning from Los Angeles. A few weeks after returning from Savannah, he called Continental and had the company exchange the one-way trip from Los Angeles to a round-trip ticket to Hawaii for July 15. Since that date had not yet come, we knew that Marin was planning a vacation. We had to work fast.

Permanent Vacation

During the course of our investigation, Marin had his security clearance taken away from him, which meant that he could not work on any classified or secret work. In essence, he was relegated to administrative duties that were very minor and that did not require any type of security clearance. Soon after, Marin's computer was taken way from him so that the forensic investigators could retrieve all of his electronic mail, along with any files he may have stored in his hard drive.

Having no security clearance or a computer to do even minor tasks, Marin wrote an e-mail during the week of April 11 to Mr. Kiley, claiming that since he no longer had a way to complete his work, he felt that there was nothing to do but resign from American Logistics. His last day was April 15. We had to get all of our paperwork to the prosecuting attorney before Marin could go to Hawaii.

While checking his computer files, the forensic investigator retrieved electronic files for his fabricated hotel claims and for his car rental claims, which is what the internal evaluators had suspected all along. In addition to the files, there was e-mail correspondence between Marin and his wife, who asked him point blank when the next travel check was coming in. They needed the proceeds to pay for the current month's mortgage. The Jensens were desperate to make this scheme work.

In the early stages of our investigation and while working with the criminal investigators, Agent Stone Huntington and Agent Thomas Harter, we learned that the office of the U.S. Attorney only took cases that exceeded a certain dollar amount. Once we calculated that the scheme exceeded $100,000, Agents Huntington and Harter brought it to the attention of the U.S. Attorney's Office. After showing Giovanni Falcone, the Assistant U.S. Attorney, what we had pieced together, he had us go back to all of the voucher claims and reconstruct them to allow for valid claims to which Marin may have been entitled. It was this reconstruction that forced us to compare the travel voucher claims against his Government Travel Card charges. Unfortunately for Marin, he didn't realize that he was leaving a trail whenever he used his Government Travel Card.

Falcone told the investigation team that he needed the field work done at least 30 days before July 15 so that he could have the warrant signed and issued to Marin before he left for Hawaii.

Agents Huntington and Harter, along with a couple of local police officers, went to Marin's house around 5:00 p.m. on July 14 with a warrant for his arrest. As he was handcuffed and led out of his house, his wife came running down the stairs to ask "Marin, what about our trip to Hawaii?"

Huntington and Harter advised Marin of his Miranda rights. The two agents drove him to the county jail where he would spend the night. Along the way, the two agents asked Marin why he carried out this scheme to defraud the federal government. He replied that he worked harder than most people in the federal government but was not justly compensated for his work.

The next day Huntington and Harter escorted Marin to the federal courthouse at the state capital. At Marin's arraignment before the federal judge, his attorney asked if Marin could go to Hawaii with his family since they were scheduled to depart that day. But the judge confined Marin to the state of his residence. Meanwhile, his wife took the children and spent a week in Hawaii without him.

Marin was charged with one count of wire fraud covering over 150 fraudulent vouchers and totaling over $150,000. He was found guilty and was ordered to pay $151,460 to the federal government for fabricating expense vouchers. He was also sentenced to 20 months in federal prison and ordered to serve three years of supervised release upon the completion of the prison term. According to the transcript filed in the federal court, Marin took the money over a five-year period to pay off mounting credit card debt.

Lessons Learned

After talking to various parties who were involved in ensuring that Marin traveled and performed his duties in conjunction with his travel orders, no one could unequivocally state that he or she knew exactly whether Marin had properly performed his duties. He fell through the cracks. He had everyone fooled. If he worked for Mr. Kiley, he would tell customers A and B that he was working for his immediate supervisor. Other times he would tell Mr. Kiley that he was working for customer A or B, regardless of where he was. Mr. Kiley had no control of Mr. Jensen, nor did he corroborate with customer A or B to attest that Mr. Jensen was indeed traveling for them. It was sheer luck that Mr. Kiley found the taped travel order in the copier—and sheer stupidity for Marin.

Although many "red flags" appeared during the perpetuation of this fraudulent scheme, nobody investigated them. For example, when the travel account for one customer had totally been expended, the budget analyst did not ask why all of the funds were spent. Individuals who are responsible to review and authorize the travel claims need to ensure that they review them for accuracy and legitimacy.

Recommendations to Prevent Future Occurrences

Implement Electronic Travel Order and Travel Voucher Claim System

Since the scheme unfolded, American Logistics has started using a new electronic travel order and travel voucher claim processing system. Controls are set to prevent the oversight of individuals who might manipulate the system, like Marin. Still, the individuals who are responsible for authorizing travel claims should review them for accuracy and legitimacy.

Require and Check for Appropriate Documentation

Travelers should submit appropriate documentation (i.e., receipts for any costs at $75 or higher) when filing their travel voucher claims. Otherwise, the voucher should be returned to the traveler until he or she can support the claim.

Use Common Sense

Ensure that the travel voucher claims, especially where the traveler has to list them, pass the commonsense test. For example, parking costs to stay at a particular hotel are usually charged to the room and appear on the final hotel bill. If the traveler claims parking fees, but they do not appear on the hotel bill, the authorizing official should investigate the claim.

Establish and/or Utilize a Cross-Communication System within the Organization

All authorizing officials should take the time to review vouchers for padded or incorrect claims. Establish a system that ensures that all departments are notified and capable of reacting when a false claim is uncovered so that proper actions can be taken to minimize damage and weed out those individuals responsible for the fraud. Directors who have oversight of employees should be included in the voucher-reviewing process, so that they can cumulatively corroborate the travel status of the employee.

Inform the Travelers of Consequences and Maintain a Watchful Presence

Travelers should be aware of the consequences of filing false claims. Communicate the penalties that can be imposed. Also, periodically conduct independent reviews so that selected travelers can be contacted directly and questioned about individual charges.

Dominic A. D'Orazio, CGFM, is a senior evaluator for a U.S. Army Internal Review Office in the northeastern United States. He has assisted the criminal investigators on numerous cases involving white-collar crime. Mr. D'Orazio is a graduate of Philadelphia University and has over 28 years of experience in auditing.

What About Pete?

MICHAEL GOLDMAN

This is a story about failed partnerships, failed marriages, and rampant bankruptcy fraud. What once appeared to be a successful company progressed through a legitimate bankruptcy filing, followed by a postpetition looting of funds. There are related-party transactions, ghost payroll checks, benefit withholdings, quadruple-entry accounting, mortgage application fraud, wire and mail fraud, money laundering, and fraudulently filed bankruptcy operating reports. The story isn't over yet, but so far there have been more than $5 million in civil judgments issued and settlement payments made by five banks that were unwitting participants in these various schemes.

It began with Fred Morgan, the owner of Gopher Design. Fred was in his mid-40s, smooth and charismatic, and always well dressed. He was slender and a little frail looking, a bona fide lady's man, but definitely not the type who would do well in prison. People have one of two reactions after meeting Fred. The majority liked and trusted him instantly. But a small minority of us felt the urgent need to check our pockets and take a quick shower after shaking his hand.

Mrs. Morgan was not as physically attractive as her husband, but had been a winner of the gene-pool lottery in other ways. Her father had built a hugely successful business empire that created enough wealth to keep his offspring very comfortable for multiple generations. Her parents didn't seem to like her husband particularly, but they were there with open arms and an open checkbook whenever anyone in the family needed money. There was no apparent reason why Fred would ever resort to theft when he was married to such a huge source of wealth.

Fred's number-two guy, Pete Slowinski, was almost the exact opposite of Fred. While Fred could sell ice to an Eskimo, Pete seemed to rub everyone the wrong way. He was rough, tough, and gruff. Physically, he was short, squat, and very muscular. And his face was very flat, as if he had been hit with a shovel in his formative years. His blank stare of ignorance was a stark contrast to Fred's apparent total knowledge about almost anything you could think to talk about.

When anyone who knew him was asked if Fred was capable of committing fraud, they answered that he was smart enough and gutsy enough, but there was no reason for it; his wife's family was wealthy beyond belief, and Fred could dip into that trough whenever he wished. The same question about Pete elicited a unanimous answer: He didn't have the brains to defraud anybody; he just did what he was told.

The differences between the two men even extended to their choices in women. Mrs. Morgan was the definition of "shrew." Employees literally quaked in fear when she walked through the office. She was loud, obnoxious, and totally abrasive. Fred was rumored to have an Italian girlfriend in Italy, whom he visited often. Mrs. Slowinski, Pete's wife, was a quiet woman well liked by everyone in the company. Employees generally felt bad for her because Pete had a public affair with the company's shipping clerk, a very plain and quiet young woman.

Gopher Design had been a successful graphic arts company for more than a decade. Its client list included many large advertising agencies, Fortune 500 companies, local restaurants, and nonprofit agencies. Gopher's customers had a tough time in the years when businesses were hit by the dearth of advertising that followed the 9/11 attacks, weakness in the hospitality industry, and massive changes in charitable donation patterns resulting from changes in tax laws, and disasters—some natural, some not. Technology changes that impacted both the way that design work is done and the way that Gopher's customers disseminate their information created a great need for large capital spending. Despite this, Gopher had not suffered the economic hardships that many of its competitors experienced.

Fred and a partner had run Gopher together since its inception, but eventually had a falling out. The partner left the business, sued Fred in state court, and won his case. Fred continued to operate the business, but had been ordered by the court to buy out his former partner for an amount in excess of $1 million. Rather than make this payment, he placed the company into voluntary Chapter 11 bankruptcy.

Gopher's bankruptcy case appeared to progress normally, but slowly. The debtor's bank suspected check kiting at various times but was never able to prove anything more than careless cash management. Personal lawsuits against the bank president filed by Fred and by other companies that his family owned kept anyone from investigating him too thoroughly. The bankruptcy court finally confirmed a plan where Gopher would pay its secured debt in full and about 33 cents on the dollar of all its other prepetition debts. Everybody was looking forward to Gopher emerging from the bankruptcy process as a healthy, rehabilitated company.

Rather than serve as the poster child for bankruptcy success, Gopher crashed and burned immediately upon its release from court supervision. It emerged from bankruptcy with no cash and hopelessly insolvent. The U.S. Trustee immediately stepped in, put Gopher back into bankruptcy, and appointed a Chapter 7 trustee to investigate what had happened.

Call to Duty

I was at the base of a mountain in central Quebec when the Chapter 7 trustee called my cell phone, introduced himself, and told me that the U.S. Trustee had recommended that he call me to help investigate Gopher. I had served as examiner in a bankruptcy case involving allegations of fraud both prior to and after the bankruptcy filing, so the U.S. Trustee was familiar with my work. He went on to explain that because there was no money at all in the bankruptcy estate, there was a good chance that I may never get paid for taking the case. I must have been drunk on the fresh mountain air, the overwhelming beauty all around me, and the joy of being with my family—I said I'd do it.

My first day back from vacation, I met Fred and an attorney from the trustee's firm outside Gopher's offices. Fred was pacing back and forth, totally distraught when we arrived—the alarm company had discontinued service, the building had been broken into, and most of the sophisticated computer equipment was missing. Fred took us inside and showed us the point of the break-in. Interestingly, the splinters still on the door all pointed to the door being kicked out from the inside. Some of the "stolen" computers were subsequently found, much later, to have been given to employees in lieu of amounts that Fred owed to them.

I asked Fred to give us a tour of the facility. We started with his office, which was totally empty except for a box of monthly operating reports that he had filed with the bankruptcy court. He explained that he was only a figurehead in the company and that Pete Slowinski ran absolutely everything. When I asked about the operating reports, he answered that he didn't understand a single thing on them, he was totally baffled by numbers and accounting, and that all he did was sign what his accountants prepared for him.

As we walked through the various cubicles, Fred became more and more distraught at each set of dangling wires where computer equipment used to be. He didn't know where any of the company's business records were or how we could get in contact with the former accounting staff, or how anything could possibly be figured out. If only he had stayed more involved, things may have worked out so much better, he whined. After all, he lost more than any creditor—his livelihood, his reputation, and all his personal net worth were gone with Gopher.

Fred's only contribution to the investigation was the ability to tell us who sat in each of the cubicles. He claimed not to know anything else about the business. File cabinets were all locked, and Fred had no idea where the keys were. Pete's office was jammed full of clutter—files and paper were everywhere. Despite the office being an incredible firetrap full of stuff, the only usable documents were a very impressive collection of carry-out menus from practically every restaurant within a five-mile radius. It was clear from the food stains on them that the menus were not there to sample different design styles.

The cubicle next to the accountant's had been vacant. There were dirty, dusty boxes jammed under the work surfaces. When I opened them, I found binders of batch reports showing inputs (billings to customers, invoices from vendors, commissions due) into the accounting system and some of the outputs (accounts payable checks paid) from the system. I was thrilled as I carried boxes out to my vehicle. This was a very messy and overwhelming way to start an investigation, but at least all those boxes gave me justification as to why an accountant might need a business truck if the IRS ever questioned my tax deductions.

A few days later, Fred attended a meeting at the U.S. Trustee's office. This was a chance for the Chapter 7 trustee to ask him questions about anything related to the case, under oath. Unfortunately, we still didn't have enough information to know what to ask. All we had to go on at this point were copies of cancelled checks provided by the bank and the monthly operating reports submitted by Fred. He wanted so very badly to help us, he said, but he just didn't know anything.

It turned out that Fred was familiar enough with the operating reports to be able to boastfully point out that he had stopped drawing a salary after the first few months of the case. He did this, he said, because the company couldn't afford him and he wanted it to succeed. Later in the questioning he admitted that the company had been paying large bills for credit cards in his name, but that was only because the company had no credit and Fred was personally paying for expenditures the company needed. Later still, he admitted that the company had made payments for personal loans taken out by him, but that was only fair since he was not otherwise being compensated for all his efforts on the company's behalf. There was already enough inconsistency here for the case to get interesting.

It's All in the Details

Back in my office, I had to figure out what to do with three truckloads worth of boxes of batch reports. My initial hunch was that since the salesmen spoke highly of Fred, he probably hadn't cheated his salespeople out of their commissions. If I compared the sales used to calculate commissions to the sales recorded in the general ledger and in the receivables system, I was bound to find discrepancies that would prove that sales were being diverted. I gave up on this after two weeks; every single item I looked at traced through all the documents just as it should have.

I visited with the bank president who had been unlucky enough to be Gopher's lender. He was convinced that Fred had been kiting checks, and gave me more boxes containing 28 months' worth of bank statements and cancelled checks. Another week of charting and diagramming the ins and outs of the bank account showed that looking for kited checks was also was a dead-end endeavor.

One curious element did pop up from the bank account work, but I didn't know what it meant or what to do with it: Fred used many different banks for his personal accounts and for the other companies that he controlled. I noticed this when I reviewed deposits into Gopher's accounts and from the endorsements on the backs of some of the checks that Gopher had written to Fred.

Stymied, I turned to the monthly operating reports. All of the activity reported through Gopher's main bank tied out to the bank statements. All of the activity reported through Gopher's secondary bank also tied out the bank statements. But if everything was tying out, there should have been more cash. It didn't make sense. I needed to look at the detail behind the reports and accounting batches.

Crawling around under the desks at Gopher's offices again, I found more boxes of documents in the area where human resources used to work. This was the good stuff: original deposit slips, copies of the checks that customers had remitted, and original remittance advices showing what the customers had paid for.