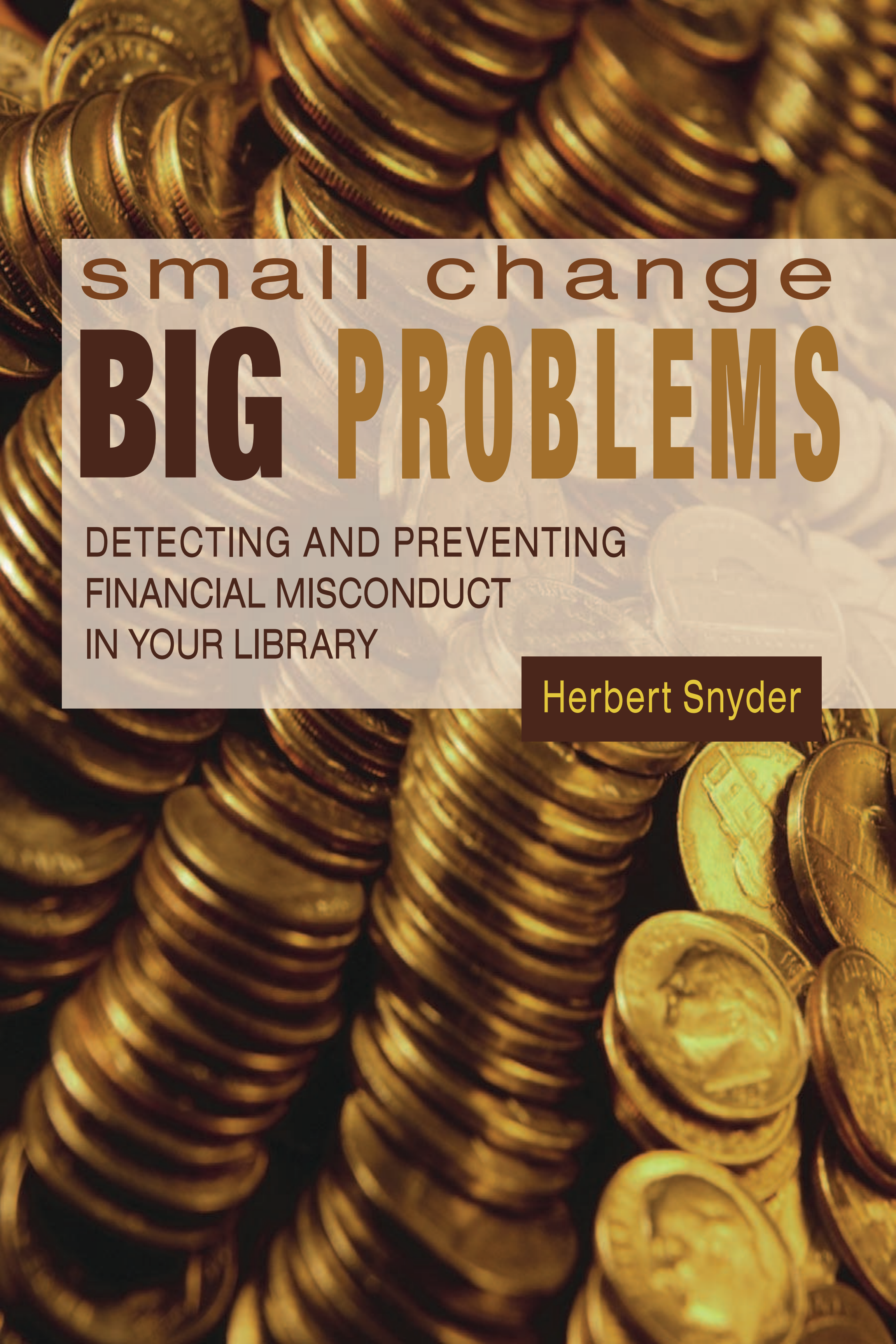
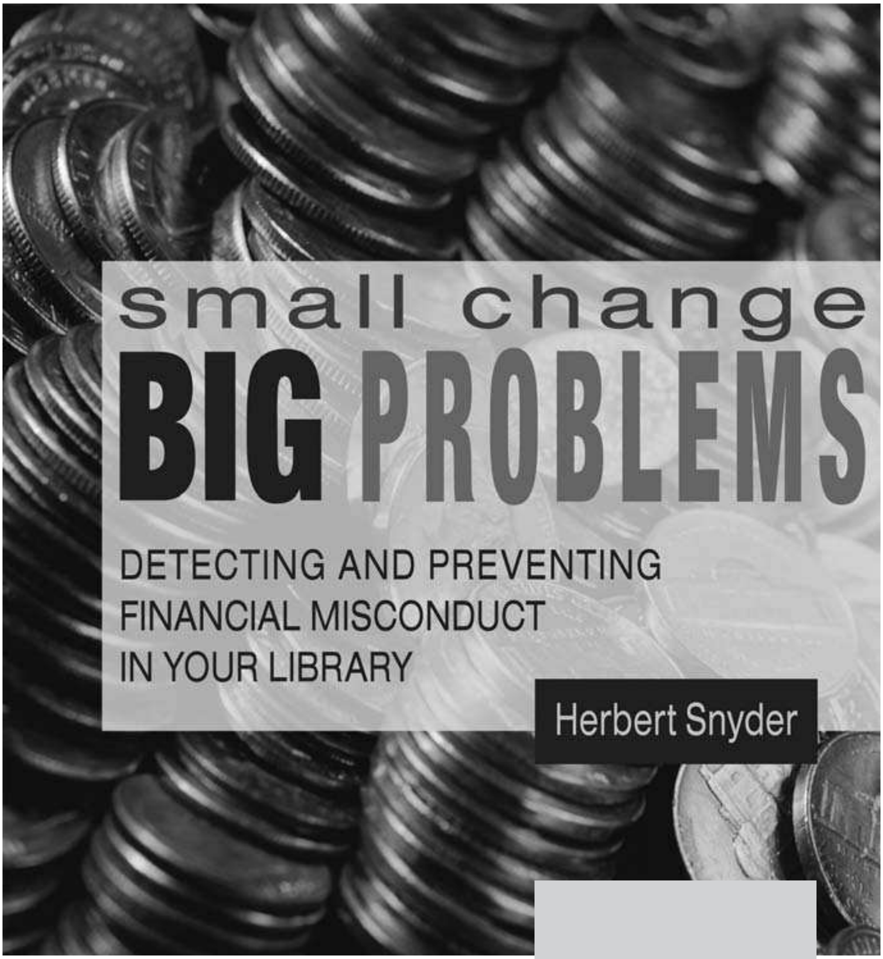


small change BIG PROBLEMS

DETECTING AND PREVENTING FINANCIAL MISCONDUCT IN YOUR LIBRARY

Herbert Snyder



small change BIG PROBLEMS

DETECTING AND PREVENTING FINANCIAL MISCONDUCT IN YOUR LIBRARY

Herbert Snyder

AMERICAN
LIBRARY
ASSOCIATION
Chicago
2006

While extensive effort has gone into ensuring the reliability of information appearing in this book, the publisher makes no warranty, express or implied, on the accuracy or reliability of the information, and does not assume and hereby disclaims any liability to any person for any loss or damage caused by errors or omissions in this publication.

Printed on 50-pound white offset, a pH-neutral stock, and bound in 10-point cover stock by Batson Printing.

The paper used in this publication meets the minimum requirements of American National Standard for Information Sciences—Permanence of Paper for Printed Library Materials, ANSI Z39.48-1992. ∞

Library of Congress Cataloging-in-Publication Data

Snyder, Herbert.
Small change, big problems : detecting and preventing financial misconduct in your library / Herbert Snyder.
p. cm.
Includes bibliographical references and index.
ISBN 0-8389-0921-3
1. Library finance. 2. Fraud—Prevention. 3. Fraud investigation. 4. Libraries—Corrupt practices. I. Title.
Z683.S65 2006
025.1'1—dc22 2006013937

ISBN-10: 0-8389-0921-3
ISBN-13: 978-0-8389-0921-8

Printed in the United States of America

10 09 08 07 06 5 4 3 2 1

Contents

Preface

Embezzling from a library? Doesn't that show a lack of ambition?

—Early reviewer of the author's research

I can't believe you'd accuse librarians of stealing.

—Excerpt from a letter received by the author in response to a journal column

I confess that I've used these two quotes before, but I begin with them because they do such a good job of illustrating the problems that face anyone who's interested in improving fraud prevention in libraries. The first difficulty is that people simply don't take the problem seriously. I admit, at one time I was one of them. But the truth is, embezzling from libraries doesn't show a lack of ambition. Whatever libraries might once have been, they are now large organizations, many with budgets in the millions.

The problem is that although many criminals have figured out that libraries have budgets worth stealing, library administrators and board members have been slower to recognize the risk. There are many possible reasons for the lag in perception. Until recently, financial management wasn't thought to be a necessary part of a librarian's training. Even today, relatively few MLS programs offer classes in it. Thieves are usually more attentive to the opportunity to steal than honest people are to the need to guard their possessions. Whatever the reasons, we've entered a period in which protecting a library's assets has become an important aspect of library management.

In response to the second quotation, I would note that contrary to popular belief, fraud and embezzlement have a long history in the profession of librarianship. Klas Linderfelt, director of the Milwaukee Public Library and president of the American Library Association from 1891 to

1892, was forced to resign from his position when he was found to have embezzled over $9,000 from his employer, the equivalent of over $100,000 in today's dollars (Hersberger and Snyder 2000). In modern times, a quick review of the popular press seems to elicit a new financial scandal in every edition (Oder and Rogers 2005; Tsao 2005; *New York Times* 2003). Librarianship isn't and has never been a cloistered profession. Plenty of librarians commit crimes, just as plenty of firefighters, senators, and nurses do. What's more important, though, is that making the observation that library assets need to be protected better isn't the same thing as calling librarians criminals. As we'll see later in the book, trust has never been sufficient to protect assets. Anyone has the potential to commit fraud, so we're forced to devise protections for what's possible, not for what we hope people will do.

For library directors, board members, and anyone else who deals with library finances, I hope this book will show you how fraud occurs, how to detect it, and, above all, how to prevent it.

Acknowledgments

Authors are delicate creatures, and the amount of support they require knows no limits. Many people helped to make this a better book, including Carolyn Crabtree, my copy editor, who struggled to ease the strain of my tortured prose.

There are, however, four people without whom this book could not have been written: my father, Harry Snyder, who originally taught me that stealing was bad; my wife, Barbara Dunn, who kept me alive during the writing and never lost her temper; Laura Pelehach of ALA Editions, who foolishly opted to read my proposal; and Barbara Preece, editor of *LA&M*, who gave me my first column, the original basis for this book. Thanks all.

~1~

Fraud: How It Occurs in Organizations and Why Libraries Are Susceptible

WHAT IS FRAUD?

Fraud is not a homogeneous crime. The crimes that we include under the rubric of fraud include elements of larceny, forgery, embezzlement, confidence games, and other crimes, depending on the statutes of the states in which they're committed. Nevertheless, we'll need some sort of working definition, because the methods for detecting and preventing fraud are different from those for other crimes such as robbery or vandalism.

The essence of fraud is to obtain property from another person or organization by illegal means. In general, there are two options for accomplishing this: forcing the person (either physically or mentally) to give up his or her property or tricking the person into doing it. Extortion and robbery are examples of the first option, whereas fraud falls into the latter category. Frauds can be committed against individuals—for example, the victims of confidence games. However, for the purposes of this book we will be concerned with frauds committed against organizations, usually by their employees. Such crimes are known as occupational frauds.

The most common working definition for occupational fraud, and the one that we'll adopt for this book, involves five parts:

1. Illegal conversion of property
2. Violation of an employee's fiduciary responsibility
3. Direct or indirect benefit of the employee
4. Concealment of the crime
5. Cost to the employer (assets or revenues) (Wells 2005)

Two elements of fraud are of particular interest to us in the context of prevention and detection. The first is violation of fiduciary responsibility. In other words, frauds are committed by people whom the organization trusts and who subsequently violate that trust. Frauds are the quintessential “inside job.” Indeed, by definition, they require an insider. The second aspect is concealment. Once the act has been committed, the perpetrator must conceal it—for example, by falsifying the accounts to conceal the theft of petty cash. Fraud differs in this way from other property crimes such as burglary or simple larceny (e.g., burglars don’t usually bother to conceal break-ins).

The combination of these two elements makes fraud uniquely difficult to investigate and prevent. To begin with, it’s often difficult to know whether a crime has been committed. Unlike the burglar who leaves a broken window, an overturned desk, and an open safe, fraudsters attempt to cover their tracks. Worse yet, many libraries have abysmal accounting systems, making it difficult to separate crime from simple incompetence. (Imagine the same burglary perpetrated in an incredibly messy office. How would you know whether an outside criminal had ransacked the room?)

Fraudsters also begin with an advantage over the investigator—they know more about the system they’re stealing from. They may, in fact, have been studying it for years. This helps them to commit the crime by understanding the system’s weaknesses, and it helps to conceal it. A fraud investigator usually spends the majority of his or her time in the initial stages of an investigation simply trying to understand how the organization’s financial system works.

Finally, people who commit frauds frequently appear to be above suspicion. In order to violate a position of trust, you first have to be trusted. As we’ll see in the following section, most fraudsters are long-time employees who performed well enough over time to rise to a position of responsibility.

WHAT KIND OF PEOPLE COMMIT FRAUDS?

The short answer to the question of what kind of people commit frauds is all kinds. Unlike serial killers or drug dealers, people who commit fraud have no consistent profile. In fact, it’s the ordinariness of fraudsters that sets them apart from other criminals. They look like we do.

Serial fraudsters are an uncommon phenomenon. In most cases, fraudsters are created, not born, and their fraud is the first crime they’ve ever committed. This has two important implications for managers interested in preventing fraud:

1. Most people are probably capable of committing fraud.
2. There's no way to predict who will commit a fraud.

Fraudsters begin as honest employees, and a combination of factors, the so-called fraud triangle, causes them to commit a fraud. In practice, a manager's intuition and experience aren't of much use for detecting employees who are likely to steal using fraud.

WHY DO EMPLOYEES COMMIT FRAUD? THE FRAUD TRIANGLE AND LIBRARIES

The basic elements needed for fraud to occur were outlined by Donald Cressey in his work on embezzlement, *Other People's Money* (1953). The elements look like the same triangle we learned about in third-grade science that showed the requirements for fire. In the case of fire, the triangle consisted of heat, fuel, and oxygen; in the case of fraud, the three elements are:

1. Financial need, sometimes referred to as pressure
2. Rationalization
3. Opportunity

As with fire, all three elements need to be present for a crime to occur. Conversely, removing one of the elements prevents or ends the crime. That being the case, let's examine each of the elements in detail, particularly as it relates to libraries.

Financial Need/Pressure

Crimes, at least financial crimes, are usually committed for a reason. The perpetrator requires money (or some other valuable commodity, including justice) and is otherwise unable to acquire it by legal means. As a result, he or she makes the decision to commit a crime to obtain it.

The important thing to consider for this element is that people's lives and needs change over time. Most fraudsters start out as honest employees. However, a formerly honest employee may undergo a personal disaster, acquire a drug addiction, or experience some other problem that increases his or her need for cash. In class, I often have students who steadfastly refuse to believe that they could commit a crime. However, when they're asked questions such as "Would you allow your mother to become homeless?" or "Would you allow a spouse to die for lack of medical care?" rather than commit fraud, they invariably find some instance in which stealing from an employer would be preferable. Some of the students, speaking with a bit more candor, also admit that they might consider stealing if they were in the throes of a severe drug addiction or gambling debts.

The point here is not to determine where an individual draws the line but simply to understand that honesty as a defense against fraud can eventually break down for most people. This is not to say that all needs are creditable or altruistic. The desire for higher social standing, to be better looking, or to drive a larger car can be equally compelling reasons for some people to commit crimes. Greed can be a powerful motivation for financial crime, especially as the media exposes us to the lifestyles and material wealth of the rich and famous.

Another type of pressure about which employers should be aware is restoring equity. Employees frequently commit frauds as a method of righting what they perceive as inequality in the workplace. This may include being passed over for promotion, not getting a raise, or perceiving that other employees are receiving preferential treatment. In a similar vein, employees may commit frauds against the organization as revenge for perceived ill-treatment or disrespect. The key word here is *perception*. What employees *believe* is happening triggers these behaviors, not necessarily what's actually occurring. From the perspective of fraud prevention (among many other reasons), it's a good idea to keep an eye on employee morale. Employees who feel valued and respected by their employers are less likely to commit fraud.

Rationalization

A second side of the fraud triangle is rationalization. In order to commit the crime, the perpetrator must create some morally acceptable excuse for doing it. Fraudsters employ a wide variety of reasons for excusing their actions. The most common is that they intended only to borrow the funds. The stolen money was intended only to tide them over during a time of temporary financial need. Funds were taken with the expectation that they would be replaced when conditions improved. No doubt some fraudsters actually do this, but more frequently the need turns out to be more than temporary or the ease with which the fraud was committed encourages the employee to continue taking the money. In any case, the funds are never replaced, and the fraud grows in magnitude. In other instances, fraudsters excuse their actions with the rationale that they took the money to benefit another person. This may even be true (as in the case of medical treatment for a spouse), but more often it's simply a matter of providing a better lifestyle for the fraudster's family.

My personal favorite involved the theft of nearly $200,000 by the director of a regional audiovisual materials library. The individual was convicted, and a psychiatrist's report was included as part of the sentencing materials. According to the good doctor, the director embezzled because she hadn't received enough love as a child and had self-esteem issues. The only way she had of compensating for her low self-esteem was to use the library's funds to acquire an expensive wardrobe.

We should also be aware that there are aspects of the library profession that contribute to the process of rationalization. Most service professions socialize their members to acquire a personal investment in the work they do—"This is *our* library." By itself, personal investment can be a positive force in the workplace; it encourages a sense of greater value in a profession that may not offer many monetary rewards. However, the sense of ownership can also foster inappropriate conclusions: "Not only is this my library but the assets belong to me." This can be an especially pernicious train of thought when librarians incur a number of work-related expenses that are not reimbursed by the library. It's often a short step from feeling that the library owes us something for the time and money we invest in our jobs to actually collecting on the debt.

Of course, not all or even most librarians act this way, but it is a real phenomenon that we ignore at our peril. There are, for example, numerous instances of library directors who forget that they are not sole proprietors of a company and who use the library's assets as if they were their own.

Opportunity

The final element needed for an individual to commit fraud is opportunity. Need and rationalization don't usually lead to crime unless there's an opportunity to steal something. Cressey initially defined opportunity as having two parts: general information and technical skill. According to Cressey, in order to commit a fraud an individual needed to be aware both that an opportunity to steal existed and that he or she had the skills necessary to exploit the opportunity. In essence, an individual's job skills dictate the type of fraud he or she is most likely to commit.

In my experience, employees who were contemplating fraud looked at three aspects of opportunity:

1. Opportunity to commit fraud
2. Opportunity to conceal fraud
3. Opportunity to avoid punishment

Aspects one and two are implied but not specifically stated in Cressey's theory. As we discussed earlier, a basic element of fraud is the concealment of the crime. Given that, the technical skill to commit the crime implies that the perpetrator can cover his or her tracks. Reducing the ability both to commit and to conceal fraud helps prevent it from occurring. What's less obvious is that employers can undermine their own antifraud efforts if they don't remove the opportunity to avoid punishment.

Simply detecting fraud does little to prevent it if there are no adverse outcomes to being caught. Employers are often reluctant to prosecute their employees, yet swift and consistent punishment is what makes employees stop and consider their actions. Termination can be explained away for a variety of reasons. Prosecution, however, even if it is unsuccessful, is a publicly humiliating experience. Remember that for most employees in this situation, fraud is the first crime they've ever committed. The shame of having to explain their criminal behavior to family and friends will be a strong deterrence to committing a crime.

Another important aspect of opportunity, at least from a management perspective, is that it's the easiest element of the fraud triangle to control. Need and rationalization are highly personal and internal elements. We can, of course, try to influence them through such actions as setting a high ethical standard in the library (which discourages rationalization) or creating employee assistance programs (which help mitigate financial need issues). For the most part, however, it is not possible or appropriate for an employer to influence rationalization and need issues. The same is not true for opportunity, however. As the employer, we establish the nature and extent of the financial control system in the library. We may not be able to change (or even be aware of) rationalization or need, but we can remove sources of temptation.

I often use this argument when I'm advising organizations to improve their financial controls: anyone's life can change; by removing the opportunity to steal, we're providing a service to our employees. Fraud almost never improves someone's life, no matter how desperate the person's finances. Therefore, by reducing the chance to succumb to temptation, we're helping that person to avoid trouble. Conversely, if someone does commit fraud, good financial control (i.e., reduced opportunity) protects innocent employees from suspicion.

HOW ARE LIBRARIES UNIQUELY AT RISK FOR FRAUD?

Although there is nothing to suggest that libraries are at any greater risk for fraud than any other type of organization, there's also no evidence that they're any better protected. There are realities of library life that increase the risk of fraud, and we don't do the profession any benefit by ignoring them. Anyone who deals with libraries as either a manager or a board member should be aware of the factors that may predispose libraries to fraud.

Higher Budgets

It's probably best to consider higher budgets in the context of opportunity—you can't steal anything if there's nothing of value to take. That certainly isn't the case today (if it ever was). According to *Library Trends*' 2005 budget survey, the average budget for a small public library (population served 10,000–24,999) was $636,000 (Oder 2005). The amount may not be large in terms of running a library, but it's more than enough to tempt a potential fraudster.

Lack of Strong Financial Management

Studies of fraud in libraries and other nonprofits clearly reveal that those organizations experiencing fraud have essentially no financial controls (Snyder and Dietz 2006; Snyder and Hersberger 1997). Such organizations regularly violate the most basic principles of financial control.

The research indicates two causes for this lack of financial control: (1) library personnel and board members are often not aware of the magnitude of library assets (particularly cash), and (2) librarians and library board members are not adequately aware of sound practices of financial management. As a result, neither group recognizes the need for more sophisticated financial management or understands the risks that libraries run in operating without it.

Cash flows have risen, and significant amounts of money are now taken in by libraries, but this development has not been met by a corresponding change in management practice. Fines, for example, are now a significant revenue source for many libraries. One library director who had experienced embezzlement noted, "I never realized how much money comes in [from] fines. We're only a medium-sized library, but we take in between $80 and $200 a day in fines. That's enough to be worth taking if somebody wanted it." A similar occurrence took place in another library, in which over $400,000 in fines was embezzled. As one employee of the system stated, “Nobody ever knew there was so much cash, so we never looked closely at our internal procedures.”

Apart from cash, library budgets have grown to levels at which more formal and sophisticated financial management is needed. As one auditor noted, “You have what are essentially businesses with budgets of $80,000 to $100,000 or more that don’t even reconcile their checkbooks, let alone keep a set of books.” Financial management, however, is not a standard part of library education, and as one director described the situation, “You don’t ever see a set of books until you have to manage a library with a $100,000 budget.”

Lack of Financial Controls and Oversight

Another problem is that daily financial management is frequently under the control of a single individual who is not otherwise subject to the financial controls and oversight normally found in profit-making entities. In many libraries, either the board treasurer or the library director supervises financial matters. In such a situation, there is essentially no segregation of duties for the financial functions. Ostensibly, the library’s board of trustees should provide oversight. However, board members often are unaware of this role and fail to exercise it.

The audit profession can also fail to notice this weakness during audits. Nonprofits frequently resemble sole proprietorships, with the result that material control weaknesses appear to be dealt with through the compensating measures of the owner’s involvement. Unfortunately, the director and treasurer are not the owners of their library, and their personal intervention doesn’t guarantee that they won’t embezzle from it.

Governing Boards Composed of Volunteers

Volunteer boards do not necessarily provide poor financial oversight. However, conditions that occur more frequently in volunteer management boards make frauds significantly easier to commit and harder to detect.

> *Board members are often not aware of their financial oversight duties*. A common theme among board members in all types of nonprofit fraud is this: “We didn’t realize we needed to provide oversight.” Although this may be an attempt by some board members to absolve themselves of responsibility, it is usually the case that they receive little or no orientation in their duties. Because boards frequently have many duties,

it may not be readily apparent that financial oversight is a key purpose.

Board members often have little or no financial background. This lack supports board members' difficulty recognizing their financial oversight duties. Board members serve for a variety of reasons. As a result, there may be no members with any expertise in accounting. This increases the likelihood that board members will not be aware of the need for independent financial oversight or, if they are aware, will not be able to provide it.

Turnover among board members can be high. Most board members serve in addition to full-time work and family life. The potential for exhaustion is high, particularly among members with professional expertise such as lawyers or accountants. Apart from the loss of expertise, high turnover reduces the level of corporate memory. At any given time, there may not be members who recall the financial history of the library or the policies that have been followed in the past to ensure financial accountability.

Lack of Independent Audits or Outside Accountability

Parent organizations such as universities or municipalities vary widely according to the amount of accountability they require from libraries. The requirements vary from complete financial control through a municipal finance office to independent finances with regular audits to no oversight at all. The trend in most governmental units has been toward greater autonomy and less oversight, particularly in the wake of shrinking tax revenues and smaller budgets.

"It Will Never Happen Here" Mentality

The organizational culture of libraries leads them to believe that their community service mission is sufficient to protect them against financial misconduct. This might be termed the law of sympathetic magic and is often shared by organizations who are engaged in a charitable purpose. Basically, the argument is this: "Who would steal from a library (or mom, or orphans, or God)?" There is, perhaps, some validity to the argument, because members of service organizations are apt to share common values. Unfortunately, as countless case histories have demonstrated, fraudsters are able to rationalize even the most heinous financial crimes.

Low Compensation—Not the Threat You Might Think

I'm sure it isn't news to anyone reading this book that working in the library profession is not the path to personal wealth. Moreover, the financial squeeze that many libraries experience in the face of tax cuts and rising benefit costs places additional financial burdens on those employed in the profession. What's interesting about this situation, though, is that there is no strong evidence that low compensation or a tight economy causes increases in white-collar crime. There's some intuitive appeal to the situation: people commit fraud when they live beyond their means; as income shrinks it becomes more likely (or even inevitable) that people will exceed their means in order to live. However, no evidence to support this theory currently exists.

WHY SHOULD LIBRARIES RECOGNIZE THE RISK?

The greatest trick the devil ever pulled was
convincing the world he didn't exist.
—Verbal Kint, *The Usual Suspects*

I'm not going to take a theological turn here, and even if I were, I'm sure I could find a more authoritative source than *The Usual Suspects*. However, there is a point to the quotation as far as coping with library fraud is concerned. Effective deterrents to fraud or any crime begin with the realization that a risk exists. In the specific case of fraud, the realization is that an organization has assets that are worth stealing. Part of the difficulty in library fraud prevention is simply getting the board and managers to believe they're at risk. They may, for example, feel strapped for cash and not realize exactly how large their budget is in absolute dollars. Similarly, a real difficulty with many libraries is simply getting them to acknowledge that their community service is an insufficient protection against fraud.

I have noticed that when we try to improve fraud protection in libraries, we are really dealing with two related problems: designing fraud prevention systems or detecting existing fraud, and changing or working around organizational behaviors that increase fraud risk. I don't want to minimize the difficulty in doing good investigation and fraud prevention, but they aren't enough by themselves. Good solutions often fail if they don't take into account the culture of libraries that predisposes them to the risks of fraud. As with many organizations, the struggle is changing or working around organizational behaviors that increase fraud risk rather than designing antifraud programs. As a result, I don't want this book to simply be an accounting text that substitutes the word *library* for *corporation*. Instead, I hope in the subsequent chapters we can work on two parallel sets of solutions: the technical aspects of detecting and preventing fraud in libraries and the change management necessary to convince library directors and boards to embrace better fraud prevention. Chapter 2 will cover what I consider the most important aspect of fraud prevention—internal controls.

2

Internal Control: What It Is and Why Libraries Need It

WHAT IS INTERNAL CONTROL?

All organizations need some type of structure to ensure that their operations run smoothly. This is the purpose of internal control (IC) in organizations, although IC isn't the only structure that organizations have. There are a number of definitions for IC in the accounting and fraud prevention community, but the most commonly cited (and in my opinion the most useful) definition was formulated by the Treadway Commission, which investigated financial fraud in corporations in the mid-1990s. (The work of this commission, also known as the Committee of Sponsoring Organizations, or COSO, is commonly referred to as the COSO IC framework [COSO 2005].)

The Commission defined internal control as

> a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:
>
> - Effectiveness and efficiency of operations.
> - Reliability of financial reporting.
> - Compliance with applicable laws and regulations. (COSO 2005)

In other words, organizations (including libraries) establish internal control to aid them in more effectively meeting their goals. More specifically for our purposes, organizations rely on IC to ensure material errors and fraud do not occur or, if they do occur, to ensure that they are discovered promptly.

IC is probably the cheapest and most effective means of dealing with fraud and is often the most overlooked. The difficulty is that although early detection or prevention or both are usually the best ways of dealing with any problem, we tend to ignore them as solutions because we don't feel any urgency for future problems. (Who hasn't, for example, known someone who never cared about diet or exercise until the first heart attack occurred?)

WHAT ARE THE ELEMENTS OF INTERNAL CONTROL?

Employee Selection

It is a truism in fraud protection that controls are no more effective than the people who use them. This precept sounds so obvious that you might imagine everyone in business not only knows it but incorporates it into business practices. Unfortunately, a surprisingly large number of managers spend little or no time trying to select honest employees. Worse, they treat the employees they have so badly that it scarcely comes as a surprise when one or more of them retaliate by committing a crime against the employer.

I am not, by the way, excusing financial crime by employees. Theft is never a reasonable alternative to bad management. On the other hand, employers need to take some responsibility for their own protection. The single most common reason employees commit fraud is not greed or financial need but to correct some perceived inequity in the workplace.

Contented, honest employees are less likely to be involved in theft or financial misconduct. Therefore, selecting competent, honest employees (together with human resources policies and competent management that keep them from becoming disaffected) should be the cornerstone of any internal control policies. General management and human resources policies are beyond the scope of this book, so let's concern ourselves with perhaps the best internal policy for selecting honest employees—checking references.

Check Employee References/Job History

Although the majority of embezzlers start out honest, this is by no means a given. A small but growing proportion of employees who commit financial misconduct have a history of doing so with other employers. In fact, employers themselves often contribute to this phenomenon because they refuse to prosecute offenders once their crimes have been uncovered. In any case, many employers never check at all.

Checking references need not be onerous or time-consuming. Employment forms generally list a contact number and a name for each former employer. At a minimum, a cursory check by phone should confirm that prior employment was in fact legitimate and that professional licenses are valid. Pay particular attention to gaps in employment history, as these are sometimes areas the candidate wishes to keep hidden. The employer just prior to the gap may often be able to supply the name of a subsequent employer.

Depending on who you are speaking to, it's often possible to elicit more detail. In particular, it helps to let former employers know that a prospective employee will be in a position of trust and to ask them to comment on past performance. Although many employers will be reluctant to make damaging remarks over the phone, this is likely to be offset by awareness of their liability should the employee commit a second crime. In particular, it helps to inform the prospective employee that you'll be checking references. This often weeds out employees with difficult pasts before it becomes necessary to check on them.

It may become necessary to conduct employee checks in greater detail, depending on the level of responsibility the candidate will hold. If the library is large enough to have a human resources manager or administrative department, this is properly the job of such an office. Although the library directors or board members may not be conducting such checks themselves, they should ensure that proper procedures are in place for checking all employees and should occasionally check to see that such controls are actually being used. In libraries in which there is no separate function or in which administrators are working in this capacity, employee background checks can be outsourced to private companies that specialize in the service.

Trusting Employees Isn't Enough Even If They Are Honest

Many library directors may be tempted to stop their internal controls at the point where they feel that they have hired honest employees and are treating them well. Although that's a fine beginning, there are two major reasons why it isn't enough. The first is that employees change. As we observed in chapter 1, most embezzlers start out honest and turn to crime when they incur some great financial need. You're unlikely to identify this change until a crime occurs, so the more effective strategy is to remove the opportunity to steal. The second reason is that honesty doesn't guarantee competence. Good internal controls also protect against errors. Even the best employees can develop bad habits over time, and better oversight from internal controls helps prevent this from happening.

Segregation of Duties

Among the advice that organizations get from auditors and fraud prevention specialists, segregation of duties is the most common and the least well understood. I often see reports from auditors that advocate better segregation of duties but never go on to explain specifically what this means or whose duties should be segregated.

Segregation of duties, at its most basic level, involves splitting related job duties among several employees. When one employee uses information supplied by another, it becomes much easier to catch errors. A clerk, for example, may be tempted not to make the bank reconciliation come out to the last penny. However, if the cash amount he or she calculates has to balance in the trial balance that a different employee prepares, then the reconciliation has to be correct. If it isn't, the second employee will uncover the error while preparing the trial balance.

A second benefit that comes with segregating duties is that many types of fraud become more difficult to perpetrate. Imagine a situation (all too common in many libraries) in which the bookkeeper approves purchases, checks in new inventory, authorizes invoices for payment, and enters all the information from these transactions into the accounting records. In circumstances like these, the following frauds become easy for the bookkeeper to commit:

Steal the inventory for personal use and simply say it was not received. The library pays for purchases it never received.

Print invoices for phantom vendors and approve them for payment. The library pays for fake purchases it never received.

Approve purchases for personal expenses and record them as different, legitimate expenses.

Collude with a supplier to bill for more goods than are actually received. Approve the inflated amount and split the difference with the supplier.

Place a legitimate invoice for billing a second time, convert the check to his or her own use, and record the second payment as a legitimate expense.

This is by no means an exhaustive list of the types of frauds that are possible, but it should give you some idea of the potential damage that can be done by an employee with interlocking financial responsibilities. (Incidentally, administrators are sometimes critical of listing possible methods for committing crimes because such lists may provide instructions for committing crimes. Trust me—the thieves already know how to do this. The larger problem is that administrators aren't aware of the risk and consequently don't know how to prevent it.)

By distributing (or segregating) duties among several employees, many of the potential crimes just listed become much harder to commit. There is, of course, always the possibility of collusion, but the risk of discovery rises dramatically when more than one person is involved. The problem now becomes one of understanding how duties should be distributed in order to minimize the risk of fraud.

Any organization has four basic functions that create and maintain financial records and transactions:

1. Executing transactions
2. Maintaining records of transactions (including but not limited to accounting records)
3. Maintaining custody of assets
4. Comparing records of transactions with actual assets

Good internal control policies prevent an individual from doing more than one of these functions for the same set of assets and transactions. For example, the same individual should not be responsible for approving purchases (executing transactions) and checking the delivery of purchases when they arrive (maintaining custody of assets). In such a situation, the individual could steal assets and still claim they had arrived. Similarly, the same individual should not be able to approve the removal of a patron's library fines (executing and recording transactions) and prepare the daily bank deposits (maintaining custody of assets). In this situation it would be simple for the employee to steal cash from the daily fines and cover the theft by zeroing the patron's fine balance and adjusting the daily deposit.

The fourth item on the list—comparing physical assets with the transaction records—is sometimes overlooked by organizations that have segregated duties. The problem in this case is that segregation by itself does not necessarily prevent theft; it merely makes it harder to conceal it. Imagine a situation in which a library maintains a cash register and each patron who pays a fine receives a receipt. As a result, the library now has a record of the individual payments made during the day. A second employee (one who doesn't work on the cash register) prepares the bank deposits each day.

This is a classic separation of duties—the employee who handles cash does not make the accounting entry to record the receipt of cash, nor does he or she make the daily deposit. However, there is still nothing in the system that prevents the employee working on the cash register from pocketing the fine money. Of course it does, you say; the cash in the drawer at the end of the day should equal the money with which we started the day plus the money we received in fines. We know the amount we received in fines, because it will be the total from the cash register. This should also be the amount of cash we deposit each day. Any discrepancy will turn up when we compare the cash count to the register total.

It's this last item that becomes problematic in some organizations. If no one bothers to compare the accounting records to the actual assets (in this case, the register total to the actual cash on hand), then the system is worthless. That may sound strange, but many organizations act as if the separate sets of records will prevent fraud and errors by themselves. This obviously isn't true. Someone still has to make periodic comparisons and follow up any instances in which the two don't agree. The system still requires administrators and employees to pay attention to the results and pursue an answer when the records don't agree.

A final point concerning segregation of duties is that although independent checks require a segregation of duties, the converse is not necessarily true. That is, simply segregating duties doesn't guarantee that you'll have independent checks. For example, two employees may be involved in ordering inventory. One employee approves the purchase, and the second checks in the shipment when it arrives and prepares the check for payment. The second employee provides an independent check that the approved goods arrived, but no one checks the accuracy of the payment check against the list of received goods. In other words, the independent checking is not reciprocal. A third segregation, between asset custody and accounting, would be necessary to ensure that the payment made was for the inventory that was actually received.

In small to medium-sized libraries, formal segregation may not be feasible. Often, there are simply too few employees to assign specific office jobs. In situations like this, the best alternatives may be job rotation and enforced vacations (see the following section). Rotating employees through key jobs such as checking purchases, opening the mail, and preparing cash deposits provides different sets of eyes to examine transactions and has the advantage of cross-training employees in a variety of skills. Similarly, vacations provide periods when other employees review the work of coworkers for extended periods.

A second method of segregating duties in most libraries is through the work of the board of trustees. In many libraries, the board is the only group that provides any independent oversight, particularly when most of the financial decisions are made by a single individual (usually the bookkeeper or the director). The difficulty that arises when boards are the primary means of segregating duties is that board members are often not aware of their financial oversight duties. In libraries that are not part of a larger political or university accounting system, boards usually have check-writing power. Ostensibly, this should be an effective segregation of duties, because accounting and inventory custody are separate from the actual payment function. Unfortunately, the system works only when the board members insist that all checks be accompanied by proper documentation. (Considerably more time is spent on this topic in the sections on proper authorization and documentation later in this chapter and in chapter 5.)

Job Rotation and Enforced Vacations

One of the great ironies in many frauds is that they are committed by individuals who seem to be the best and most conscientious employees. "I can't believe it. He has been with us for twenty years. In fact, I never once saw him take a sick day or a vacation." This is a common reaction of many directors when they first learn of employee fraud. In fact, employees who never take a day off work should be viewed with concern, if not necessarily suspicion. Similarly, be wary of employees who never allow anyone else to observe their work or to learn how it's done.

Although enforced vacations and job rotation are two different internal control measures, they do essentially the same thing—have the same work reviewed by two different people. Generally, frauds require a great deal of attention and rarely stand up to scrutiny by outsiders, particularly for a week or more of vacation. However, even in cases where there is no fraud, fewer ongoing errors occur if one employee's work is checked by another employee.

These are often the easiest ways of segregating duties in a small office. In the case of job rotation, it is often necessary only to rotate key tasks such as opening the mail or making up bank deposits. Job rotation also has the advantage of cross-training employees so that key functions such as bill paying don't go idle during an employee's absence.

Bonding

Bonding is a form of insurance that reimburses the organization for losses incurred by the misconduct of a person in a position of trust. Should the employee commit some act of financial misconduct as part of his or her job duties, the policy indemnifies the employer for the loss. Many readers who have worked in retail establishments may have had experience with bonds that cover all the employees in a store for the theft of merchandise. Bonds also are available, however, for individuals in positions of financial trust (e.g., bookkeepers, treasurers, directors) and will repay the employer in cases of embezzlement.

Bonding is relatively common in the library world and may be mandated by law, depending on the type of library and state law. (In Indiana, for example, state law requires bonding for public library directors and treasurers.) However, library administrators and boards of directors often don't understand how little coverage they have compared to their levels of exposure.

Why Aren't Libraries Sufficiently Bonded?

It's easy enough to be critical of libraries that are underbonded, but in fact it is quite common to be underinsured. Most organizations grow, with a concomitant increase in the value of their assets. In many cases, however, no one ever considers the value of the organization's property until there is some reason to replace it. (How many of us, for example, ever bother to reassess the value of our own belongings and increase the limits of our homeowners' coverage?) A common practice in many organizations (including libraries) is to maintain the employees' bonds at the historical level of coverage. As one director described the situation, "We renew the bond based on what it was last year. I doubt there'd been a change before the embezzlement for twenty years."

Underbonding, however, is not simply a matter of setting policy coverage too low. Bonds generally cover only specifically named individuals. If someone not specifically named in the policy commits a crime, there's no reimbursement. The problem in many organizations is that the number of positions has increased but no one has examined the potential damage that an individual in these positions can accomplish. As a result, there may be many individuals with the capacity to commit financial misconduct who are not bonded simply because no one in administration realized that trust is required in their job.

How Can Libraries Become Better Bonded?

This section is probably starting to sound like a sales pitch from a life insurance salesman who's trying to frighten you into buying a policy by illustrating all of the colorful ways you'll die in the next twenty-four hours. Most library employees aren't on the verge of embezzling from their employers, but that's no reason not to take reasonable and cost-effective measures to help protect the library's assets. If you're interested in examining how well bonded you are, here are some areas to consider.

Who has responsibility for assets in your organization? More specifically, who handles money? This may require some research concerning job duties, but it doesn't need to be a major job analysis. Small libraries usually can be analyzed simply by taking the time to think about what each individual does. In larger organizations, a review of job descriptions is often enough to eliminate many positions from consideration. Keep in mind that positions of trust usually go unbonded simply because no one took the time to realize that there was any potential for loss. Also keep in mind that theft of cash is not limited only to people who handle cash. Employees who are able to approve payments, even if they don't physically handle cash, perpetrate numerous frauds such as creating phantom vendors.

How large is the exposure? If an employee has responsibility for assets, how valuable are those assets? Employees who handle checks and cash in the thousands or millions of dollars are clearly in a position to damage the organization more easily than those who deal only with petty cash. This is not to say, however, that such employees are the only ones who may need to be bonded. The frequency with which money is handled also needs to be considered. Many large embezzlements are the result of numerous small thefts over long periods.

Who is covered by your bonds and what is the level of coverage? As we've discussed earlier, almost everyone is underinsured, so you should expect to need higher levels of bonding for your current bonds and new bonding for the positions you've just discovered carry financial trust. The bad news is that your premiums will rise, but the good news is that they won't rise as much as you might imagine.

Premiums on bonds behave much the same as other insurance policies—the largest part of the cost is for the initial policy. Once you pay for the basic coverage, incremental increases aren't that expensive. For example, a basic $10,000 policy may cost $300 per year, but increasing the coverage tenfold (to $100,000) requires only an additional $100 in premiums, rather than a parallel increase to $3,000.

Under what conditions will your bond reimburse a loss? The companies that issue bonds are like any other insurer—they don't pay out simply because you ask them for money. Bonds have restrictions. Among the more important are reimbursements only for documented losses and the right not to pay for losses if an embezzler remains in a position of trust once a crime is suspected.

Both restrictions sound absurd until you realize exactly how disorganized and irrational organizations can be. For example, an appallingly large number of nonprofit organizations (including many libraries) have few or no financial records. With no records, it is not only very easy to embezzle money but also very difficult to prove money is actually missing. Similarly, many organizations are embarrassed to admit that embezzlement has occurred and are reluctant to take steps against anyone they suspect. As a result, embezzlement is very rarely reported as a crime, and embezzlers are even allowed to keep their jobs rather than risk the bad publicity of an arrest or dismissal.

Bonding Is a Good Idea, but It Isn't Enough

Most people, I suspect, balk at the idea of paying for insurance. After all, the industry is predicated on collecting money for events that usually don't happen. In some cases, the loss associated with an event is too small to be worth insuring. Recognize, however, that all organizations underwrite their losses one way or another, some through insurance, others by absorbing the losses out of operating funds. The key to cost-effective bonding, as with other kinds of insurance, is in recognizing which losses can be absorbed and which need to be insured.

Insurance is a wise idea because disasters happen despite our best precautions. Having said that, though, it's equally important to recognize that prevention is always easier in the long run than treatment. A bypass operation may keep your heart pumping, but it's probably better to avoid surgery altogether, if you can, by exercising and eating right. Similarly, bonding is an effective measure for protecting assets only when it is integrated into a larger program of financial control. A bond may reimburse embezzled money, but it is much better to avoid the crime entirely by hiring honest employees, maintaining a good record-keeping system, and having regular audits.

Proper Procedures

At the beginning of this chapter, we learned that internal controls are management's responsibility. It's time to revisit the topic because none of the internal controls we've discussed work unless managers are willing to make them work. An accountant can set up a purchase order/vouchering system for your library, but unless you insist that purchase orders be approved before purchases are made and unless you insist on proper documentation before you'll sign a check, the system is worthless.

The truth is, if you insist that your employees follow proper procedures, you are not always going to be everyone's best friend. It doesn't sound that hard until some Friday afternoon before a long weekend. The bookkeeper, whom you've known for ages and trust, presents you with the month's checks for signing. Some of them don't have complete documentation and you'll be tempted to sign them anyway because you don't want to make trouble and are rushed to leave for the beach. Don't do it. It's a slippery slope, and being liked by the bookkeeper isn't as important as protecting the library's assets.

The process doesn't need to be fractious and confrontational. If you're making changes in how things are done, warn the employees in advance and explain why the changes need to be made. (See chapter 4 for some useful change management strategies.) But stick to your guns. Once everyone understands you won't sign checks without proper documentation, they'll stop presenting them to you. On the other hand, you need to be prepared to put up with the inconvenience of your own controls. If you're a board member going on vacation, be prepared to make alternate arrangements for check signing rather than pre-signing a few blank checks.

Proper Authorization

Authorization in the Library Context

Everything that a library purchases should be properly authorized before the order is placed. Everything that a library pays for should be properly authorized for payment. This seems like straightforward common sense, until libraries actually start the purchase process. It's at about that point that most organizations wake up to the idea that properly authorizing purchases and payments is both inconvenient and time-consuming. Before I explain why this is both correct and desirable, let me spend a little time discussing what proper authorization means in practice.

The basis of proper authorization is that someone needs to be accountable for every purchase before it's made and for every payment for a purchase before it's paid. Further, the number of people who are held accountable, and by extension who have the power to authorize, should be limited. There are several reasons for this. The first is that it helps segregate execution (the authorization in this case) from other functions. This is, of course, assuming that the people to whom authorization is limited don't have responsibilities for accounting and asset custody. (See the earlier section on segregation of duties for a more complete discussion of why this is desirable.)

Second, preventing fraud isn't the only benefit from limiting the power to authorize; it also gives organizations better control over their assets. I once worked in an office where no one had the sole responsibility for ordering copier paper. Whenever supplies ran low (or more usually whenever we ran out), everyone in the office placed an order for copier paper. The result was a storeroom filled with paper. We spent more money on paper than we needed to and sometimes had cash flow problems because of the large unplanned purchase. Anyone who has had a joint checking account has probably had similar problems when the joint owners write checks without informing each other.

Finally, when authorizations are limited and when the people who have the power to authorize are held accountable for the money they spend, significantly more attention is paid to purchasing. The result is a better use of assets and fewer cost overruns. The need to hold managers responsible is key, because authority without accountability has very little power to produce careful oversight.

Vouchering and Authorization

The most common method of documenting proper authorization for a purchase is called *vouchering*. A voucher is simply a collection of the documents that are needed to determine that a purchase is legitimate and should be paid. It normally begins with a purchase order (PO), which lists the vendor, description, price, and quantity of the items being ordered and the signature of an employee authorized to make the purchase. In addition to the PO, there are documents attesting the order was received in the proper amounts (invoices, receiving reports, etc.) and a check for payment. In practice, the individual with check-signing power inspects the voucher to make sure all of the documentation is present and correct before signing the check. In the event the voucher is incomplete, the check signing is postponed until complete documentation is present. (See chapter 6 for a detailed description of the PO and vouchering process.)

Why Proper Authorizations Are Inconvenient and Why It Doesn't Matter

Everyone hates getting proper authorizations, and I suppose rightly so. Purchase orders make buying supplies more troublesome, and gathering the proper authorization for payment is time-consuming. You will hear these objections and many others if you try to insist on instituting a system of authorizations. They're all correct, but that isn't the point. Proper authorizations are supposed to make ordering and payment take longer—that's their purpose. People need to think about the consequences of spending money before they commit to doing it. They also need to be sure that what they're paying for was a legitimate expense before they release any funds to make a payment.

The counterargument I often use when I'm faced with these objections is this: if convenience is what you're concerned with, the best thing to do is convert all of the library's funds into $5 bills and keep them in a big box in the office. That way, anyone who needs to make payments can simply walk to the box and take out the cash. Nothing could be more convenient. Of course it's an absurd scenario, but without proper authorizations and controls the situation isn't much different. This isn't to say that the inconvenience shouldn't be taken into account. Jobs will take longer and be more difficult to learn, and managers will need to be aware of this. (See chapter 4 for change management strategies.) However, the gains in control over your assets are well worth the cost in time and effort.

Physical Security

It can be very easy in a high-tech environment to lose track of the fact that physical assets have value and need to be protected. I've often seen cases of offices with expensive firewall software installed on computers that were protected by doors with $10 locks. In addition to cash, libraries have a number of physical assets that are both expensive to replace and attractive to thieves. To make matters more complicated, libraries are in the business of making their assets (or at least some of them) available to the public.

The key to physical security is first understanding that you have something worth stealing. This is fairly obvious in the case of computers or rare books, but even mundane assets such as dictionary stands, chairs, tables, and atlases carry high price tags and are costly to replace if lost or stolen. In many cases, it isn't apparent that the assets have value or are at risk until they are gone.

One thing that isn't obvious about security is that weaknesses don't normally produce any symptoms. The first symptom of a weakness in physical security is usually that assets have gone missing. To check for security problems, the best method is to try regularly to defeat your own security measures. You can hire firms to do this for you, or you can use it as a staff exercise. (This makes a great topic for staff meetings if you are looking for something to get your employees engaged.)

A few words of caution if you do decide to try this at home. Choose a time and place where your patrons are unlikely to watch you. It isn't a good idea to expose security weaknesses to an audience. I mention this because I witnessed a similar training exercise in a shopping mall. A management training seminar was being held at a clothing store, and the trainer was demonstrating how a customer could defeat the security tagging system. Unfortunately, the training was conducted at 11:00 a.m. on a weekday and collected a crowd of shoppers as an audience. I can only assume that inventory shrinkage increased as a result.

Asset Inventory and Control

A good place to begin is a brief inventory of your assets. You may already have something like this for insurance purposes. Pay particular attention to high-value items such as rare books. If there are valuable assets such as first editions or Audubon prints, I usually advise libraries to consider whether they can provide a safe environment and whether such items are really appropriate to the library's mission. Imagine a situation in which a small library receives a Gutenberg Bible as a bequest. It's a wonderful item, but is it relevant to the needs of the library and the community? Consider the cost of insuring and protecting it, particularly in comparison to the proceeds from its sale. That's a bit exaggerated, of course, but only a little in light of the thefts of materials from libraries.

If you do decide to keep valuable materials, control access to them. Properly identify the persons to whom you grant access and be sure to check that the materials are still in place before you allow visitors to leave. On a more commonplace level, simply be aware that other assets are potential targets of theft. Even if someone is wearing overalls and carrying a clipboard, don't let the person walk out of the library with a table and chairs without making sure the removal is authorized.

Physical Cash Management

Let me begin this section by stating that we're concerned here with protecting cash as a physical asset. There are numerous methods for stealing cash from an organization without ever bothering with its physical existence (forged checks or fake invoices, for example). Most of the important frauds that deal with unauthorized payments will be dealt with in chapter 3, but for now we're simply interested in protecting cash as an object.

A consistent topic in discussions of fraud is the ease with which cash can change hands illegally, and how, once that happens, there's relatively little the original owner can do to get it back. A primary reason for the difficulty in claiming ownership of cash is that currency is what economists refer to as a *fungible* commodity. In essence, this means that any fungible item is perfectly substitutable for any other fungible item. For example, any $5 bill can be used interchangeably with any other bill of equal value. In contrast, your paint-by-number copy of the *Mona Lisa* is not interchangeable with the one painted by Leonardo da Vinci. This leads us to the sad fact that once currency gets into somebody's wallet, it becomes very difficult to prove that it wasn't there to begin with. Unless we plan to record the serial numbers on all of our currency, the only option we're left with is making sure that the money in question doesn't get into someone else's wallet.

Not so very long ago, the need to safeguard cash would probably have been a minor consideration in libraries. Libraries traditionally have had few sources of cash, such as fines and copier charges, but these have expanded to include user fees for items such as videotapes and sales from retail outlets run by the library (Denver Public Library's store, for example). On the surface, this still doesn't look like much money to worry about, and I can recall making a snide remark a few years ago along the lines of, "Oh, and what are people going to do, steal the fine money?"

It turned out the joke was on me. Fines have become a major source of funds in many libraries, and it isn't unusual for even small public libraries to take in $50 to $200 per day in fines. Nor are fines the only source of large amounts of cash. (Here's where the business about the difficulty of creating satire comes in.) As I was talking about sources of funds and theft, I mentioned that an enterprising thief might be tempted to steal money from a copier machine, but that the physical labor of carrying the coins around was probably more work than a real job. As it happens, one of my students worked in a large university that had recently experienced a series of copier machine thefts. The criminal was eventually apprehended, but not before he'd stolen more than $6,000 over several months.

It's fine to swap horror stories about losing money and, apart from entertainment, there's some value in the discussion. After all, the first principle in maintaining control of valuable assets is realizing that you have something to protect. But beyond that realization, there are two basic precautions your library should take to minimize the loss of cash: physical security and record keeping.

Keep in mind first that cash is a physical commodity and it needs physical protection. The place best suited to provide this is a bank, and that is where the vast majority of a library's funds should reside. Cash is necessary to make change for fines and the copy machines, and a petty cash fund is useful for making small purchases that are inconvenient to pay by check, but the majority of payments a library makes should be with a check or some other form of bank transfer.

In practice this means that cash needs to be deposited on a regular basis as soon as it exceeds some predetermined level necessary to run the library's daily operations. The level will vary by institution; however, a good rule of thumb is to keep the level at an amount that is sufficient to carry out daily operations but that will not cause a crisis if taken. (For example, all of us have seen the signs in convenience stores that say, "No more than $50 on premises.") Ensuring that deposits are made regularly is as much a matter of general management as of accounting. It's easy to allow too much cash to accumulate during busy periods when going to the bank may be less convenient, but these are precisely the times when a library is most vulnerable to theft. Library supervisors need to insist that the procedures for protecting cash are carried out, or there's no point in having them.

A second reason for depositing cash is that doing so creates a record of its existence in the library's financial records. This is not to say that a bank deposit should be the only, or even the first, record that cash has been received, but that generally we keep control of assets through the use of accurate financial records. The longer that cash sits without being recorded in the library's financial records, the greater the chance that it will be misappropriated or lost.

Cash officially exists in an organization when it appears in the general journal ledger (i.e., an entry is made in the organization's accounting records of the transaction that caused the cash to flow into the organization). The record may be created automatically (as in the case of a cash register or fine-management function of an automated circulation system) or through the entries a bookkeeper makes to record transactions. In either case, the quicker an entry is made, the less likely that the cash will be taken or lost without a trace. Record keeping won't necessarily prevent a loss, but it will alert you that something is missing and allow you to investigate and plug the leak.

All these procedures bring us back to managerial oversight as well as good accounting practice. No one necessarily expects library directors to become bookkeepers or to personally count the cash drawer and make individual bank deposits. However, it is a supervisor's job to make sure that the people who do perform these duties do so in a correct and timely fashion. (See the earlier section concerning proper procedures.) Cash registers make a fine beginning for keeping track of cash, but all of us have seen busy store personnel making change out of an open cash register without ringing up a sale. The same situation can occur with financial records. A good set of books doesn't help keep track of cash if no one bothers to make a record, and creating accurate records isn't much use if the cash itself isn't secure.

Independent Checks

Some General Comments concerning Independent Checks

First, let me point out that most of the independent checks that occur in an organization should be performed by members of the organization. In essence, every time you have a second pair of eyes look over another employee's work, you're performing an independent check. The key in making internal independent checks work, however, is in ensuring that the employees who do the checks are independent of the people whose work they're checking. In other words, good segregation of duties leads to good independent checks.

A similar rule holds for the administrative level of the person who performs independent checks. Normally, the person who's doing the checking should be at a higher level in the organization or at least answer to a different supervisor. It isn't an especially good control if a subordinate checks a supervisor's work because the lower-level employee may feel that he or she can't be fully candid about any irregularities. This will be particularly true in cases where a subordinate reports the errors directly to his or her supervisor.

This explanation probably sounds a bit disingenuous, since the independent checks that most of us think of involve an outside auditor. There's some truth to this, but before we go on to discuss audits as a control measure, I want to stress that auditors simply examine and verify what your library is doing. Independent checking needs to be done on a regular basis throughout the year, and it's the job of the library's management and employees to make sure that it happens.

Audits as Independent Checks

WHAT REALLY HAPPENS IN AN AUDIT?

From an audit perspective, the advantage of standardized practices is that they remove (or at least reduce) the need to examine all the individual transactions in an organization. If the standardized practices are correctly drafted, following them will produce accurate financial records. By extension, then, all that an auditor needs to do is ensure that the standards are being met, from which he or she can infer that the organization's financial records are accurate.

For example, rather than check each payroll entry to make sure it is accurate, the auditor need only examine the procedures that ensure accuracy in data entry and prevent tampering (e.g., time clocks, supervisor signatures on time sheets, password protection on payroll systems, etc.). The audit may require an examination of a small number of transactions to test the system, but this is a far cry from completely reworking an entire year's payroll.

The principles and theories that help maintain uniformity in reporting systems are referred to as *generally accepted accounting principles*, or GAAP, in the United States. (Other countries have similar sources of governing standards.) As with any set of rules, GAAP is far from foolproof, but it continues to be refined through experience and provides a reasonable starting point for creating useful and reliable financial records.

"This is all well and good," I hear you say, "but why should I welcome the auditor into my library?" The answer goes back to the basic reasons for having financial records: to maintain better control over our financial resources and, by extension, better management of the library. Accounting standards are subject to a number of criticisms, but generally, the better we follow them, the better our records; the better our records, the better our management. The problem in any organization, however, is that actual practices frequently deviate from standards. Normally, the deviation isn't intentional (although in many cases it can be the result of inattention), but the result is still a set of financial records that are less useful for making good managerial decisions.

A good audit alerts library management to areas that need improvement. Libraries have become big business, and in many cases their financial control systems haven't kept pace. A good auditor will show you where you're vulnerable. In fact, a more useful way of thinking about the audit is not in terms of finding mistakes in library practice but in communicating best practices to the library. The common element on which all of my colleagues who have been audited agree is that the library runs better after an audit. In the end, the library gains better policies and better control over its assets.

There are also immediate, concrete advantages to having regular audits. Chief among these is that many funding agencies in the federal government, as well as many private charities such as United Way, will not release money to organizations that are not audited. If your library has any interest in applying for grants, audited financial statements may be a requirement.

HOW DO I FIND AN AUDITOR?

"Okay," you say, "you've convinced me. How do I find someone to visit my library and perform one of these miraculous operations?" In theory, any good accounting firm should be able to perform an audit for you. Having said that, however, let me point out that nonprofit audits are a bit specialized (particularly if federal money is involved) and as a result, some accounting firms may be unwilling to perform them. A good source of guidance in this regard is your local United Way headquarters. United Way is a great promoter of nonprofit audits, and the local office usually has a referral list of accounting agencies. Other good sources are referrals from library colleagues who have regular audits.

The regular audits that are performed by state agencies probably aren't performed frequently enough or in enough depth to be particularly helpful. Many states conduct audits only about every two to four years, which is a very long time to have mistakes go uncorrected. (It is also possible to steal a very large quantity of money over three years, even in a library.) Similarly, state audits are often more concerned with making sure the library uses state money for purposes specified by regulation rather than whether it maintains useful financial records. (This is not a criticism of state audit agencies, but simply an acknowledgment that their interests may differ from the library's.)

A final cautionary note about audits: they are not cheap. A library can easily spend $2,000–5,000 (or more) for an annual audit. Firms vary widely in their costs, however, and it is often worthwhile to solicit prices from a variety of firms or negotiate bids or both. Many accounting firms engage nonprofit clients at a reduced rate as a policy of goodwill to their communities, so it may also be useful to ask about special rates for nonprofits at accounting firms or with your local United Way.

WHAT STRATEGIES WILL HELP ME SURVIVE AN AUDIT?

1. Talk to other librarians who have been through audits. See what your colleagues have experienced. You'll be better prepared for the experience with a little foreknowledge, and you can see the positive results of audits at other libraries. (Believe it or not, in my experience, nobody has anything bad to say about the results of their audits, at least after the audits are over.)
2. Understand that the auditor is not out to get you. I can attest to this personally. When I originally trained as an accountant, my auditing professor drilled into the class that the firms we audited were our clients and that our job was to help them perform better,

not to catch them in mistakes. (This won't be the case in a forensic audit, but if you do things properly now, you won't need to worry about financial misconduct occurring.) I'm glad to say that the auditors my colleagues dealt with must have gone to similar schools. Everyone I spoke with agreed that the accountants who examined their books were uniformly helpful and seemed genuinely interested in helping the library run better.

3. Ask questions. Don't be passive. Ask what's going on and why things are being done. An audit should be a learning experience for the library. Find out what the accounting practices are trying to accomplish and ways to improve your financial record keeping. If there are recommendations in the audit report that you don't understand, ask for an explanation. This doesn't need to be confrontational, and a good auditor should be willing to help you understand and implement his or her recommendations. (In fact, this isn't a bad practice with any professionals you hire. Ask them to explain what they're doing and what their recommendations mean. If they're not willing to explain, find someone who will. Keep in mind that you may not have the expertise of an accountant, an attorney, an architect, and the like, but you do know more about how your organization runs than they do.)

Remember, the reason we have financial records is to run the library better. Anything we can do to improve financial control means better programs.

3

Common Weaknesses in Your Library's Internal Control System: How to Recognize and Correct Them

Nobody thinks you're a criminal. Let me rephrase that—probably nobody thinks you're a criminal. You may, in fact, be a criminal, so I don't want to issue a blanket amnesty to everyone who works in a library. Why am I beginning a chapter this way? It's because the chapter deals with situations in which some member of the library community (e.g., board member, director, bookkeeper) has too much (or sometimes too little) authority. As soon as we begin talking about changing job duties or redistributing power, people become defensive. The purpose of this chapter is not to throw suspicion on a library employee, but rather to understand the organizational weaknesses that can foster a higher risk of fraud. In some respects, this is just an extension of the issues that were raised in chapters 1 and 2. The only difference is that here we will examine the specific internal control weaknesses that are common in libraries and use the framework of internal control to remedy them.

WHAT ARE SOME COMMON AREAS OF WEAKNESS?

If libraries have control weaknesses, they're commonly found in one of four areas: the financial control system itself (or lack thereof), the range of job duties for the bookkeeper, the extent of the director's authority, and the degree to which the board is involved. Let's examine each of these in greater detail.

There's a Bad Financial Control System or None at All

Everything that we discuss in this book is predicated on having a functioning set of financial records. *Functioning* in this case can be defined as financial statements that are both accurate and timely. The library's transactions are entered within a reasonable period after they occur and are entered correctly. Unfortunately, many libraries have little or no financial control other than their checkbook. They share this characteristic with many other businesses, but as we've seen, the magnitude of library budgets makes this a significant risk.

Library management and the board should jointly undertake the task of ensuring that the library has adequate financial records. Both groups will be using the records, and having two sets of eyes oversee their creation helps ensure high quality. In addition to creating the system, both groups need to ensure that it's used correctly. Often, good systems are created but become ineffective due to lax management and oversight.

The Bookkeeper (or Someone Else) Has Too Many Interlocking Job Duties

In most libraries, the bookkeeper has the primary responsibility for handling financial matters. The bookkeeper may, in fact, have the only responsibility. As such, it's important to make sure that this person doesn't acquire too many interlocking duties. As we discussed in chapter 2, the same person shouldn't be responsible for authorizing purchases, certifying them, and authorizing payment. The problem in many libraries is that the bookkeeper has grown into the position. She or he, and certainly other library managers, may not even be aware of the situation or realize that it's a potential risk. The problem may be further complicated because no one in the library generally pays enough attention to its finances.

Often, simply examining the bookkeeper's job duties is enough to discover the interlocking jobs. A complete segregation of duties may be beyond the capabilities of some smaller libraries, but job rotation and increased oversight by the board and the director can usually compensate.

The Director Has Too Much Power

In chapter 1, we noted that financial control in libraries is often in the hands of a single individual, usually the director, who isn't subject to standard financial controls found in for-profit companies. Library directors hold an unusual position that they share with other nonprofit directors.

They act as sole proprietors in organizations that they don't actually own. This can have significant implications for internal controls.

In many small firms, the owner (sole proprietor) oversees every aspect of the business. This can include ordering inventory, approving payments, and writing checks. There is significant efficiency in carrying out business this way, particularly in businesses with only a few employees. The downside to this efficiency is that, in theory, it violates the classic segregation of duties that we discussed in chapter 2. However, sole proprietors compensate for the lack of segregation because they don't operate against their own interests. In other words, they don't defraud the firm because it's in their own interest to keep it successful. They act as their own internal control.

The problem that many nonprofits face is that they look like sole proprietorships but aren't. There may be entirely creditable reasons for the resemblance: the director is the only professional or full-time employee or both in some libraries, the library has developed and grown as the result of the director's vision and entrepreneurial spirit, or there simply wasn't anyone else interested in doing the work. Whatever the reason, it isn't in the best interest of good internal control to allow the director to have too many interlocking duties. At a minimum, it's usually a good idea not to allow check-signing authority to reside with the director; it's more appropriate for the board to sign checks based on supporting evidence from the library. That doesn't prevent more elaborate frauds from occurring, but if the board is doing its job, fraud becomes much more difficult.

Ideally, the same segregation of duties used for the accounting, custody, and execution of transactions should be maintained in constructing the director's job duties. Many directors don't perform all the financial management in a library. The job is more commonly performed by a bookkeeper or financial manager, so the specific segregation is more usefully applied to directors' job duties. It is useful to watch more closely in cases of management overrides of internal controls. The best internal controls become useless if upper management can render them inoperable.

The Board Isn't Doing Its Job

Many nonprofit organizations, including public libraries, divide the responsibilities of management between an executive officer and a board of directors. The exact division of responsibility varies considerably among organizations, but in financial matters the board of directors is typically responsible for raising funds and approving expenditures. In practice, this usually means that the director or another employee under his or her direction writes checks for expenses then passes them on to the board for review, approval, and, ultimately, signing.

In most organizations with boards of directors, several board members have check-signing powers. In fact, in most cases, two or more signatures are needed for the check. Usually, the signing members are presented with a pile of checks that require their signatures. In theory, each check should have accompanying documentation (e.g., signed purchase orders, invoices, receipts) that indicates it was a legitimate, approved expense. The signator(s) should then review each individual item to make sure the documentation is in order before signing the check. If the information is insufficient, the signators do not sign and instead request better documentation. That's the theory, but here's what often happens. Someone places a huge pile of checks in front of the board member, who signs them without actually looking at the amounts, documentation, or recipients of the checks. Worse, the board member may actually pre-sign blank checks for the convenience of the office staff. It doesn't take much thought to realize that if this is the extent of oversight, then embezzling money becomes appallingly easy, and that's essentially what happens in many cases of library embezzlement.

How do board members help embezzlement to occur? Unfortunately, many of the worst lapses in oversight arise out of a genuine desire for cooperation between boards and administrators, or at least a misunderstanding of the duties of board members. Many library boards regularly abdicate their responsibilities for exercising financial control by presigning checks or by approving payments for expenses without reviewing the supporting documentation. In some cases, the lapse of responsibility may be the result of negligence or inattention on the part of board members. More often, board members are ignorant concerning their duties or the risks involved with approving expenses without reviewing the documentation. All the board members interviewed in the study stated that they did not understand that embezzlement could have happened, that they had the ability to prevent or reduce its occurrence, and that they would have been more vigilant had they understood the process better (Snyder and Hersberger 1997).

As we noted in chapter 1, the consistency of this response may reflect the need of some board members to excuse their role in embezzlement. But it is consistent with the finding that most board members have no professional training or experience with finance prior to their appointment, nor is there any evidence that financial expertise is considered a necessary or desirable skill for a board member. In addition, library board members usually receive little or no training concerning their financial responsibilities.

Even if trustees are interested in matters of financial control, there is often little guidance available to them. The standard reference and training materials for trustees such as the ALA Trustee Association monographs deal mainly with budgetary and fund-raising duties and condense financial control into a single paragraph.

A second, related problem is that board members often simply do not consider the possibility of financial misconduct by a library director or another board member. As one board member put it, “We trusted the director or we wouldn’t have hired her in the first place. Besides, what do I know about accounting?” Another observed, “Who do you think trains board members in their duties? The librarian they’re supervising.”

WHAT ELSE CAN WE DO TO CORRECT WEAKNESSES IN INTERNAL CONTROL?

Don’t Point Fingers

The key to any effective strategy for protecting library assets lies first in the awareness by both the library staff and the board that a risk might exist. This shouldn’t be a matter of suspicion and placing blame, but rather an effort to work together to make the library run better. This, in particular, is at least as much a managerial concern as one of financial control. Many plans for improved oversight fail because employees or the director feel that the board suspects them of misconduct. Conversely, board members may feel they’re under attack for incompetence or inattention. Neither situation helps the library, so try to examine your procedures in the context of improving the library rather than criticizing individual behavior. Chapter 4 of this book is devoted exclusively to change management and fraud prevention.

Educate Your Board Members and Your Staff

A variety of materials are available to educate board members and nonprofit administrators and to help your board work more effectively. Among the best (in my opinion) are those produced by BoardSource (formerly the National Center for Nonprofit Boards [NCNB 2005]). Its publications are brief and reasonably priced, and they make good additions to your professional library.

In an ideal world, every library board would include an accountant and an attorney. In reality, it may not be practical to find people with this much expertise who are willing to serve. Remember, however, that the aim is to make board members better aware of their responsibilities rather than turn them into auditors. Most of the oversight is a matter of common sense. What exactly are we paying for? Do the amounts seem too large? Are they going to places that seem unusual? My experience with boards has been that most people who sign checks don't realize that they should also be reviewing the documentation. Once someone tells them this, it makes complete sense to them and they have no trouble exercising oversight.

Keep in mind that libraries and other nonprofits may eventually have no choice in the matter. The Sarbanes-Oxley Act of 2002 deals with some of the lapses in corporate governance that took place at Enron and other corporations. Among other rules, it mandates that at least one member of the board for publicly traded companies be knowledgeable in accounting. The law doesn't apply to nonprofits, but increasingly it's being seen as the template for all organizational governance, even in the nonprofit world.

Examine Employee Job Duties Periodically

Employees and their jobs change over time. Corresponding internal controls will also need to change if they are to remain effective. Many of the most successful frauds in libraries have been carried out because no one in management thought to examine what employees really did, as opposed to what the job descriptions said.

Remember, the most common duties that need to be separated are the following:

- Opening mail and sorting bills
- Writing purchase orders and approving purchase orders
- Approving invoices and writing checks
- Writing checks

Take the time to walk through an employee's job and see how many of these duties fall under the control of the same individual.

Cultivate Some Distance

Boards and directors often get along so well and trust each other so much that they don't follow proper procedures. Need a few blank checks to take care of purchases Monday morning? No problem, we trust you. The purchase order isn't attached? I don't want to cause you bother, so I'll just sign off this time. The real difficulty here is that our natural inclination to be friends sometimes interferes with good business practices. Keep in mind, however, that if the board and the director both do their jobs competently, there will be friction at times. For example, asking the commonsense questions that I mentioned earlier may require more work from the library staff to provide better documentation.

Effective oversight, however, means work and responsibility from both the board and the library staff. Board members need to have the courage to insist on proper documentation, but they must also be prepared to do the extra work to review what they've asked for. This may mean a longer review time or an extra trip to sign checks that weren't documented properly the first time. Conversely, library staff members need to insist that board members take the additional time to review the checks they're signing and be willing to do the extra work needed to properly document expenses.

All of this may sound onerous, and it's possible it may be for the first few times. But my experience has been that once both parties get used to the idea of proper documentation, it becomes the norm and requires relatively little extra work. Board members understand their responsibilities and take the time to perform them, and library staff members aren't left with unsigned checks because none are presented for signing without proper documentation. In the end the library (or any other organization) has better-managed assets and obtains better service value for its money, which is why you're all there in the first place.

~4~

Change Management and Fraud Prevention: Allowing the Improvements You Make to Work

Madisonville Public Library (MPL) had just won over the voters in its county. (MPL is an actual library. The name and some of the details have been changed.) After years of shrinking budgets and a deteriorating building, MPL was about to receive $12 million over the next twenty-four months. Even more exciting was the chance to leverage this tax windfall into another $4–5 million in matching grants. The only problem was that the library was missing $600,000. An unscrupulous bookkeeper with too much responsibility had simply stolen it all. The scams were simple—multiple or inflated salary checks, payment of personal expenses with library funds, and payment of phantom invoices from a shell company owned by her boyfriend. Moreover, the signs of fraud were there for anyone to see. She drove an expensive Lexus, had an extensive wardrobe, and had recently undergone cosmetic surgery that wasn't covered by her medical plan. How did she manage this in a library that had successfully negotiated an increase in funding and was flourishing? The answer, ironically, is that the library was a victim of its own success. It had simply outgrown its control mechanisms.

HOW GOOD LIBRARIES CAN GO BAD

The case of MPL is not unique in the world of fraud prevention, nor, unfortunately, is it even uncommon. What happened with MPL is the combination of two separate but related problems: a library that had grown too large for its internal controls and a director who was unwilling to delegate sufficient authority to institute better controls. The real difficulty that antifraud professionals face in libraries like MPL is not in designing or implementing financial controls, but in convincing the director to make the necessary investment and to give up sufficient authority to allow the controls to work.

All libraries hope for growth and success, but few of them actually seem to expect it to happen. A less obvious consequence of this situation is that most directors and boards don't follow the managerial steps necessary to keep the library running as it grows and becomes more successful. As a result, small libraries can become too unwieldy to manage and often fail just at the point where they seem poised to take off. In the case of MPL, the director had spread himself too thin. Where he once personally approved every purchase order and payment check, his hectic fund-raising schedule and hands-on management style now kept him on the road four days every week. When his bookkeeper offered to take up the slack, it seemed like a gift from heaven. Unfortunately, the same director's oversight no longer applied, and the bookkeeper was able to take advantage of this weakness to loot the library treasury.

This problem is particularly acute with directors who are used to having complete control of their operations. MPL was undermined by embezzlement, but dishonesty is not necessary to destroy an organization; in many cases, the inability to act is sufficient. Many libraries fail simply because the director neglects to give employees enough authority to run the organization. If the director of MPL hadn't given his bookkeeper the power to approve purchases or pay bills, operations might have ground to a halt as the result of outstanding bills or insufficient purchases or both. All libraries, if they continue to grow, will expand beyond the point where a single individual can keep track of all the necessary operations.

Fortunately, the specific changes in internal control that a library like MPL should adopt are relatively straightforward: segregation of duties, independent checks of the financial records, vouchering for all checks, and so forth. Indeed MPL already had many of these in place but was unable to take advantage of them because it didn't follow its own procedures.

MORE THAN INTERNAL CONTROLS: GETTING DIRECTORS TO CHANGE

The issue in cases like MPL is as much one of change in management style and strategy as of accounting. In the quest to design better antifraud protections, we often lose sight of the fact that good ideas don't necessarily sell themselves. A major consideration in fraud prevention is convincing library directors not only that they need better protection for fraud but also that they need to change the way they manage in order for these protections to work. What follows is a series of change management issues to discuss with boards, library directors, and employees to help them understand and adopt better financial controls.

Even Though You're Small, You're Still at Risk

Good fraud prevention plans begin with the understanding that an organization may be at risk. However, many library directors have difficulty believing they are at risk for fraud. "We're too small for anyone to bother" and "I trust everyone here; they've been with me for years" are among the common objections directors state. A good place to begin the process of developing better internal controls is to educate directors and board members about why they may be at risk.

There are at least four reasons why small libraries in particular are especially at risk for fraud. First, the very size of the organization limits its ability to separate functions related to the authorization, record keeping, and physical safeguarding of assets. Without this segregation of duties, internal control functions are weakened or susceptible to circumvention. In very small libraries, these weaknesses are mitigated through the director's personal oversight. However, as the library grows, the director is less able to review every transaction, and the opportunity to commit fraud is increased. Conversely, the personal oversight of a director is not a guarantee that fraud is effectively deterred or detected.

Second, smaller organizations tend to disregard or subordinate the importance of periodic accounting functions such as account reconciliations and analyses. In other cases, the preparation of the financial statements is outsourced. Therefore, the individual transactions are never scrutinized by anyone within the organization who knows whether they are correct.

Third, the director and employees may not have adequate fraud awareness. That is, they may not realize the areas in which the library is vulnerable to the risk of fraud and therefore do not take the appropriate measures to prevent it. Along these same lines, it is very common for the management of smaller libraries to believe that the close relationships that exist among a smaller group of people prevent fraud from being committed. In reality these feelings of absolute trust may create an environment of perceived opportunity to commit acts of fraud.

Finally, even the personal oversight of a director is not a guarantee that fraud will not occur. As we have seen earlier, the compensating measures that a director's oversight provides do not protect the library from fraud committed by the director or board members.

Your Mission Does Not Protect You

This might be termed the law of sympathetic magic and is often shared by organizations with a charitable purpose. Basically the argument runs, "Who would steal from God, starving children, or libraries?" Unfortunately, as countless case histories have demonstrated, fraudsters are able to rationalize even the most heinous financial crimes. As with size, the real difficulty is simply getting libraries to acknowledge that they are at risk and that their public service is an insufficient protection against fraud.

You Can't Do Everything Yourself

This is probably the most difficult aspect of change management with library directors. Directors often become successful as the result of their attention to detail and hard work, so it seems counterintuitive to argue that these same qualities are now getting in the way of that success.

A good approach in many cases is to discuss the director's time as a commodity that produces benefits for the library. The issue then becomes how to invest this commodity for the good of the organization. That is, the director may be good at many aspects of library management, but not all of them are equally valuable to the library. Thus, although he or she may be a good bookkeeper, the time spent doing this work doesn't generate funding for the library. A good internal control system allows the director to spend more time in the areas that help the library to grow, without losing control over the important aspects of its finances. This leads logically to the next point.

Internal Controls Are an Investment in Your Library

All managers tend to believe that financial controls are an unfortunate expense like insurance. As with insurance, people are reluctant to pay for items for which they see no immediate benefit. One way to deal with this is to put internal controls in the context of an investment in the library.

The most valuable commodity a director has is his or her time. As we just discussed, a director's time ought to be spent in those activities that generate the most benefit. Therefore, good financial controls aren't just an expense; they're actually an investment that allows the library to become more successful by freeing a director's time to do those things that provide the greatest benefit to the organization.

Similarly, it isn't enough simply to bring in more resources; they have to be protected once they enter the library. As the value of assets increases, the measures to safeguard them also need to improve. Most library directors understand this concept in the context of physical assets. Once the connection is made with financial assets, directors usually grasp that good financial controls are an investment in protection in the same way that a burglar alarm or better locks would be for valuable collections or office equipment.

Better Internal Controls Don't Mean You Don't Trust Your Employees

Internal controls are matters of good management. Establishing and maintaining an honest workforce is a good beginning for internal control, but relying solely on employee honesty is poor management. Internal control involves more than financial misconduct. Control of organizational assets also means that the assets are used effectively. Honesty by itself does not ensure accuracy.

You Have to Sell the Employees as Well as the Director

A general principle of change management is that support from top management is necessary but not sufficient for effective change. Even if the library director is convinced that better financial controls are needed, it is still necessary to gain the support of the company's employees. In fact, a director's reluctance to alienate longtime employees is often an impediment to improving internal controls.

Feelings of distrust, that somehow the director suspects them of misconduct, may be common among employees when organizations attempt to institute financial controls where historically none have existed. Similarly, employees may view internal control procedures as an additional workload and resist adopting them. The following steps can ease the transition to better controls and help ensure that the employees will become willing partners with the directors in change:

1. Make the same case for the employees that was made for the director. Inform them from the beginning that the measures that are being instituted are for better management, not because of doubts about their honesty. Solicit their input on changes. Employees

often have a better idea than management concerning shortcomings in internal control. Employee input not only gives management better information concerning internal control, it helps ensure adoption of any changes by making the employees part of the process.

2. Give employees time to learn their new tasks. This is a basic step in implementing any new system. It is often overlooked, however, when management modifies a job that employees have done in one way for a long time. Former ways of performing tasks interfere with the new system and may require a period of adjustment.
3. Allow for tasks to take longer or require more work. Many jobs such as ordering and paying for purchases with a purchase order will be less convenient and take longer.

EPILOGUE: MPL SURVIVES AND BECOMES EVEN MORE SUCCESSFUL

MPL's director and board did save the library and it is flourishing again. The bookkeeper was convicted of fraud, served a period in jail, and was required by the courts to make restitution. She now lives in another state and is making monthly payments.

In the course of salvaging the library, the board brought in an accountant who revamped the accounting system and divided the tasks among several employees. MPL managed to save most of the funding it received, but as the director noted, "The loss of public trust will take years to recover. We aren't likely to win another tax increase after what happened. I should have done this years ago, but I just didn't understand. I finally learned how to delegate, but the loss of the money and our standing in the community was a pretty high price for that lesson."

The failure of a library is a high price and one that directors, boards, and employees should try to avoid paying. Part of any fraud prevention program should be educating the library personnel about the need for change as well as making the changes. By the time they learn the lesson themselves, it may be too late to help.

5

Specific Types of Fraud: Understanding, Detecting, and Preventing Them

Librarians love classification systems, so it's probably a good idea to begin a discussion of common types of financial misconduct by setting out a classification scheme for fraud. The most common scheme is one devised by Joseph Wells in *Principles of Fraud Examination* (2005). Generally, we can divide fraud into three broad categories: corruption, financial statement fraud, and the misappropriation of assets.

Corruption is the misuse of an official position to provide gain to the person who holds the position. Misuse in this context involves gain at the expense of the organization. A director, for example, receives a bribe from a vendor and subsequently makes purchases for the library even if that vendor doesn't have the best price for the purchases. Wells identifies four categories of corruption: bribery, illegal gratuities, extortion, and conflicts of interest. Although corruption tends to be rare in library settings, it does occur, and we'll return briefly to some specific symptoms and preventions later in this chapter.

Financial statement fraud is usually committed by upper management and is usually committed to defraud investors and creditors. The sorts of financial shenanigans we saw perpetrated by Enron and WorldCom are typical of this type of fraud. Although it's possible that someone committing fraud in a library might try to manipulate the financial records to hide the crime, financial statement fraud really isn't a major concern of libraries. So instead, let's push on and examine asset misappropriation in greater detail.

In layman's terms, *asset misappropriation* means stealing things. The methods for doing this may be more or less sophisticated, but basically asset misappropriation falls into two broad categories: thefts of cash and thefts of other types of assets. Cash misappropriation accounts for about 80 to 90 percent of all financial misconduct (Association of Certified Fraud Examiners 2004). This isn't a very surprising statistic given the ease with which cash can be taken and used. (Cash in this instance means both currency itself and cash surrogates such as checks.)

Although the outright theft of cash is a major component of cash misappropriation, it isn't the only type or even the most damaging. Cash thefts are limited to whatever cash is physically on hand in the library. However, many techniques for misappropriating cash never use cash per se. Organizations can be defrauded by having them pay for purchases they never received, hours that were never worked, trips that were never made, or checks that were never properly written. Specifically, these frauds concern billing, payroll, expense reimbursement, and check tampering. All of them involve the misappropriation of cash in some way, and we'll examine them in detail in the following sections of this chapter.

In each of the following sections, we'll look at examples of specific frauds, examine how they occur, and discuss strategies for detecting and deterring them. There are no types of fraud that aren't deterred by better segregation of duties, so all the sections include advice on the segregation of duties as well as other measures. All the examples are taken from real cases. Unless stated otherwise in the example, however, the names and details of the case have been altered to protect the privacy of the source.

STEALING CASH

As we've discussed earlier in this book, nothing is easier to steal than cash. Nothing seems to bring out the ingenuity of fraudsters like cash does either. The only thing more amazing than the variety of scams used by library fraudsters is the amount they are able to steal by using them. To show the range of schemes, here are some examples from actual libraries.

The Case of the Missing $20s

In 1999 an account clerk in the Burlingame, California, library system pleaded guilty to stealing almost $130,000. For more than twenty years, the employee had the task of counting and transferring the library's overdue fines and other receipts to the city's finance department. During the course of these duties, she appeared to pocket every $20 bill in the library's cash register. Indeed, when the library and city finally performed an independent reconciliation and audit of the library's deposits, they discovered that no $20 bill had been included in a library deposit (Squatriglia and Lynem 1999).

Apparently, the employee was able to get away with the thefts for so long because her job duties included reconciling the cash register tape, deposits, and cash on hand. The library installed a cash management module as part of its computerized circulation system, but it apparently did little good because no one except the perpetrator ever bothered to check whether the cash register tapes matched the daily bank deposits. The fraud was eventually detected only when a colleague noticed an envelope filled with twenties in the culprit's desk while she was away on vacation. After over a year of investigation, police and library officials were still left with two questions: Where had the money gone? and How did a clerk manage to steal so much from a library that served a community with fewer than 30,000 people?

Subsequent to the thefts, the library tightened its oversight of cash. Cash counts are now performed by two employees, and more frequent reconciliations between the cash register and bank deposits are made.

The Thief Who Got Away

The Fort Worth, Texas, public library was found to be over $70,000 short in a 2004 audit. The only problem was that administrators couldn't be completely sure who took it. Police believed that they had narrowed the suspects down to two but were unable to prove the case because of the library's internal controls. The library used couriers to move funds from the system's branches to the main library. Couriers had been observed transporting the money in unlocked containers and even putting it in their pockets. Worse, a safe in which the funds were stored was frequently left unlocked during the day and accessible to a variety of unauthorized people such as the cleaning crew (Rogers 2004).

The Secretary Who Helped Herself to the Bank Deposits

The secretary of the Floral Park, New York, public library was arrested for stealing $77,000 over an eight-year period. Among her duties was keeping the financial records and making the bank deposits for the library's sale and rental of videos. The funds were collected centrally and later divided among a number of envelopes for deposit in the library's several bank accounts. The secretary apparently took some of the money from the envelopes and entered both the original amounts and the lesser amounts into a cash receipts ledger. A subsequent independent audit uncovered the discrepancy, and the secretary eventually paid over $89,000 in restitution (*New York Times* 2003).

And so on . . .

How Thefts of Cash Occur

The seemingly trivial and obvious answer to the question of how thefts of cash occur is that cash thefts occur when cash is taken. This really means that cash can be taken anytime it's physically available in the library. There was probably a time when having cash on hand wouldn't have been a major consideration. Libraries have traditionally been free and, unlike retail establishments, didn't collect fees for the use of their materials. Sometime during the last twenty years or so, this situation changed. Libraries are still free, but increasingly they are required to assess charges. These may be in the form of overdue fines, which as one of the preceding examples demonstrated are a large source of funds in many libraries, or charges for services, as in the case of the video rentals. In any case, the sums taken in by many libraries are now significant and, at least as important, are largely in the form of cash.

As the cash enters the library, a potential thief faces two choices: take the money before it's recorded in the library's financial records or wait until after it's entered into the records. These two types of theft are known, respectively, as skimming and cash larceny. Although the thefts can occur anywhere that cash exists, the likelihood of skimming is greatest at the point where cash is entering the system and hence hasn't yet become part of the financial record system.

Skimming

Skimming is the theft of cash before it enters the accounting system. Because there isn't a record of the cash before it's stolen, skimming is rarely uncovered as the result of routine audits. Obviously, the longer cash sits around before being recorded, the more likely it is that a skimming fraud will occur. The best way to prevent skimming frauds is to make sure that cash is entered into the accounting system as soon as it comes into the library.

Skimming can be accomplished as easily as pocketing cash as it comes in without recording the receipt. Often, however, the fraudster is required to make a show of entering the cash. This is especially true when a cash register is used, and fraudsters employ a number of schemes to skim cash while using a register, including making false sales.

FALSE SALES

Fraudsters can simulate the use of a cash register by ringing up a no-sale or otherwise opening the register without recording a receipt. The fraudster collects the money and makes any change needed without recording a sale. The method has the disadvantage of not producing a sales receipt for the customer, but customers frequently don't notice without being prompted. (Reversing a sale through a false void also allows the theft of cash, but this is more correctly a cash larceny because it involves a theft after a record exists for the receipt of cash.)

SKIMMING THAT DOESN'T INVOLVE CASH

Libraries receive a number of payments in the form of checks. These can be payments from patrons or remittances for regular revenues such as grant funds. Employees who are tasked with entering these remittances, particularly those employees who open the incoming mail, are in a position to take the checks before anyone else in the library notices they've arrived and convert them to their own use. The conversion is more difficult with checks than with cash because the check is made out to someone other than the thief, but there are several ways to convert checks.

Forgery and *check tampering* are the traditional means of converting stolen checks. Later sections of this chapter discuss check tampering in detail; however, the use of credit cards has made the conversion of stolen checks an easier process. A fraud I worked on recently involved the theft of checks from the residents of a nursing home. (Nursing homes are wonderful places to commit thefts. Many of the residents have no one who looks after their interests closely, and they're usually not in a position to look after themselves.) The thief in this case opened a number of credit card accounts and overpaid them by enclosing the stolen checks with the monthly bills.

As it happens, most credit card companies process their payments automatically. No one ever looks at the checks to see if the credit card is the legitimate payee. By making a number of overpayments, the fraudster built up credit balances in her card accounts, effectively cashing the stolen checks without actually forging any signatures. She was eventually discovered when a relative followed up on a missing payment, but not before the scheme had continued for over a year.

Cash Larceny

Larceny is the misappropriation of assets without violence. In this case, *cash larceny* is defined as the theft of cash after it has been entered in the library's financial records. Whereas skimming is more likely to occur as cash enters the library, cash larceny can occur at any point where the thief has access to cash. Cash larcenies are easier to detect than skimming because a paper trail exists in the accounting system. Most successful cash larcenies occur, however, because no one ever bothers to review the records or because the records are in disarray. Among the more common methods used in cash larcenies are false voids and refunds, stealing from other registers, shorting deposits, and destroying records.

FALSE VOIDS AND REFUNDS

Anyone who uses a cash register invariably makes mistakes. Most registers have a mechanism for voiding out and reversing transactions. This feature can be used to void out legitimate transactions, after which the fraudster collects the cash and still produces a transaction record that balances with the cash drawer. If the library has goods and services that are suitable for refunds (sales of books, for example), the same system can be employed to indicate a refund has been made for a legitimate sale.

STEALING FROM OTHER REGISTERS

A simple way to steal cash when records are kept is to take it from another employee's register. Under the worst circumstances, employers don't assign employees to specific registers; either all employees use the same register or any employee can use any register. If an employee removes cash from a register, it may be possible to tell that the cash is missing but not who took it. Thus, there's no deterrence in keeping records of transactions. Even though the register tape may help identify a loss, it cannot identify who caused it.

Assigning employees specific registers or login passwords or both can help control cash larcenies, but only when the logins are unique and are kept confidential. Too often, employees and managers are careless with sharing their passwords or even leave the registers open.

SHORTING DEPOSITS

As cash enters or leaves the library, there is a period where it's under less physical control than when it's locked up or in the bank and thus easier to steal. Deposits in transit are one instance of this. Typically, the fraudster waits until the deposit is ready to be taken to the bank, removes some or all of the deposit, and rewrites or destroys the deposit slip. The shortage can be discovered when the bank statement fails to coincide with the library's cash records, but only if someone in the library takes the time to reconcile the records.

DESTROYING RECORDS

Destroying records is probably the least elegant technique for carrying out cash larcenies, but there's no denying that it's effective in many libraries. If there are no records of the cash receipts or transactions, then proving larceny is very difficult. The loss of such records should be an immediate red flag for fraud and possibly the grounds for dismissing the employee who destroyed the records. Unfortunately, many libraries have such poor record keeping that the destruction goes unnoticed or without consequences.

Detecting and Preventing Cash Thefts

Segregate Duties

There are three basic functions in collecting and recording cash that if separated will make stealing funds significantly more difficult to carry out or to hide if it is carried out:

- Recording the initial collection (usually with a cash register)
- Depositing the cash
- Reconciling the register and deposits

Separating these functions won't deter every instance of cash theft; by themselves they aren't particularly useful for unearthing skimming, for example. However, done together they will make it unlikely that you'll fail to uncover the types of fraud illustrated by our examples from Floral Park and Fort Worth.

SEGREGATING CASH COLLECTION—AN ILLUSTRATION

The flowchart in figure 5.1 shows one possible system for segregating cash-handling duties. This system isn't the only way to segregate cash handling, but it isn't a bad way either.

Step 1: Cash collection begins in a *branch library*. Incoming money is collected and each transaction is entered into a cash register or point-

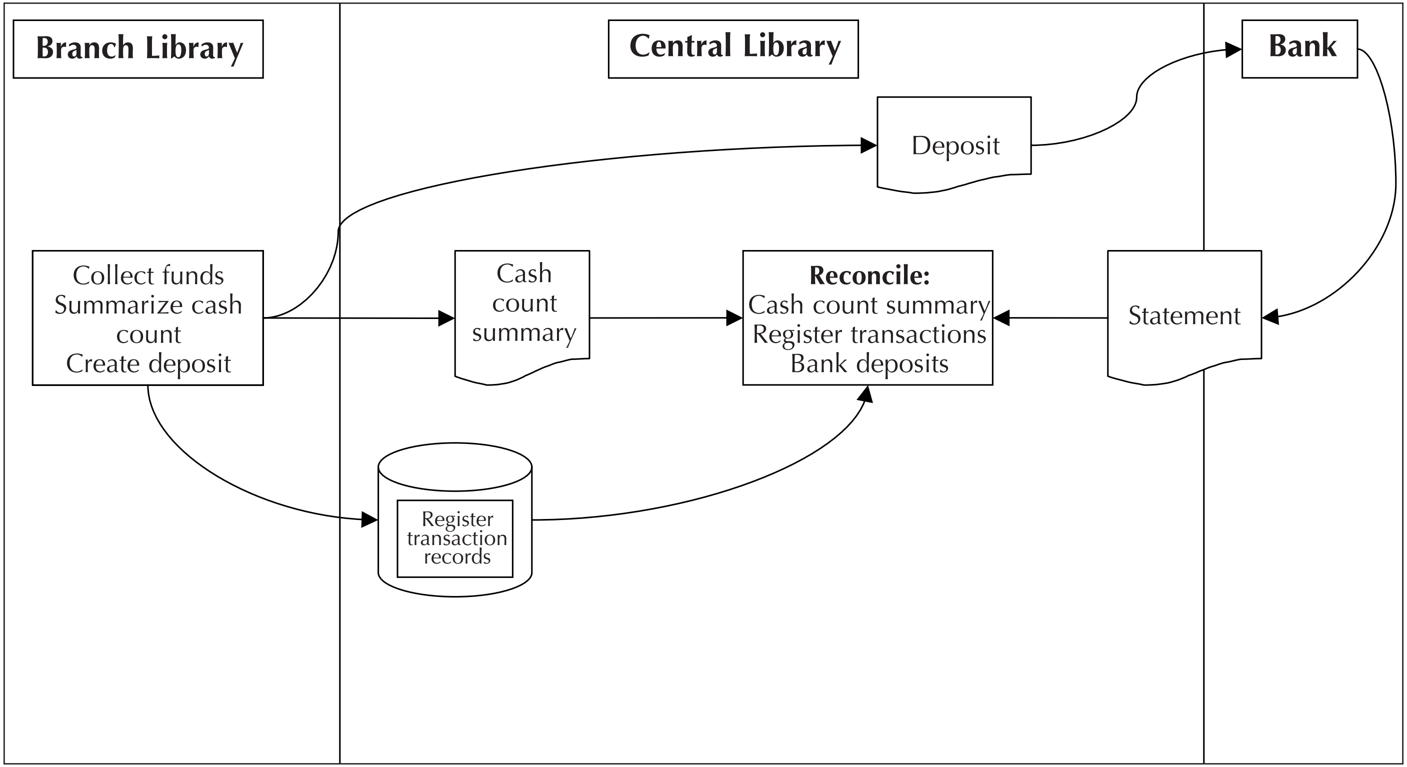


Figure 5.1

SAMPLE FLOWCHART FOR SEGREGATING CASH-HANDLING DUTIES of-sale terminal. We're making the assumptions here that employees have separate login codes, that patrons expect to receive a receipt, and that the register transactions are stored in a separate data file. These first assumptions are discussed in the following section and should be part of any cash management system. Storing the transaction data in a separate file is a useful aspect of a system. It allows the central library to access transaction data immediately and makes it much harder for anyone at the branch to tamper with the data. Separate storage isn't completely necessary, however. Register tapes will do as long as they arrive in a timely fashion (and don't go missing) and as long as they're difficult to tamper with. The key is to have a complete and accurate record of all the transactions that occurred at the register.

At the end of the day, a total is run from the register and a cash count summary sheet is created that reconciles all the transactions made at the register with the cash in the till and with other documents such as register voids. If the amounts don't reconcile, the branch manager needs to investigate. In any case, a copy of the summary sheet is sent to the central library and kept until the bank sends a statement.

The final task that the branch performs is to gather any cash and checks and make a daily deposit at the bank. It's usually a good idea to keep copies of the deposit receipt. In some cases, the deposit receipt is sent to the central library to be verified with the bank statement and transaction records.

Many decentralized libraries first send the cash deposits to the central library, but this invites problems. The longer the cash remains outside a bank, the easier it is for the cash to be lost or stolen. As we observed in our examples from California and Fort Worth, it's all too easy for an unscrupulous employee to take money out of a deposit. A direct deposit from each branch provides the central library with revenue information in just as timely a fashion and has the advantage of getting the cash to the bank faster. The money can also be ready for use just as quickly by using branches of the same bank or by making an immediate transfer of funds from the branches' banks to the central library's or by doing both.

Step 2: The *bank* has the simplest step in this process. On a regular basis, it sends statements to the central library that list the individual deposits of each branch. The information can be as timely as the central library wants in most cases, with features such as e-mail deposit notifications or online access to account histories.

Step 3: The final piece of the system is the *reconciliation* of the daily cash summary, the register transactions, and the bank statements. If the system is working with no serious error or fraud, all three of the components should tie together in the reconciliation: the register transaction should tie into the daily cash count summary, the summary should tie to the day's deposit, and the bank records should reflect that the same amount was actually deposited on that day.

IMPLEMENTING UNDERLYING ASSUMPTIONS

Several assumptions need to be met in order for the final part of the preceding system to be effective. The first is that the person who performs the reconciliation isn't the same one who prepared the cash count summary or the deposit. If the same person does all three tasks, it's too easy to falsify the data to cover up a theft. The second assumption is that the reconciliation is done in a regular and timely fashion. If the system is set up but no one ever looks closely at the three sets of data, any discrepancies will never be found. Creating the system isn't the same as using it. Finally, the most important underlying assumption for the system is that if a discrepancy is found, someone is responsible for following up and resolving it. Remember, discovering a problem doesn't mean you've solved it. Too often, organizations make it too difficult to deal with suspected frauds or have no policy at all for resolving them.

Increase Management Presence Where Cash Is Received

A library official in the Burlingame Public Library theft said, "No one was looking over her [the employee's] shoulder." No one expects library supervisors literally to be looking over their employees' shoulders, but an ongoing management presence is a strong deterrent to the casual theft of cash. Simply stopping by the register several times during the day and observing operations can help deter theft and is a reasonable part of management oversight.

Install Surveillance Equipment

Installing surveillance equipment at registers or other places where cash is accepted is the "nuclear option" for cash control, but it is prevalent in many businesses that take in large amounts of cash such as bars. Surveillance technology has decreased significantly in price over the last five years, as has storage. It's essentially impossible to monitor the cameras in real time, but they provide evidence if a crime is later suspected. Whether the step is warranted, especially in light of the changes in employee morale it could bring, is a matter for the library's management to decide. However, the volume of cash and the risk of loss may make the trade-off a reasonable one in some libraries. (Keep in mind that video surveillance can be a protection for library employees as well, especially in libraries located in high-risk areas.)

Implement Multiple Employee Cash Counts

The principle behind any segregation of duties is that when several pairs of eyes examine the same material, it becomes more difficult to perpetrate a fraud. When two or more employees observe a cash count, it becomes very difficult to pocket some of the bills. The possibility still exists, of course, but the theft now requires the collusion of two employees, which increases the risk of exposure. Understand that the best protection comes from having the two employees observe the cash count simultaneously; otherwise the first employee can still take the cash and provide a lesser, altered amount to the second employee who counts it.

Conduct Surprise Cash Counts

It is common in many firms such as banks for a supervisor to make unannounced counts of an employee's register. The cash count is reconciled on the spot, which precludes the employee making later adjustments to the register tape or cash drawer to hide a cash theft. It's often a good idea to delegate the count to an impartial third party, such as a board member, to preclude collusion between employees and to lessen tensions between employees and management.

Require Cash Register Receipts for Purchases or Payments

Most of us have eaten in restaurants or shopped in stores featuring the policy that "your meal/purchase is free/discounted if you don't receive a receipt." The point of such policies is not to hand out free food or merchandise but to guarantee that the sale is entered into the register. Once the sale is entered, it creates an accounting record that lessens the likelihood of a skimming fraud such as false register sales. Some adjustment of this type of policy is probably needed in a library because taking books out is already free; however, it is possible to offer something along the lines of a "get out of jail free" card for forgiveness of the next overdue fine. Similarly, if the customer doesn't receive a receipt, businesses will often offer merchandise discounts that can be used later. The important thing in these cases is not to give something away but to draw the patron's attention to the receipt or lack thereof.

Use Registers That Store Transaction Information Away from the Register

It's possible for an employee to conceal a fraud by altering or destroying the record of transaction that a register makes. Although the lack of documentation should be a warning sign in itself, missing records hamper the investigation and prevent the library from using the information for other purposes. Many registers and point-of-sale terminals have storage features that allow transaction records to be stored in secure locations such as a locked closet or a remote office by using a LAN.

Limit the Number of Employees Who Are Authorized to Void Register Transactions

Because false voids and refunds are a common method of concealing skimming and cash larcenies, it's common practice to limit the number of employees who have the authority to void transactions or make refunds. The practice is really a segregation of duties and separates the ability to keep records of the transaction from custody of assets (cash in this case). The disadvantage of the practice is that it slows down transactions, as anyone who has waited for a manager to arrive and void a sale at a retail outlet can testify.

The authority is normally delegated through special passwords or keys that are needed to void or refund a sale. For the system to work, knowledge of the passwords must be restricted. Harried managers often give out their keys or passwords so employees can process their own voids, which negates the usefulness of the practice.

Use Individual Logins for Registers

Individual employee logins have two uses in preventing cash thefts. First, they limit physical access to the register, thereby reducing the likelihood of theft. Second, they show who had access to a register if theft does occur. In many instances, particularly those involving skimming, detection comes only by observing trends in cash collections over time. Individual logins allow managers to connect anomalous behavior such as drops in revenue with specific employees. As with controls on voids and refunds, the system loses its effectiveness if the logins are not kept confidential.

Remove Cash from the Library on a Regular Basis

If cash is in the bank, not only is it out of harm's way in the library, it becomes insured against theft if the bank is robbed. There's no reason to keep large amounts of cash in a library. Deposits should be made on a regular basis such as once each day or whenever cash exceeds a set limit.

Don’t Use Cash Receipts for Expenses

When cash is lying around, you may be tempted to use it for minor expenses. Resist the temptation and pay your expenses with checks or through petty cash. Three major problems result from paying expenses directly out of receipts. First, it encourages the library to keep cash around (see the preceding caution). Second, the library is fostering an environment in which many employees come in contact with cash. Both loss and theft increase with the number of times cash is handled. Finally, cash purchases support poor buying habits by facilitating purchases without a PO. (Even worse, some employers allow employees to cash personal checks out of organizational funds. I hope this doesn’t need much explanation; a library isn’t meant to be a bank. Leave check cashing to the professionals.)

Choose Carefully the Employees Who Handle Cash

Choosing employees to handle cash is a minor point, but one that’s easy to implement. I once worked with a nonprofit that entrusted a week’s cash deposit to a new employee. (I know—the first mistake was waiting a week to make the deposit.) It amounted to several thousand dollars, and after three or four hours, a problem became apparent. Long story short, the new employee was a convicted drug dealer and used the money to finance a weeklong bender. The agency could have avoided the whole problem if it had done a background check on him or, more charitably, kept him out of temptation’s way by sending the deposit with another employee.

Stamp Checks with a Restrictive Endorsement

Restrictive endorsement is another simple control that too few organizations use. Require employees to immediately stamp every arriving check with the phrase “XYZ Library, for deposit only.” Such an endorsement won’t prevent the theft of every check, but it makes a check much more difficult to negotiate and is essentially without cost.

Monitor Trends in Cash Collection

Many cash frauds are not easy to prevent or detect at the time they occur. Detection in these cases comes from recognizing trends over time. For example, an examination of cash collections over time might indicate they drop on average during particular days of the week or when a specific employee is on the job. Another analysis may show a higher occurrence of voids during a particular shift. The trends don't, by themselves, provide evidence of a crime, but they indicate an increased risk of fraud that requires further investigation. (Chapter 6 deals with analytical techniques for uncovering fraud in greater depth.)

STEALING MONEY THROUGH BILLINGS

Billing schemes are among the more complicated frauds to set up, but once they're in place, they are probably the most financially damaging schemes that a criminal can perpetrate. As a result, the schemes are not as frequent as cash thefts such as skimming or larceny, but they result in much larger dollar losses when they occur. Billing schemes are characterized by having the library pay for goods and services it never receives or grossly overpay for those it does receive. The fraudster, usually an employee, pockets the proceeds. The most common types of billing frauds are shell companies, vendor collusion, pass-through schemes, and vendor overpayments.

A Mere Shell of a Company

The treasurer and the director of Millersville Public Library were conferring over the library budget figures in August. Something was clearly out of the ordinary. Although $5,000 had been allocated for the maintenance of the grounds, the library had already spent almost $7,000, and there were still at least four weeks left of lawn care. As they went through the bills trying to decide where the money went, they uncovered a number of invoices from J&L Landscaping Services that amounted to more than $1,500. Neither of them had heard of the business before. The address listed was a post office box, and there was no phone listing on the invoice.

At this point, they decided to check at the county courthouse to see who had registered the company and subsequently uncovered the name of an employee of the library. A bit more investigation revealed that he had inserted the invoices into the stack of bills to be paid. The bookkeeper never bothered to check whether the work had been done and simply cut a check for the amount on the invoice. The board member who signed the check never bothered to look beyond the fact that the check amount matched the invoice.

In the end, the employee was prosecuted for fraud and served 180 days in jail. Although the court also imposed restitution on the employee, he subsequently disappeared from town. The library has yet to see any money from him.

How Shell Company Schemes Work

Shell company schemes to acquire funds require a three-part process, some aspects of which are more difficult than others to accomplish. The process requires setting up the shell company, submitting an invoice or a bill, and obtaining payment approval for the fraudulent invoice or bill.

Setting Up a Shell Company

The scheme begins with the creation of a false company. The company is usually created solely for the purpose of the fraud and has no actual assets—hence the term *shell* because it has only the outward appearance of a firm. In most states, creating a business under an assumed name is easy and legal. Anyone wishing to do business under an assumed name simply registers the company as John Smith "Doing Business As" the XYZ Company. Creating a DBA is relatively inexpensive and almost anyone can do it, so it's a simple matter for the fraudster to set up a false company. (I should stress again that a DBA company is common and completely legal as long as it isn't used for criminal purposes.) On rare occasions, the fraudster may go to the length of incorporating, although the expense and additional documentation usually make this unworkable for a simple billing fraud.

Submitting an Invoice or a Bill

Once the shell company has been created, the next step is to create fraudulent invoices using the company name and submit them for payment. Desktop publishing software has made it easy to create professional-looking invoices with a company name, although some fraudsters still use preprinted blank invoices from office supply stores. In either case, the completed invoices are submitted to the library for payment. This can be done through the mail, as with a legitimate invoice; however, it is much more common for the fake invoice to be inserted into a pile of bills to be paid. This is done because billing schemes, as we'll discuss in the next section, usually require an accomplice employee to facilitate getting the invoice approved for payment. (There are instances where legitimate vendors attempt billing schemes. These are less common but are becoming more frequent, as we'll see in a subsequent section.)

Obtaining Approval for Payment of the Fraudulent Invoice

Almost anyone can form a shell company and submit fake invoices for payment. The real difficulty in a shell company scheme comes in getting the fake invoice approved for payment. This is the point where an accomplice employee becomes valuable. There are three basic schemes for getting false invoices approved—self-approval, inattentive supervisors, and the authority of the false documents—all of which become much easier with inside knowledge or authority.

SELF-APPROVAL OF INVOICES

Self-approval is the most efficient means of perpetrating a billing scheme. The fraudster creates the false invoice and then approves it for payment. Depending on the library involved, the fraudster may be able to create and approve the purchase order for the invoice as well. Such a situation arises in organizations with poor or nonexistent segregation of duties.

INATTENTIVE SUPERVISORS

Nearly as good as the fraudster's being able to approve his or her own invoices is having supervisors who routinely approve any expense placed in front of them. Even if the library has good internal control and segregation of duties, they fail to work if the people who are charged with carrying them out don't take their duties seriously. It's interesting to note that in this case, the accounting part of the system works correctly, but a fraud still occurs because of a failure of managerial oversight.

DOCUMENT AUTHORITY

In some cases, the fraudster can't approve his or her own invoices and may even have a supervisor who reviews bills before approving them for payment. The fraudster will then have to rely on the authentic appearance of the fake documents to generate an approval for payment. This requires some additional work, but as we've noted, the quality of desktop publishing programs makes it much simpler to create authentic-looking documents. The technique works best in libraries that don't use a purchase order system, because only the invoice, not an invoice and approved purchase order, is needed to receive payment.

Fraudulent Invoices from Legitimate Companies

A growing trend in white-collar crime is the submission of duplicate or fabricated invoices from firms with which the library does business. This is not a sophisticated crime. Such businesses submit invoices that have been paid previously or are entirely fabricated along with legitimate bills. The scheme succeeds when the library has such poor internal controls that it simply pays any bills that it receives without checking their authenticity. The scheme is especially insidious because the company really exists and provides legitimate services along with the fraudulent ones.

Colluding with Vendors

In some cases, a dishonest employee can collude with an equally unscrupulous vendor to defraud the library. The scheme is similar to a shell company in that the dishonest employee verifies that a vendor shipment has arrived as ordered. The vendor, however, has shorted the order while the employee certifies that all the goods on the invoice have arrived. The scheme is more hazardous because it requires more parties, which, in turn, increases the risk of discovery. It has the advantage, however, of providing an existing business as a cover for the fraud.

Pass-Through Schemes

Cleaning Up on Cleaning Supplies

The Allerton library system had fairly loose controls concerning purchasing. If the purchase didn't involve books or other standard library materials, no one in the organization was interested; ordering and checking in supplies were not glamorous. The job usually fell to whoever didn't attend that month's staff meeting, so when the library cataloger actually volunteered to do the job, everyone else gave a sigh of relief. The cataloger became, in essence, the library's purchasing manager.

What wasn't obvious, however, was that the cataloger's wife also ran a cleaning supplies company. At first there was no problem—supplies were ordered and delivered at the going market price—until it dawned on the two spouses that although the assistant director verified that the purchases were delivered, she never bothered to examine the prices closely. Over the next few months, the unit prices of the cleaning supplies gradually rose until they were 50 percent higher than retail. The scheme proved so successful that the pair decided to branch out into commodities that weren't handled by the cleaning company.

The cataloger and his wife created a shell company and began routing the purchase of office supplies through it. The pair ordered and paid for the office supplies through their shell company but had the supplies delivered directly to the library. The shell company created a new invoice for the deliveries at an inflated price, and the pair pocketed the difference.

The beauty of the scheme was that the library received everything for which it paid, albeit at much higher prices than it should have been paying. The scheme might have gone on indefinitely; however, the city council was forced to cut its entire budget and required the library board to reduce their budget by 15 percent. Tasked with examining the magnitude of their budget for the first time, the board quickly realized that the library was spending well above market for its supplies. It became apparent at almost the same time that the cataloger and his wife were the cause.

Although the cataloger was forced to resign, it wasn't clear from the statutes that he'd actually broken the law, and the library chose not to prosecute. Ironically, the cuts were easily absorbed in the wake of the investigation by simply paying for supplies at competitive rather than inflated rates.

The situation just described is commonly referred to as a pass-through scheme. In these schemes, an employee charged with making purchases buys the items requested by the organization and "passes" them through his or her own company. As the goods change hands, they increase in price even though no value has been added. (This distinguishes the practice from that of legitimate wholesalers who do add value by buying goods in large quantities, transporting them to other locations, and reselling them in smaller quantities.) Enterprising fraudsters (such as the ones in our example) mark up the price of the goods without ever taking possession.

Pass-through schemes flourish in environments where purchasing is done with little or no oversight for costs. Most rudimentary controls only ensure that purchases arrive and that the bill accurately reflects the merchandise received or service rendered. If there is no budgeted amount for the purchases or if no one checks the reasonableness of actual expenses, no action is ever taken unless the goods never arrive.

Schemes That Involve Overpaying Legitimate Vendors

Too Much for Too Little

Ann S. was the accounts payable clerk of a large regional library system. On a regular basis, she would deliberately overpay an invoice for a legitimate expense. For example, a vendor would bill $500 for materials and Ann would write a check for $700. Often, the person signing the checks would overlook the overpayment and simply sign the check. In some instances, instead of overpaying the invoice, Ann would remove it before sending the check and resubmit it several weeks later, double-paying the bill.

Most vendors behaved honestly and sent a refund check for the overpayment. Ann would intercept the check in the incoming mail. She subsequently used the checks to overpay a credit card account. The credit card company never examined the checks to determine if she was a legitimate payee (note the section on stealing cash for more about this technique), and she was able to make thousands of dollars of purchases using library funds. The fraud only came to light when one of the vendors mentioned to the director that the clerk seemed intent on giving too much money. This made the director suspicious, and a subsequent investigation uncovered the fraud. The clerk eventually served nearly a year in jail.

As the preceding example illustrates, sometimes fraudulent payments are made without the vendor's knowledge. In most cases of this sort, two conditions are necessary: the individual signing the check is inattentive, and the person who causes duplicate payments or overpayments must have access to the refunded money.

Detecting and Preventing Billing Frauds

Segregate Duties

Segregating purchase authorization from payment and custody of the purchases is the classic segregation of duties that most accounting texts begin with. All three of the schemes just discussed can be extensively deterred if the following sets of duties are divided among different employees.

AUTHORIZING PURCHASES

Although anyone in the organization can be assigned purchasing duties, the final approval should reside with only a few people. It isn't enough, however, simply to give approval; it needs to be provided in some formal way in writing. Moreover, the approval needs to be for a specific number of items or service at an explicit price. As we discussed in chapter 2, the best way of collecting and presenting the information is in a purchase order (see the following item).

The purchase order isn't effective, however, unless the employees giving the authorization are not the ones making the request. Nor is the system effective if the authorization is made after the purchase occurs.

CONFIRMING PURCHASES

The second segregation of duties needs to occur between the person who makes the purchase and the one who certifies that the purchases arrived (either physically or in performance if they're services). The segregation between requesting and authorizing purchases isn't particularly effective unless there's independent verification that what was ordered arrived. For example, an unscrupulous employee could receive proper authorization from a supervisor to purchase five computers. If no one other than the employee checked on the shipment, it would be simple to claim that all five arrived when there were only three.

AUTHORIZING PAYMENT

The separation that should occur to guard against billing schemes is between authorizing payment, confirming the shipment/performance, and authorizing the purchase itself. The best place to ensure this is at the time the check is signed. As we noted in chapter 2, a board member usually signs the checks. However, the responsibility rests with whoever authorizes payment to verify that the purchase was properly authorized (a signed PO exists with an appropriate date and number) and that the merchandise arrived correctly or the service was performed properly (an invoice exists that matches the amount on the check and on the PO and that has been properly checked against what was actually in the shipment or the work that was done).

Require Purchase Orders for Payment

The whole point of requiring purchase orders is to ensure that anything the library buys is not only legitimate but necessary. Prior approval for expenses, particularly if the approval comes from someone other than the person who's doing the ordering, makes it much harder to commit any of the three billing schemes. Shell companies are harder to hide because two documents are now required for payment, pass-through schemes become more problematic because good POs require costing before the order is made, and overbillings or multiple billings are less likely to occur because a PO is necessary before an invoice can be paid.

Periodically Compare Budgeted Expenses with Actual Expenses

I hope that you're comparing actual with budgeted expenses on a regular basis anyway, because it's good financial management. More specifically, however, all of the billing schemes will create higher expenses, because the library is paying for things it doesn't receive or paying more than anticipated for things it does. A regular comparison between actual and budgeted expenses will uncover the discrepancy, and the more frequently the comparison is made, the earlier the problems can be uncovered. Remember to look at unit cost (how much does a single item cost), not just the total amount. Don't be afraid to question costs that seem unreasonably high, even if they're properly documented. Even if no fraud is occurring, such scrutiny can alert you to poor purchasing practices and subsequently save the library money.

Match Employee Addresses and Phone Numbers with Vendors

Obviously, checking addresses and phone numbers won't catch the more diligent fraudsters, who will often use the addresses of friends and relatives or post office boxes. However, it's a quick and low-cost technique to find the obvious cases. Even if the employee is also a legitimate supplier, this is a potential conflict of interest that needs to be brought to the attention of the library's management.

Examine the Purchases of Services Closely

There's nothing inherently wrong with services except that they have no physical existence. Therefore, it's hard to prove that the service wasn't performed. This characteristic makes it much easier to create fake invoices for services than, for example, for inventory, which has a physical presence and can be observed and counted.

Create an Authorized Vendor List

An excellent method of deterring shell company vendors is to require purchases only from an authorized vendor list. Such a list can confirm not only that the vendor exists but that it's a reputable, reasonably priced source. Keep in mind that the vetting process must be carried out by someone other than the purchasing employee in order for it to work effectively.

Permanently Mark Paid Invoices as Paid

Marking paid invoices is a simple, virtually costless procedure that effectively keeps the library from double-paying invoices. Be sure the term *paid* is permanent, either by using indelible ink or by perforating the paper with the word. (You can buy perforating stamps in most business supply stores.) A similar safeguard can be found in many accounting software packages, which prevent an invoice with a duplicate number from being paid. (Note that this doesn't preclude an incorrect invoice number from being input. Presumably the invoice numbers on the check and the actual invoice won't match, but that's asking for a lot of vigilance on the part of the check signer.)

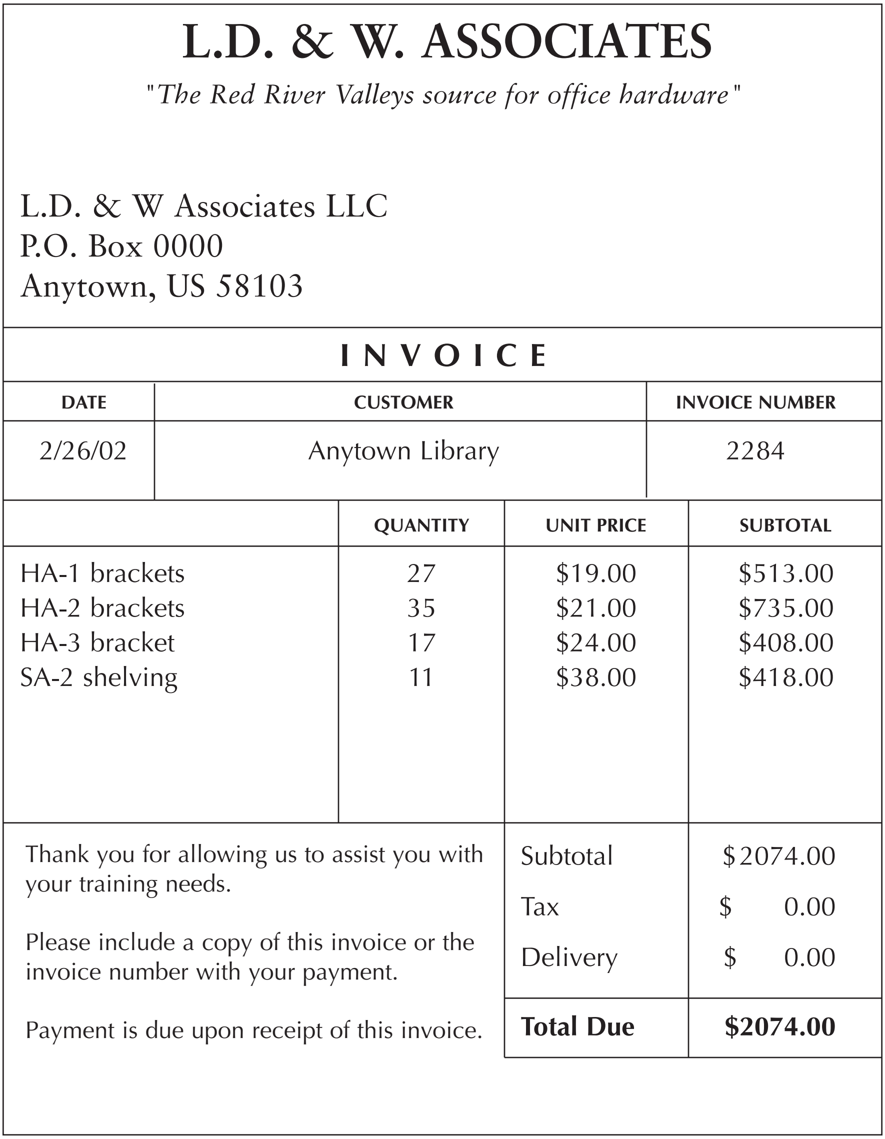
Be Alert for Symptoms of Fraudulent Invoices

Extremely diligent fraudsters will often go to great lengths to cover their tracks. The best deterrence is to keep them out of the system, but sometimes even the best controls fail, and you end up with an invoice or bill that makes you suspicious. Or, better yet, you may want to review your outstanding bills periodically for anything unusual that's gotten past your controls. Fortunately, there are warning signs that can alert you to bills that are at a higher risk of coming from fraudulent sources.

Figure 5.2 is an example of an invoice that contains a number of warning signs for fraud. Let's look at it in more detail.

POST OFFICE BOX ADDRESS

Many shell companies use a post office box as their address. This isn't too odd if you consider it. The company doesn't really exist and has no assets, so why should it have a physical address? Of course many businesses use post office boxes for mail, but they usually have a physical address on their letterhead as well. I would be particularly suspicious of any business that deals in physical inventory and doesn't have a physical address.



L.D. & W. ASSOCIATES

"The Red River Valleys source for office hardware"

L.D. & W Associates LLC
P.O. Box 0000
Anytown, US 58103

INVOICE

DATE	CUSTOMER	INVOICE NUMBER
2/26/02	Anytown Library	2284

	QUANTITY	UNIT PRICE	SUBTOTAL
HA-1 brackets	27	$19.00	$513.00
HA-2 brackets	35	$21.00	$735.00
HA-3 bracket	17	$24.00	$408.00
SA-2 shelving	11	$38.00	$418.00

Thank you for allowing us to assist you with your training needs.

Please include a copy of this invoice or the invoice number with your payment.

Payment is due upon receipt of this invoice.

Subtotal	$2074.00
Tax	$ 0.00
Delivery	$ 0.00
Total Due	**$2074.00**

Figure 5.2
INVOICE WITH WARNING SIGNS OF FRAUD

Consider adopting a policy that the library will not deal with any vendor that doesn't have a physical address. This is a common policy in many organizations, but it won't help much to deter shell companies unless the library also adopts a policy to check whether the business exists at the listed address and to periodically compare vendor addresses with employee addresses.

NO PHONE NUMBER

The same caveats apply here as they do for post office boxes. A phone is another expense that many fraudsters are reluctant to make or that they forget about. A quick cross-check with employee phone numbers can uncover less competent fraudsters, although the proliferation of cell phones has made this technique less useful. (If you're really suspicious, it might be worth checking whether the number is for a cell phone. It wouldn't be unreasonable to include such a check as part of the vetting process for an authorized vendor list.)

TYPOGRAPHICAL ERRORS

The possessive apostrophe in "The Red River Valleys source for office hardware" and the period after the W in L.D. & W are both missing. Poor writing skills aren't indicative of criminal behavior, but it's unusual for a reputable company to make mistakes in its letterhead and invoices.

LACK OF DETAIL

Fraudulent invoices work better when they're difficult to confirm. In many cases, the goods or services for which the invoice is being presented have little or no description. Note that in the example it's essentially impossible to know what was actually delivered.

MISSING EXPENSES

Fraudulent invoices often leave out expenses that would normally be found in legitimate ones. This is understandable because the fraudster is making up the data and can't be expected to remember or know all of the real costs that would be associated with the purchase. The invoice in figure 5.2 lacks both sales tax and delivery costs. It's possible that a library would be tax exempt (although the tax-exempt number is usually included on the invoice to justify that no sales tax was collected), but it's highly unlikely that the purchase of over $2,000 of hardware wouldn't have an accompanying delivery cost.

ROUND NUMBERS FOR COSTS

The example in figure 5.2 isn't as clear in this regard as some shell company invoices can be, but notice that all of the costs are even dollars with no cents. Many fake invoices are even more obvious, with a preponderance of numbers ending in zero or five or with duplicate numbers. It's more difficult than it appears to create convincing fraudulent financial data, and obvious patterns tend to appear that aren't otherwise found in genuine costs.

NO TAX OR EMPLOYER I.D. NUMBER

Identification numbers aren't included for the same reason that no physical address is listed—they don't exist. This isn't as positive a sign as some of the others in the list, but it's a good secondary check if there are other symptoms.

CONSECUTIVE INVOICE NUMBERS

Consecutive invoice numbers can't be determined from the example in figure 5.2, but it is something to look for if you're suspicious. If the company is a fake, it isn't likely to be doing business with anyone else but you. As a result, invoices that are widely separated in time often have consecutive numbers. It might be worth looking at earlier invoices from the same company, if there are any. It would be highly suspicious, for example, if the invoice from 12/18/01 was number 2283. Is it likely that a legitimate company would have made only two sales in over two months?

STEALING MONEY FROM PAYROLL

Payroll schemes traditionally fall into three categories: paying wages for employees who don't exist (also known as ghost employee schemes), paying workers who do exist for more hours or at a higher pay rate than they deserve, and overpaying commissions. Commissions are rarely used in library compensation, so this section will focus on the two remaining types of payroll schemes, which are found in libraries.

Ghosts in the Library

A Case of Nonhaunting

> Chippewa Trails library system had an extensive array of branch libraries that extended over three counties. Although the system office processed each library's payroll, the individual branches were responsible for hiring their own staff and for sending in the time cards on which weekly paychecks were based. The branch manager was responsible for hiring and for signing off on the weekly pay sheets. Although the application materials were

reviewed and stored at the central office, no one except the branch manager ever spoke directly with new hires. Nor did anyone other than the branch manager ever check to see if the hires were on the job.

The system director made a practice of stopping by branches and chatting with employees. She happened to make an unannounced appearance at the Elkton branch on a day when the manager was out sick and ended up chatting with the children's librarian. During the course of the conversation, the librarian asked when the funds would become available for a program assistant. "According to the branch manager," she said, "the funds aren't there this year. We could sure use the help." The director left with a promise to look into the matter. She was confused because the funds had been included, and, in fact, the branch manager had hired an assistant over a year ago.

A review of the branch's finances showed an employee had been issued paychecks for over a year. An even closer examination, however, uncovered that the assistant's Social Security number was only one digit different from the director's. A subsequent investigation disclosed that the branch manager had been cashing the paychecks and had collected more than $25,000 before she was discovered. She was convicted of payroll fraud, lost her job, and was placed on three years of supervised probation. She continues to pay restitution.

How a Ghost Employee Scheme Works

The system just described is known as a ghost employee scheme. In it, a fictitious employee is created (usually by a supervisor, but sometimes in collusion with an employee in payroll or human resources) who is issued a paycheck even though no employee exists. The supervisor and his or her conspirators falsify the ghost employee's time records and deposit the paychecks. The schemes can become quite elaborate with bogus evaluations and even vacations or promotions for the ghost employee.

Ghost employees can also be created from legitimate employees who are terminated or who leave and are never removed from the payroll. In some cases, the supervisor continues to submit bogus time records; however, if the employee is salaried, the system may automatically continue to issue paychecks until the employee is removed from the system.

Creating a Ghost

In order to create a ghost employee, the fraudster typically proceeds through four steps.

STEP 1: HIRING THE GHOST EMPLOYEE

The process of creating a ghost employee begins with adding the employee to the payroll—that is, hiring him or her. In cases where hiring is decentralized, supervisors often have a great deal of independence in deciding who to add to the payroll. By itself, this isn't a problem; libraries can gain a number of efficiencies by allowing local autonomy. In addition to reducing delays in hiring, local managers usually have a better idea of their labor pool, and local autonomy can promote greater ownership of the branch and better morale. The difficulty comes (as in our beginning case) in situations where there is no additional oversight concerning the hires. In our scenario, the branch manager was solely responsible both for hiring new employees and for verifying the hours they worked.

Even if hiring is more centralized, however, it's possible to acquire ghost employees. The key to overcoming centralized hiring lies in the payroll accounting function. In many bureaucracies, an employee need only exist as a computer file in order to generate a paycheck. If the payroll clerk or a similar person has the power to add an individual, and if there is no additional review of individual pay records, then it's still possible to add a nonexistent employee. However, in that case it may be necessary to collude with a supervisor in order to accomplish the second step: collecting the time worked.

STEP 2: COLLECTING TIME INFORMATION

Once a ghost employee has been added, the next step is to collect evidence that the fictitious employee worked so that a paycheck can be generated.

Employees are usually paid based on the time they work in a given pay period. Often, employees keep their own time records, which are approved by a supervisor before being sent to payroll. An unscrupulous supervisor can fabricate a time sheet for the ghost employee and send it to the payroll department along with the rest of the legitimate employees' time sheets. Because the ghost employee already has an identity in the payroll system, the payroll department simply enters the time data and a check is subsequently created.

In cases where someone in the payroll department is working alone, a time sheet from a supervisor may not be necessary. The employee simply enters time data for the ghost worker directly into the payroll system. The supervisor may not, in fact, be aware that the ghost employee has been added to his or her department.

If the ghost employee has been added as a salaried employee, time sheets may not be necessary. Depending on the nature of the employee's compensation, once the salaried employee has been entered, the system simply produces a paycheck at regular intervals (weekly, biweekly, monthly, etc.).

STEP 3: PRINTING THE PAYCHECK

This is usually the simplest part of the process; the fraudster usually doesn't need to take an active part in printing the check once the payroll information is in the system. Most accounting systems automatically create paychecks for employees based on the input pay data. The payroll system can't distinguish a real employee from a ghost as long as the personnel and time information looks the same, so it creates a check for the ghost employee just as it would for anyone else in the system.

STEP 4: DISTRIBUTING THE GHOST EMPLOYEE'S CHECK

After the check has been created, the final step in the process is getting the check from payroll into the hands of the fraudster. In many cases, this isn't difficult. If the checks are distributed by the payroll office, then the employee who created the ghost employee can simply remove the check from those that are distributed to legitimate employees. Similarly, the checks may be distributed by the employee's immediate supervisor, in which case the supervisor who created the ghost employee or who colluded with the payroll department simply removes the check.

When checks are mailed or deposited directly to the employee's account, some additional work is necessary. If the check is mailed, the fraudster must be sure it is sent somewhere to which he or she has access. This may be as simple as using the fraudster's home address, but it can also encompass the addresses of friends and relatives or post office boxes. The same is true for direct deposit. However, working around direct deposit is slightly more complicated. As the result of provisions in the PATRIOT Act, individuals are now required to provide evidence of their identity before opening an account. Therefore, a bank account provides a clearer link to the fraudster than a post office box.

Paying Incorrect Wages and Hours

The second type of payroll fraud that's likely to be encountered in libraries is paying employees for more hours or at higher rates than they're entitled to receive. In most cases, this fraud is perpetrated in the payroll accounting or human resources office. Typically a clerk who inputs hours and wages changes the pay rate for the employee or inputs more hours than the employee actually worked. A similar fraud can be carried out by someone in human resources who changes the employee's base pay rate.

Less commonly, the employee commits the fraud, usually by reporting more time worked than was actually put in. (Very rarely, an employee will discover a way into the payroll system and change his or her own pay rate.) The approval of a supervisor should, in theory, prevent most employees from submitting time sheets with more hours than they're entitled to receive. This fraud thus can include colluding with the supervisor, forging the supervisor's signature on time sheets, or altering time sheets once the supervisor approves them. Supervisors who approve time sheets without actually reviewing them also make this type of fraud possible.

Detecting and Preventing Payroll Frauds

The nice thing about payroll frauds, at least from the perspective of preventing them, is that by definition they're tied to specific people, and not just any people. These people can be found in the workplace. This limits the number of places to investigate if you suspect a problem, and you can regularly ask your employees, unlike your vendors, to identify themselves as a condition of getting paid. This isn't the only technique for dealing with payroll frauds, but it's central to most of the methods we'll discuss here.

Segregate Duties concerning Employee Hiring and Payroll

There are five basic payroll processes that should be separated among different people.

1. ENTERING AN EMPLOYEE INTO THE PAYROLL SYSTEM

To prevent ghost employees from entering the system, the ability to create a new employee account should be separated from the ability to prepare individual paychecks. Normally the ability to input a new employee is limited to the human resources department. Similarly, human resources should be responsible for making any changes to an employee's pay rate.

If the library is too small to have a separate human resources department, then the payroll system should at least be modified to prevent the employee who enters payroll data from adding a new employee or changing an existing employee's pay rate. Most accounting software packages will allow you to segregate these functions with passwords, which should be controlled and limited to management.

2. AUTHORIZING PAY RATE CHANGES

As noted, rate change authorization should be limited to human resources personnel rather than individual supervisors or payroll employees. Rate changes usually depend on promotions or time in position, so verifying this information is properly the job of human resources rather than payroll. Although promotions are usually based on the recommendations of an employee's immediate supervisor, they should still be vetted through human resources. This not only deters fraud but also ensures that raises and promotions are properly documented and legal.

3. AUTHORIZING HOURS

It's appropriate for supervisors to have the authority to verify the number of hours or days that an employee works, but not to input the hours or add the employee. When the same person has both duties, it becomes too easy to create a fictitious employee and verify his or her equally fictitious hours.

4. ENTERING HOURS WORKED

Inputting hours worked is really a clerical function. There's no reason for accounting personnel who input regular payroll information to be able to change pay rates. Moreover, every time payroll data are input, they should have accompanying time sheets authorized by a supervisor.

5. DISTRIBUTING THE PAYCHECKS

In a perfect world, the person who distributes paychecks would not be involved in any other part of the payroll function. This is unlikely in most libraries, but at a minimum, neither the person who inputs the payroll data nor the one who authorizes hours should be charged with handing out the checks.

Verify Employee Identity

Periodically, the library should verify that the employees who receive paychecks really exist. The best way to confirm employees is to distribute paychecks to individual employees and require positive identification in order to receive the check. The library can follow the procedure even for employees who are paid via direct deposit. Such employees can be required to produce identification to receive the transmittal notice that summarizes the gross salary, withholding, and amount deposited. The library can further protect itself by delaying the transfer of funds until the employee's identity is verified.

Employee verification is a powerful tool for preventing and detecting payroll fraud, but it's effective only if the library management follows some additional steps:

1. The verification must be made by someone independent of the payroll process. It doesn't do any good if the person who verifies employee identity is the same one who created the ghost employee. It's too easy to claim that the ghost employee appeared and produced identification if no one else saw it.
2. The verification should be unannounced. Given sufficient lead time, an enterprising fraudster can find someone to impersonate the ghost employee, complete with identification. Similarly, it's common for ghost employees to be on vacation when paychecks are handed out.
3. The unclaimed checks must be properly secured after the identification process is over. If the checks are left lying around, it's easy to steal them or claim that the employee showed up later and received the check.
4. Library management must follow up on any unclaimed check. It isn't enough to verify that an employee wasn't there. If a check is unclaimed, it's necessary to determine why. The employee might have been ill, on vacation, or nonexistent. It's important to determine why the employee was missing, and, if it is a ghost employee, who created it.

Compare Employee Addresses and Social Security Numbers

An easy test for ghost employees is to look for duplicate addresses. As we noted earlier, many fraudsters use their home addresses for the ghost employees they create. The same is true for Social Security numbers. Fraudsters often use their own numbers or numbers that differ by a single digit. Obviously, an enterprising fraudster will be difficult to uncover using these tests, but many criminals aren't that industrious, and in any case the tests are essentially without cost.

Set Limits on Paychecks

Most payroll programs can be configured to limit the amount of hours credited or dollars paid to an employee in a given pay period. By setting an upper limit, libraries can prevent the most egregious frauds. As with address verification, setting limits won't catch a sophisticated fraudster, but it eliminates the worst fraud incidents at a very small cost.

Compare Payroll Records to Employee Files

Every legitimate employee should have a complete personnel file. Any employee who appears in payroll but not in human resources should trigger an immediate investigation. Even if a file exists, however, it needs to be reviewed for completeness. It's extremely difficult to fabricate an entirely fictitious personal history. Any files that are incomplete should trigger further investigation. This control has the added advantage of ensuring that human resources has the information needed to comply with nonpayroll regulations such as equal opportunity and workers' compensation.

Run Historical or Budget-Related Analyses of Payroll Expenses

Ghost employees create increased payroll expenses. An easy diagnostic test for payroll is to determine whether more is being spent this year than in previous years or than was budgeted for. An unfavorable variance doesn't mean a ghost employee exists, but higher labor costs are worth investigating to determine whether the library is exceeding its budget and why.

In addition, supervisors should be required to periodically review their payroll budgets to ensure that everyone who is being paid actually works for the department. (Supervisors should regularly review all of the cost and budget information associated with their areas to ensure that the numbers are accurate.) A supervisor's review is particularly important in organizations that are far-flung geographically or have large staffs, because it may not be possible to know everyone personally.

Have Supervisors Keep Copies of Signed Time Sheets

If a problem develops with altered time sheets, it may become necessary to investigate whether they were altered after the supervisor signed them. A copy in the supervisor's possession can help determine if an employee forged or subsequently altered a time sheet.

Have Supervisors Send Their Approved Time Sheets Directly to Payroll

Time sheets should not lie around after they've been approved. Doing so increases the likelihood of an unscrupulous person altering them.

Periodically Check Payroll Data against Approved Time Sheets

Every paycheck should be generated as the result of an approved time sheet. Managers should periodically review a sample of payroll transactions against time sheets to ensure that every paycheck is both authorized and written for the approved number of hours.

STEALING MONEY THROUGH EXPENSE REIMBURSEMENT

An $8,000 Taxi Ride

Monica S. was the director of a medium-sized public library. In addition to her regular job duties, she was an elected officer of a national professional organization, which required her to travel extensively. It soon became apparent to Monica that much of the cost of her travel was not going to be paid by either her employer or the state organization. Although both would reimburse her for lodging, neither organization would pay for travel expenses from the airport to her hotel when she flew. After paying several hundred dollars for taxi and airport shuttle trips, Monica hit on a method for getting reimbursed—she applied for lodging reimbursement from both her employer and the professional organization. Using photocopied receipts, she was able to submit the same hotel bill to both organizations. At first she did this sparingly, rationalizing that an occasional double-billing was only fair given the volume of expenses she was required to incur. As time went on, however, it became easier to rationalize the double reimbursement. Eventually, she began not only to request lodging from both organizations but to request reimbursement several times for the same trip.

Monica's employers never seemed to take any notice of the dates of her trips or made any attempts to match her expenses with the dates of actual trips. As a result, she was able to request reimbursement for the same hotel stay several times by using photocopied bills. Unlike many fraudsters, she kept her scheme within the constraints of her employer's travel budget (although she did lobby successfully to increase it over several years). She might have gone on looting the library's travel account indefinitely if she hadn't made an indiscreet remark about her travel during an office party. The remark, something along the lines of the library travel fund paying for a new car, irritated a coworker enough for her to make a formal complaint to the board treasurer. An examination of Monica's lodging reimbursements almost immediately turned up the duplicate receipts, because she'd never made any attempt to cover them up. In the end, the library accepted almost $8,000 of restitution in exchange for not prosecuting, although Monica was forced to resign. Along with Monica, several members of the board (including the treasurer) were asked to resign for failing to provide adequate oversight of the library's expenses.

How Expense Reimbursement Frauds Occur

Expense reimbursement frauds are similar in many ways to billing or payroll fraud. In all of these situations, a bill for some outstanding obligation (purchases, hours worked, or travel made on behalf of the employer) is presented to the employer with either inadequate or fraudulent documentation. Payment, when the scheme is successful, is made for goods or services that the library didn't receive. Expense reimbursement fraud differs from other types of fraud only in that the employee incurs personal expenses on behalf of the library rather than the library incurring the expense directly.

In general, expense reimbursement fraud is carried out through four basic mechanisms:

1. Improper Classification of Expenses

Although an employee can incur many expenses during the course of a business-related trip, employers commonly only reimburse some of them. A traveler may, for example, have a suit dry-cleaned during a trip or make a call to a 900 number. Such expenses may be legitimate and work related, but the employer pays only for meals and lodging. Other expenses may be less legitimate—for example, an expense for alcoholic beverages when the employer pays only for food. The point is that the employee may be tempted to camouflage the nonreimbursable cost in his or her expense report as something for which the employer will pay.

The technique in such cases is to claim that the nonreimbursable expense was for a reimbursable payment. The dry-cleaning cost, for example, can be miscategorized as a taxi fare. Similarly, the liquor expense can be added into a legitimate restaurant receipt to make up the difference. Many experienced travelers keep a supply of duplicate, blank receipts for just such contingencies. Even worse, many disreputable businesses issue nondescript receipts that camouflage the true nature of the expense.

A particularly damaging form of misclassifying expenses can occur when employees attempt to have their employers pay for expenses not related to work. Among the most common varieties of this fraud is classifying personal or family travel as work related. The degree to which this fraud occurs can vary from reimbursement requests for a spouse's airfare to the entire cost of a family vacation that involves no business at all.

2. Fabricated Expenses

Fabricated expenses occur when the employee puts in a claim for reimbursement for expenses that he or she never incurred. The degree of fraudulent behavior can vary extensively. It is common, for example, for one employee to claim the expense of another. They may share a cab for which the first employee pays but is uninterested in receiving reimbursement. The cab was an actual expense, but not of the employee who is claiming it. Similarly, an employee may obtain blank receipts from a taxi driver and use them as evidence for several fares that were never paid.

3. Overstated Expenses

In some cases, the expense itself is legitimate, but not at the amount at which the employee makes the claim. Individual claims for shared expenses are common examples of this technique. As we just noted, several employees may share a taxi and split the fare, but one passenger makes an individual claim for the full amount. Similar situations can occur with hotel rooms.

When employees are reimbursed for the exact amount of an expense, they may be tempted to overstate the amount. The situation that we discussed in improperly classifying expenses can occur when the employee is simply trying to receive more expense reimbursement. A restaurant meal for which the employee paid $30, for example, is submitted as $40.

4. Duplicate Expenses

In the earlier example involving Monica S., our fraudster generated most of her ill-gotten gains by submitting duplicate travel receipts. Two basic situations foster the success of this type of scheme. The first situation exists when multiple entities sponsor the trip or employ the individual. Monica's case involved an employer and a professional organization, but the fraud can also occur with parent and subsidiary organizations. The risk of fraud arises in these cases because there is no communication or coordination between the entities.

A second situation that fosters multiple, fraudulent reimbursements is illustrated by Monica's employer. The lack of internal control and financial oversight meant that bills were paid without any stringent review. Because no one examined her lodging bills closely, and because there was no corporate memory concerning what had been paid in the past, it was a simple matter for Monica to resubmit the same bill after enough time had passed for the board members to forget that they had already paid it.

Reimbursements for Items Other Than Travel

Travel expenses are the most common form of employee reimbursement, but they are not the only ones. Employees frequently submit claims for other expenses such as office supplies, program materials, or long-distance calls. The more frequently the library allows this to happen and the greater the range of expenses that employees pay for out of pocket, the greater the risk that some error or fraud will occur. It is poor management and unfair to your employees to have them incur expenses on behalf of the library even if no fraud ever occurs.

Detecting and Preventing Expense Reimbursement Frauds

Segregate Duties

Because travel and other personal expense reimbursement is a purchase, the same segregation of duties that we have discussed earlier should apply. Employees should not be able to approve their own requests for travel or approve requests for reimbursement at the conclusion of the trip. Even more important for travel and reimbursement, however, is to closely scrutinize the details of the trip to ensure the expenses are reasonable and work related. This places more responsibility on the person who signs the check (usually a board member). Too often the person who approves reimbursement looks only at the bottom line and not at the individual expenses.

Require Preauthorization for Travel

Travel is a purchase made on behalf of the library, and, like any other major purchase, it should be properly authorized. Some organizations actually use a purchase order, and indeed many travel expenses such as conference fees can be paid via a PO. This isn't a bad system if you have vendors who are willing to accept it; it gives the library control over the purchase and it keeps the employee from incurring too many out-of-pocket expenses for work.

For many travel services such as airline tickets, however, the only workable system may be to have the employee make the reservation and request reimbursement. In cases where the employee is making his or her own arrangements, the library should still require preapproval for the trip. If a purchase order can't be used, the library can substitute a travel request form or memo from the employee. (Many organizations simply have a policy that requires a letter or memo outlining the request, which is dated and countersigned by a supervisor. The key is to ensure that the request is made and approved before the trip is taken, which may require the use of a date/time stamp rather than a sequential form such as a PO.)

Require Original Receipts for Reimbursement

Photocopies invite abuse of the expense reimbursement system. It's always a good idea to use the original receipts. Remember, however, that the point of the requirement is to verify that the expense was actually incurred by the employee at the amount he or she is requesting. I mention this because many travel expenses no longer produce what we think of as an original receipt. When travel arrangements are made on the Web, the only document may be an e-mail receipt. In such cases, there's usually additional documentation such as a credit card bill that shows the employee paid for the item.

Require Petty Cash or Purchase Orders for Any Work-Related Purchases

Employees should use their personal funds for work-related purchases only rarely. Don't get in the habit of letting your employees pay for work-related purchases with their own money. Apart from the fact that it isn't fair to the employees, it creates an environment that is ripe for abuse. Once you start reimbursing your employees, it's that much harder to keep track of the expenses. The problems don't even have to include fraud. The point of petty cash vouchers and purchase orders is to maintain control of expenses. The library loses that control once employees can make purchases without prior approval.

Regularly Review Travel Expenses for Reasonableness

Travel is normally a small part of library budgets. Any abuses should appear quickly as deviations from the budget if employees are padding their travel expenses or making unauthorized trips. Reviewing travel expenses is also good politically. If the library is a publicly funded institution, be aware that there's something about travel that especially arouses public ire. (No doubt it's the images of all the riotous ALA conventions they've heard about.) Abuses in personal expenses seem to carry a disproportionate weight, so it's a good idea to keep close control.

Don't Help Your Employees Act Dishonestly

Stealing from an employer is never the right thing to do, but employers often seem to go out of their way to make it easy for their employees to rationalize fraud. Let me provide an example. I have a friend who once traveled frequently for her employer. In order to save money on airfare, she was frequently asked to stay over a weekend and leave for work again on Monday. Although this separated her from her friends and family and was a considerable hardship, she did her best to accommodate the request. She quit finally. The company lost a good employee, and the final straw that sent her out the door was laundry. When she stayed over the weekend, she had no opportunity to use her own washing machine or visit the dry cleaners. It was nearly impossible to bring enough work clothing, so she faced the dilemma of starting Monday's work on the road with wrinkled, dirty clothing or sending her clothes out. The company, however, refused to pay for laundry expenses under any circumstances. As a result, she was forced to pad her taxi and meal expenses to pay for her out-of-town cleaning costs, costs she'd incurred for the sake of her employer.

Why, you may ask, is this something to be concerned about? The problem is that employers can be unreasonably cheap about travel. Often, the first place an organization looks when it wants to cut costs is travel. This is fine up to a point, but it creates problems when an employer refuses to pay reasonable and legitimate costs. The real difficulty is that employees begin to look for ways to "game" the system in order to recoup what they see (correctly in many cases) as legitimate expenses. This not only creates an environment in which cheating your employer comes to look reasonable, but it breeds feelings of resentment that create other frauds. Recall that a major cause of frauds is to right perceived inequities.

At the very least, an organization should consider expense policies that don't foster dishonest behavior. Many organizations, for example, simply give employees a blanket per diem to cover all daily expenses. The employee keeps the daily payment regardless of what he or she actually spends. Assuming the amount is realistic for survival ($50 per day to cover all expenses in New York City probably isn't, for example), employees become remarkably frugal when they can keep any leftover travel money.

A second problem that employers create for themselves is misdirecting their internal controls. There's something about frauds involving expense reimbursement that drives employers over the edge. I don't mean to minimize the problems with expense reimbursement; they exist and create extensive losses to employers. But the truth is, compared to billing or payroll frauds, they don't cause that much damage. Employers, however, seem to devote an inordinate amount of time and energy to preventing their employees from charging breakfast if the trip started after 7:30 a.m. By all means scrutinize expense reports, but remember that resources for internal control are finite. In many cases, some of the effort to control travel expenses would be better spent paying closer attention to billing or payroll.

STEALING MONEY WITH CHECKS

Thefts of cash per se are usually limited to the amount of cash that is physically on hand in the library. Although libraries traditionally keep very little cash compared to their total expenditures, this doesn't preclude an enterprising fraudster from using other methods to steal cash. In many cases, the use of library checks not only allows for larger thefts but is also a significantly easier method than carrying off bundles of currency. Such schemes are usually referred to as check tampering.

Tampering requires the perpetrator either to prepare the check or to intercept it on the way from the library to the legitimate payee. Check tampering is unusual, in fact, because it requires the fraudster to physically prepare or alter the check in some way to make it payable to himself or herself. The more common mechanism for frauds is to alter or fabricate the documentation that causes a payment to be made rather than alter the check itself.

It's useful to note the distinction between fraudulent billing schemes and check tampering because the methods may look similar. Billing schemes begin with a false or inflated invoice, which results in the library issuing a check for goods and services it didn't receive. The documentation for an expense exists before the check is issued. Check tampering schemes, on the other hand, begin with a fraudulent check. In some cases, false documentation may be created, but it's done after the fact to justify the issuing of the check. In other cases, both the check and the expense are legitimate, but the amount to be paid is changed (I hope I don't need to explain that it's increased) or the name of the person to whom the money is to be paid is altered. Check tampering is also different from the theft of checks sent to the library. The fraudster who steals checks intended for the library and converts them to his or her own use commits cash larceny or skimming.

How Checks Are Altered

Checks generally have four areas that can be manipulated in order to use the check for illegal purposes: the maker, the payee, the amount, and the endorsement. Because the methods of detection and prevention are slightly different for each area, it will be useful to examine them in detail.

Maker Schemes

Maker schemes are relatively difficult to put into effect but can be extremely damaging and hard to detect once they become successful. In schemes of this sort, the fraudsters obtain blank checks from the organization, make the checks out to themselves, and obtain or create a signature that authorizes payment. To obtain a signed check, the fraudster needs to complete four steps: obtain blank check stock, fill out the check, obtain a signature, and avoid detection after the check has been processed.

STEP 1: OBTAINING CHECK STOCK

The term *check stock* is used here because the fraudster doesn't necessarily need to begin with an actual check. Many businesses today purchase blank check stock from office supply stores and print their own checks using an accounting or check-writing program to write in the account information and check numbers. If you order your blank checks from a high-end paper company (Crane Paper, the folks who make the U.S. currency stock, comes to mind), you might give criminals some trouble copying your checks.

Very few office supply stores, however, keep close security on the sale of check paper, so it's simple for a would-be forger to buy exactly the same stock your library uses. (Really, is it fair for Office Depot to take an individual interest in your paper purchases?)

Even if the paper is different, however, relatively few outlets for processing the checks ever bother to take a close look. Your bank might (or it might not), but certainly credit card processors (note their use in converting stolen checks in the sections concerning skimming and larceny) or payday loan centers will not.

An even easier method of obtaining blank checks is to take them from the library. Although many libraries take great care in protecting their cash, they forget that checks can be converted into cash. As a result, libraries often fail to take sufficient precautions to protect their blank checks. This is especially true when the stock is blank and checks are subsequently printed on it. Because the paper doesn't look like a check, it's difficult to recall that it can easily become one. Boxes of the paper lie around in a way that would never be tolerated with boxes of printed checks. (To be fair, libraries are no more guilty of this than any other organization; it's the nature of the check stock that makes it easy to forget.)

Locking up the blank stock, unfortunately, doesn't prevent maker schemes from occurring. The stock still needs to be used to print legitimate checks, so someone has to have access to it. If you think about this for a second, it becomes obvious that one logical choice for a fraudster who commits check tampering is an employee. Who better to create fraudulent checks than the person whose job it is to create legitimate ones?

STEP 2: FILLING OUT THE CHECK

Once the fraudster obtains the check stock, the next step is to create a legitimate-looking check. If the fraudster is fortunate enough to have stolen an actual blank check, then this step can be as simple as filling out the check with a pen. If the checks are printed, the process becomes more complicated, but only by a small amount. With the advent of scanners and desktop publishing software, professional-looking checks are the work of a few minutes.

I once worked on a fraud case that involved such a scheme. In that case, the perpetrator would get a job working for a mini-mart. He would work a single day, or sometimes only a few hours, and then quit. It's not much of a career path, but his only reason for working was to obtain a legitimate check from the company. Once he had the check, he scanned it into his computer. The scanned copy allowed him to manipulate the date, amount, and check number. He printed numerous forgeries and cashed them in various places that didn't inquire closely about the source. He was caught and the mini-mart wasn't held liable for the forgeries, but it took days of work and inconvenience to get the matter sorted out.

The mini-mart isn't a library, but it could easily have been. Any organization that produces hard-copy checks is at risk. Moreover, the mini-mart firm had a highly competent accounting staff that noticed the forgeries within a day of their inception. A less attentive or less professional staff might have allowed the crime to go undetected for weeks or months, assuming the money in the account didn't run out.

STEP 3: OBTAINING A SIGNATURE

In theory, among the most difficult aspects of obtaining a check is getting it signed. We've all seen crime movies in which a skilled forger practices a signature until it is indistinguishable from the original. Most would-be fraudsters don't have this level of skill or the patience necessary to develop it, but the truth is they don't need to in many cases. To begin with, the same scanning technology that facilitates printing checks also makes it easy to print signatures. The scanned signatures don't resemble written ones very closely, but many organizations no longer hand-sign checks, making the distinction moot. Moreover, many of the outlets that make the theft of checks so easy work just as well for forged checks.

Even worse, however, are situations that make it easy for the fraudster to obtain a legitimate signature. The most basic are those in which the fraudster has the power to sign checks. In those cases, the check isn't forged at all; it's simply made out for the wrong things. I can recall one instance in which the board felt that the director should have the power to meet any expense as it arose, without waiting for a board meeting. (As I recall, it was the director who made the case.) As a result, the director had signature power for the checking account. She began by writing checks for her personal expenses such as her American Express bill and, heady with the success of the scheme, proceeded to write several large checks that cleaned out the library's operating funds.

Check-writing power isn't necessary, of course, as long as the fraudster can get someone else to sign the check without expecting it. In the section concerned with billing schemes, we discussed the situation in which individuals with check-writing authority (usually board members) didn't understand or didn't bother with their oversight duties. They simply signed any checks that were presented to them without bothering to confirm documentation. The same situation holds for personal checks. Given a sufficiently inattentive check signer, a bold fraudster need only insert a check made out to cash or to himself or herself and get it signed.

STEP 4: AVOIDING DETECTION AFTER THE FACT

The final step in accounting for checks is to examine their disposition once they've been written. The process usually includes reconciling the balance in the checkbook with the returned checks, outstanding checks, and the bank statement. If the process is concerned only with making the numbers balance, then the reconciliation will uncover a maker scheme only if the fraudster has failed to record the checks in the account register. However, many bookkeepers are more attentive than this and will make additional comparisons to see whether there is supporting documentation for the checks, whether the payee is correct, and so on. The additional examination will often uncover the illegitimate checks and needs to be avoided if the fraud is to go undetected.

A good way for fraudsters to avoid detection is to perform the reconciliation themselves. This is often the case when the fraudster is an employee charged with writing the checks or signing them or both. The check register balances with the bank statement, so it's only a matter of making sure that the true recipient of the check goes undetected. Another, less elegant method of eluding detection is to lose or destroy the checking account records. The fraudster often intercepts the bank statement and destroys it. Similarly, he or she can destroy or fail to maintain checking records.

It may not seem reasonable to avoid detection by destroying records such as bank statements that can be replaced, but keep in mind that destroying records is usually done in organizations that have little or no financial controls to begin with. When documents go missing, there's rarely any incentive to replace them because there are no records to check them against. It's also in the best interest of fraudsters to keep financial records from becoming useful, because the best way of covering up financial crime is to have no records at all. As appalling as it sounds, it may not even be necessary to create forged checks that look convincing because no one ever bothers to examine them.

Altered Payees and Amounts

Both of these check tampering schemes involve physically altering information that is written on the check. The alteration can be a modification to the original information on the check, or the original information can be removed and new information substituted. It is relatively difficult to change payee information, so this method is usually limited to opportunistic combinations such as changing IRS to I.R. Stevens. (I think many of these instances are urban legends, but it remains a possibility, especially if the last name of the payee is a common one in the community.) More likely the fraudster will alter the amount, although even this is somewhat problematic.

Check tampering is also accomplished by washing out the ink in the check using a variety of solvents and replacing the information with that of the fraudster. Modern checks and ink make this difficult to do without leaving a trace or destroying the check, but less attentive check-cashing establishments may let the check through. In a variation on this theme, the perpetrator writes some information using erasable ink and later erases the entry and replaces it with a fraudulent amount or payee or both. These techniques are much less common now that scanning software is readily available, but they remain a risk in situations where the check is diverted before reaching the legitimate payee.

Forged Endorsements

Forged endorsement schemes occur when legitimate checks are intercepted before reaching the proper recipient. In these cases, the perpetrator either forges the recipient's name and pretends to be the recipient or (still in the role of the proper recipient) signs the check over to himself or herself and deposits it into his or her own account. (This last ploy sounds too stupid to be real, because it creates a direct link to the perpetrator. However, it costs essentially nothing to do, and a surprisingly large number of fraudsters are, in fact, stupid.)

Detecting and Preventing Check Tampering Schemes

All the following techniques are predicated on the library's instituting and maintaining a good set of checking account records. *Good* in this instance means that checks are recorded in the check register in a timely fashion, bank statements are reconciled as they arrive and discrepancies are noted and followed up, and the checking account generally fits into a larger set of financial records. Assuming all that is being done, the library can take several specific steps to reduce the risk of check tampering.

Segregate Duties

Once again we return to segregating duties to protect library resources. In this case, at least three separate sets of duties should be divided among different people.

CHECK WRITING

People who write checks shouldn't be allowed to sign them as well. It's simply too easy to create a false entry in the check register or simply not make any entry at all. An additional safeguard is to ensure that no checks are ever written without the accompanying documentation proving that the expense is legitimate.

CHECK SIGNING

This job is usually relegated to board members. Directors should be strongly discouraged from having check-writing authority, given the power that they probably wield over the check-writing employee. At least as important as segregating the authority is making sure that the person who signs the check doesn't do so without the proper authorizing documents.

CHECKING ACCOUNT RECORD KEEPING

It may not be possible to segregate this duty from check writing in smaller libraries. If check signing is segregated and the signer insists on adequate documentation, there is less likelihood of a problem at this step. A good compromise may involve the board or director periodically spot-checking the returned checks. Make sure that the account is reconciled on a regular basis and be wary of lost statements or reconciliations that are seriously behind. Remember that making sure the numbers balance is a good starting point, but its usefulness is limited if no one follows up on breaks in the sequence or other oddities.

Control Check Writing

Controlling check writing really applies only to printed checks. Many accounting programs that print checks also allow you to control (usually via passwords) who can print checks. Try to find accounting software that gives this added layer of protection and use it to limit check-writing power in the organization. More generally, if you limit checks to those that are printed rather than handwritten, you limit the ability of fraudsters to alter a check.

Use Hard-to-Duplicate Paper for Check Stock

Fraudsters have a significantly more difficult time with forgeries when the check stock is unique or difficult to duplicate. Watermarks, for example, are patterns found in the body of the paper and make duplication more difficult. Similarly, checks can be printed on paper that exhibits text such as *Duplicate* when the paper is photocopied. The additional cost of better-quality check paper is usually negligible compared to the increased security against forgeries. At the very least, consider using something other than the cheapest generic stock from Office Max.

Control Check Stock

When you aren't writing checks, lock up the unused check stock and limit the number of people who have access to it. It won't do much good to procure hard-to-duplicate check stock if you allow a potential fraudster access to it in the office.

Look for Out-of-Sequence Checks

Any bank reconciliation should take note of checks that haven't cleared, but a less obvious problem is what to do with checks that have cleared but are out of sequence. Most forged-maker schemes will use higher-numbered checks to avoid duplicate check numbers. If a check has a significantly higher number than the rest of the returned checks in a statement, the individual tasked with the reconciliation should follow up to determine whether documentation exists for a legitimate expense. Most banks will alert you if out-of-sequence checks are part of the statement, but the information doesn't do much good without an investigation when checks are significantly out of order.

Control the Storage and Disposition of Signed Checks

The key to carrying out altered payee, amount, or endorsement schemes is to obtain a legitimate, signed check. The chances for doing this are decreased significantly if the checks are kept under control once they're signed. Specifically, the persons who sign the checks should distribute them immediately after signing. This can be done by handing the checks to the recipients (paychecks, for example) or immediately placing the checks in sealed envelopes after signing and then posting them. If possible, don't give the signed checks to another individual after they've been signed, especially if that person also wrote the checks or reconciles the bank statements. A further safeguard is to eliminate physical checks altogether and pay employees via direct deposit. (This practice doesn't preclude an insider from carrying out a forged-maker scheme, but it does make it more difficult for third parties to steal the actual check.)

Examine the Front and Back of Returned Checks

Examining checks has become both easier and harder with the advent of electronic check clearing. In most cases, you will no longer receive the physical check, but you can review electronic images of the front and back online. You lose some image quality but gain access to the check image as soon as it clears. Examining the check costs almost nothing. Even if it catches only the most blatant instances of forgery or improperly paid checks, examination is still a good investment.

Look for Odd Patterns in the Recipients of Payments or the Amounts That They Receive

This procedure is similar to examining the front and back of checks. It won't uncover sophisticated frauds, but it costs essentially nothing.

There's no algorithmic way to do this, but whoever is responsible for reconciling the bank statements should be alert for anything that looks odd. For example, are more checks than usual showing up with second endorsements, or is another employee receiving money from the library if she or he never has before? Most frauds by their nature are something out of the ordinary, and even a cursory examination will turn up many of them. Nothing is more embarrassing or pathetic than learning that a fraudster failed to cover his or her tracks and could have been discovered if only someone had bothered looking.

STEALING INVENTORY

Some Things We Just Have to Live With

If you had to choose an environment in which it was difficult to protect inventory against theft, you would be hard-pressed to find a better one than libraries. The entire purpose of libraries is not only to provide access to their inventory (or at least most of it) but to allow people to walk home with it in their possession. (I'm taking the liberty here of defining *inventory* as the physical assets of the library. This includes the collection as well as the equipment used by the library staff.) The amazing thing about libraries isn't that items get stolen but that anything is ever returned.

For a very long time, part of what protected libraries against the theft of materials was that the materials weren't especially valuable. Libraries had relatively little in their collections except books, which were only nominally valuable. Today, however, libraries stock a range of materials in their collections such as artwork, computers, and DVDs, which not only are valuable but also can be extremely portable (DVDs, for example). Even the once-humble book has risen in value and become the target of book thieves and vandals.

The problem of inventory theft is further exacerbated by the growth of outlets in which stolen materials can be sold. Rather than being limited to the local Salvation Army thrift store or to the occasional foray into a used-book store, thieves can access a national market of book buyers through eBay and other Internet-based sales sites.

Does this mean that it's hopeless to try to protect the library's physical inventory? Not necessarily. A number of techniques for protecting inventory are applicable to libraries, either for materials for which there is no public access or, to a lesser degree, for materials that are publicly available. Moreover, one of the best protections is still the attention of informed employees, so the library gains some control simply by making employees aware of how thefts can occur. However, and this is a big however, many of the classic techniques for preventing inventory thefts are simply not compatible with library operations, and a degree of inventory shrinkage is simply the price of running a library.

Some Very Overdue Items

The former head librarian of the Edgerton Public Library was arrested and charged with the theft of more than $6,000 worth of library materials, including books, videotapes, and CDs. The thefts were probably as unsophisticated as a fraud could be. After the materials arrived at the library, the director would wait until all of the other employees left and simply take the materials she wanted out of the open shipment. According to her testimony, she would sometimes peruse suppliers' catalogs to include items she would later take and on other occasions steal items at random that appealed to her. She finally became so blatant that an employee noticed missing items that had been there the day before. The employee became suspicious and alerted the police, who found many of the missing items still in the director's possession at her home. She eventually pleaded guilty to a reduced charge and paid more than $9,000 in restitution (Ostrander 2000).

Lost and Found

An even larger theft occurred at the South Bend public library where a former employee pleaded guilty to stealing more than $43,000 of library materials over three years. Among the employee's duties was to check in returned and new materials. Although the items were listed as being returned to the shelves or in transit to other branches, the employee took the materials home and subsequently sent many of them to her adult children as presents. The matter finally came to light when a library director in Grand Forks noticed the South Bend library stamp on books in a used-book sale. The books appeared never to have been used, which made her suspicious. She called the South Bend library to inquire, and the employee was subsequently fired, pleaded guilty to charges of larceny, and paid restitution. (An interesting footnote to the story is that the restitution was largely to pay for freight charges. Most of the stolen materials were still in the possession of her children and needed only to be shipped back to South Bend [*South Bend Tribune* 2002].)

How Inventory Frauds Occur

Simple Larceny

The most common method for employees to obtain inventory is to take it—that is, pick it up and take it out of the library. As we saw in the preceding cases, this isn't a particularly sophisticated technique. Employees often wait until the facility is closed (or at least when there are no other employees nearby) and simply take the materials. Often, there is no attempt to conceal the theft, and, in the case of libraries, there is no need to conceal it. The constant circulation of library materials makes it difficult to know when materials are missing.

In some cases, there is no attempt to conceal the theft from other employees. In part this may be the result of coworkers who are not aware that a crime is being committed. Library workers routinely walk around the building or even out of doors with materials for legitimate purposes that are hard to distinguish from thefts. In other cases, coworkers may be aware that the theft is taking place but never report it. Some of this may be due to lingering tensions between employees and management, but failing to report a crime can be the result of fear of reprisals (if the thief is a manager) or simply that there is no easy method for making the report.

Miscounting Shipments

Another common method for stealing inventory is to purposely falsify the items in a shipment. In most cases, this is done with an incoming shipment. The fraudster checks in a shipment of books, for example, and reports that only forty-five were received when fifty actually came in. The remaining items are taken out of the library at a more convenient time, and a lost-item report is sent to the shipper. Less commonly, the same technique can be applied to outgoing shipments. In the case of the South Bend library, an inflated shipment of materials was created for a branch, and the missing items were taken home by the employee who created the false report.

Selling "Surplus" Inventory

A common method for disposing of stolen inventory is to sell it as unused or damaged goods. Valuable inventory is written off as damaged or obsolete and sold to an accomplice at a bargain price. An accomplice may not even be necessary in libraries with little or no internal control; the fraudster simply takes the inventory and subsequently writes it off as a surplus sale. Most libraries have a legitimate outlet for selling assets that are genuinely damaged or obsolete. The advantage to a fraudster who has access to this outlet is that there is no need to conceal the inventory shrinkage. The library's records balance, and a legitimate paper trail exists for the assets' disposal.

Misuse of Assets

It isn't always necessary to take possession of assets to commit fraud. In some instances, the fraudster may simply "borrow" the assets and use them for some non-work-related purpose. This practice can be relatively benign as in the use of a library laptop to type a term paper, but not all "borrowing" is innocuous. Using a bookmobile to move furniture on the weekends increases the wear and tear on the asset and reduces its effective life. Libraries are at much less risk for this type of asset fraud than, say, a construction company, but managers should still be aware of the potential for abuse when assets are used for nonwork purposes.

Detecting and Preventing Inventory Frauds

Segregate Duties

Inventory control is one of the classic examples used to illustrate the segregation of duties. In general, accounting for assets, authorizing the use and purchase of assets, and physically controlling assets should be divided among separate individuals or departments. As we've discussed in several sections of this book, the proper authorization for purchasing assets begins with a properly signed purchase order that's created before the purchase takes place.

Segregating the physical control of assets is usually the most difficult task in a library, particularly when it concerns incoming shipments. The best protection is provided by creating a separate department for receiving shipments. Unless your library is very large, however, it isn't likely to have a shipping and receiving department. The next best thing is to have an employee who checks in shipments but who doesn't order or approve any purchases. In very small libraries, it may not be possible to segregate the duties even this much. If that's the case, the next best solution is to rotate the job of checking in inventory among the staff.

Whatever system for segregating custody is used, the process of control that began with the purchase order should be continued by having the incoming purchases checked against the original purchase order. Whoever is in charge of approving payment for purchases (usually a board member) completes the process of segregating duties and control. Before authorizing any payments, the signer should insist that proofs of proper authorization and custody of the assets (PO and receiving report, respectively) are present.

Physically Check Inventory on a Regular Basis

I know that checking inventory is one of those pieces of advice that will not prove to be very useful. Librarians have known for years that reviewing items in the collections—shelf reading—is an integral part of circulation and collection management, but it's also one of the first activities to be reduced as budgets become tighter. If it's possible, physical counts are one of the best techniques for checking on inventory.

Even if shelf reading proves unfeasible, many other valuable items in the library can go missing and should be accounted for. Telephones, office furniture, and computer equipment are just a few of the items in a library that are valuable enough to be of interest to a thief. These should all be inventoried on a regular basis to ensure that they actually exist. The more valuable the assets, the more frequently they should be checked. If the library has extremely valuable assets such as rare books or maps, these should be inventoried immediately after anyone has access to them. An appallingly large number of rare book and map thefts occur because no one in the library thinks to examine them until long after the user has left with the stolen items.

A general tenet from the accounting world is that records and documentation are not sufficient to verify the accuracy of your inventory records. They're a good place to start, but records don't establish the existence of physical assets. This shortcoming is, in fact, one of the classic means by which auditors are fooled by fraudsters. Auditors are trained to look for discrepancies in records, but not necessarily in the physical world. It's easy to make records look consistent, but that doesn't mean they reflect reality.

Process Materials as Quickly as You Can

Don't leave shipments sitting around for long periods without checking that they include what you ordered. In this regard, inventory is similar to cash. The longer materials sit around without being processed, the easier it is for a dishonest employee or patron to remove an item. Until the materials are inventoried, there's no way to know whether items were taken or whether the order was mispacked. Promptly checking inventory has the collateral advantage of making claims for lost or damaged merchandise easier to process. Most shippers have limits on the time they will refund or replace orders.

Secure Your Inventory

Inventory has a physical existence, which means it needs physical protection. You need to lock valuable items up when they aren't in use and control the number of people who have access. Obviously, if this principle is carried to its logical conclusion, a library will cease to operate. But just because the collection circulates doesn't mean you can't lock the doors to the storeroom. Your office supplies, computers, and uncataloged books don't need to circulate with your collection. When you decide to use locks, don't buy cheap ones. I can't recall the number of times I've seen computers protected by $20,000 firewalls and $9.95 locks. Also, if you use keypads instead of keys, be sure to use combinations other than those that come from the factory. Consider changing the combinations periodically. Despite your best efforts, the key codes will eventually get out and become worthless.

Physical protection doesn't just mean locks. As part of an experiment, a colleague and I once backed up a van to a library loading dock and walked out with several television sets, VCRs, and personal computers. Not only did no one try to stop us but the employee on duty very obligingly offered to help us load the van when we told him we were repairmen. Not once did anyone ask to see identification or question what we were doing. The library had an excellent alarm system and set of locks; we simply took the electronics when the systems weren't being used. (By the way, we immediately returned the electronics. The exercise was only to prove a point about security.)

Alert and informed employees are part of what makes security work. Employees should be trained and encouraged to ask questions when they see inventory that has gone missing. No one would ever have discovered the missing materials in the Edgerton library if a staff member hadn't noticed the missing books. In many libraries, it is likely that having observant coworkers is the only workable safeguard against employee theft of materials. Short of installing surveillance systems or checking employees' bags as they leave (see the Install Surveillance Systems and Perform Physical Checks section later in this chapter), the culture of libraries makes it very difficult to institute any further measures to control the movement of materials.

Control the Documents That Allow Access to Inventory

Locking up your valuables is a good place to begin, but it doesn't provide much security if you don't control access to the storage. I once worked in a secure document facility that kept its holdings in a vault. Access to the materials was allowed only with a special written pass that was examined by a guard outside the facility. The only problem was that although the vault was heavily guarded, the blank pass forms weren't. Rather than break into the vault, it was easier simply to steal a blank pass, fill it out, and present it to the guard, who granted admission. Fortunately, the weakness was discovered as part of a routine security examination and not by a thief.

Physical security can't stop with putting locks on the doors. Locks also have keys, which need to be controlled. Similarly, proper authorization should be required before any inventory is shipped or otherwise moved outside the facility. Be sure that authorization forms are controlled or verified with the same degree of diligence as the inventory.

Libraries have the added burden of controlling library card issuance and access. Once a library card has been stolen or falsely issued, the holder is allowed access to a wide range of valuable materials such as DVDs. If the card isn't legitimate or if it's being used by someone other than the legitimate owner, the effect is rather like a stolen or forged credit card. The cardholder has no reason ever to return any of the items checked out.

Limit and Review Inventory Disposal

Writing off damaged or obsolete inventory should require the same sort of authorization as purchases. Rather than justifying the need for new inventory, however, write-offs need proof that the items are damaged or no longer useful before they can take place. Nor should the scrutiny stop with the disposal. Surplus items should also be reviewed after the disposal to ensure that they're not being sold at bargain prices. Similarly, the sales need to be reviewed periodically to determine whether there are buyers who receive preferential treatment. (It may not be necessary to craft a new policy for asset disposal for many libraries. If the library is part of a larger political entity such as a university or municipality, it may already be subject to regulation concerning the disposal of surplus property.)

Install Surveillance Systems and Perform Physical Checks

Many businesses that suffer extensive thefts of inventory institute strong measures to ensure that employees are not leaving with stolen merchandise.

These include placing surveillance cameras in high-theft areas such as warehouses or stores, checking employee handbags and backpacks when leaving work, and even periodically examining employee lockers and desks.

These systems are expensive and frequently have corrosive effects on employee morale. They are, however, effective means of deterring theft if used properly. The question then becomes whether they're worth the cost. There isn't an easy, algorithmic answer to the question. In general, the more valuable the assets and the greater the risk of loss, the more sense that extensive security measures make.

Antique maps and rare books have come under severe risk for theft. In 2005, for example, a map dealer attempted to steal maps worth more than $900,000 from the Yale University library. The maps were small enough to fit in his pockets and would be a tempting target for any would-be thief, including employees (Mehren 2005). Surveillance systems are a more reasonable alternative in this type of environment than they might be in the children's reading room.

At a more general level, the situation raises questions of what is reasonable for a library to own. If the cost of protecting the assets is prohibitive or severely at odds with the library's operating policies, then it may be more reasonable to consider disposing of the assets.

STEALING THROUGH ABUSES OF POSITION

Underlying Principles

The amount and quality of service that we receive in the private sector varies widely according to how much we are willing to pay. There is an expectation that by paying more money, we are entitled to better consideration. It seems perfectly logical to most people (at least in the United States) that the amenities we receive as guests at the Waldorf-Astoria will be better than those accorded to us as guests of Motel 6. However, the same is not true when we consider public services.

Public services—those that we deem benefit society as a whole and that are paid for with public money—operate under an entirely different ethos and set of laws than does the private sector. A guiding principle of public service is that every member of the public is entitled to competent and equitable service. A corollary to this principle is that no member of the public is entitled to preferential treatment, even if he or she is willing to pay more money. These principles are written into law at both the state and federal levels and form the basis for occupational crimes that involve the abuse of position.

Keeping It in the Family

Arthur was the director of a medium-sized public library in the southeast United States. The library was responsible for providing its own maintenance and grounds work, and Arthur's duties included interviewing and hiring a contractor to repair the building, shovel the sidewalks, and mow the lawns. The firm he hired appeared to do all of these tasks competently, and all went well until a disgruntled employee of the maintenance firm decided to talk to a newspaper reporter. It transpired that the same firm that maintained the library also mowed the director's lawn, plowed out his driveway, and hung his storm windows. By itself this wouldn't have been a problem except that the contractor did it for free, and, after some digging, it appeared that this was a condition of getting the contract. Although no criminal charges were filed, the director was forced to resign, and contracts have since been placed on an open-bidding system.

How Abuse-of-Position Frauds Occur

Bribery

The preceding situation is an example of bribery. Most people think of bribery as requiring the payment of cash, but the crime is described more broadly in a three-part definition. Bribery is normally defined as

1. the giving or receiving of
2. anything of value
3. in order to influence an official act or decision [18 U.S.C. § 201(b)].

As we can see, the director both solicited and accepted something of value (home maintenance services) and allowed this to affect one of his official duties (the selection of a maintenance contractor for the library). What's interesting is that the contractor performed his duties satisfactorily and might even have been the best person for the job, but it became a crime when the director accepted "something of value" in order to make the choice. (Such crimes can actually be considered fraud at a technical level. The presumption is that the public is failing to get the full benefit of their tax dollars if the choice of a vendor is influenced by anything other than merit.)

In our example, the crime was clearly bribery because the payment was obviously made to influence an official decision. But what about cases where there is no immediate decision being made? Public officials are frequently offered gifts of one kind or another that can vary from cookies baked by a grateful library patron to the free use of a vacation home in the Bahamas to free or low-interest loans. Does the acceptance of these constitute a crime, especially if nothing specific is sought in return? The answer is maybe, depending on the magnitude of the gifts and the relationship of the giver.

Illegal Gratuities

The acceptance of gifts by a public official can constitute a lesser crime known as accepting illegal gratuities. An illegal gratuity differs from a bribe in that the gift is not made with the intent of influencing an official decision. More specifically, an illegal gratuity is defined as

1. the giving or receiving of
2. anything of value
3. for or because of an official act [18 U.S.C. § 201(c)(1)(A)].

Unlike bribery, an illegal gratuity doesn't require criminal intent.

Of particular importance in cases of bribery and illegal gratuity is the *appearance* of influencing the decision or rewarding the official for carrying out his or her duties. The library director might well have chosen the same maintenance company, but the appearance created by accepting the free maintenance clouds the issue.

Obviously, the standards of propriety can be absurdly restrictive. How, for example, can the gift of cookies from a patron be construed as an illegal gratuity? The difficulty comes as we move farther along the continuum. A box of cookies is clearly not an illegal gratuity; the gift of a Mercedes SUV almost certainly is. How far along the continuum do we need to proceed before we cross the line? Most states and municipalities as well as the federal government set monetary limits on the gifts that officials can receive before those gifts are considered illegal. (Clearly this doesn't apply to personal services such as sex that have other standards.)

Dealing with Abuses of Position in Libraries

Most libraries have limited means by which employees can use their positions for personal gain. Some contracts might be valuable, but the range of official decisions that would be worth a bribe is probably small.

Having said that, however, a board should always closely examine any contracts negotiated by the library for the appearance of conflicts of interest or undue influence on the decision. If the library is not subject to a statute that defines the limits of an illegal gratuity, it would do well to adopt standards of its own.

A second situation in which any library could face potential difficulties is doing business with board members. Because board members have the potential to adversely affect the library and its employees, any business they do with the library gives the appearance of being unfairly awarded. In general, libraries and boards should be extremely wary of doing business together. Unless there is absolutely no alternative, libraries are usually better off adopting a blanket policy of not doing business with any members of their board. In cases where there is no alternative (e.g., a board member is the only plumber in town), the library and the board need to be scrupulous in documenting that the choice was made in an impartial fashion (competitive bids, board member recusing himself or herself from the decision, etc.). If a board member has skills that are likely to result in such a conflict, the library would do well to reconsider the appropriateness of having the individual serve on the board.

6

Uncovering Fraud: Techniques for Your Library to Use

I used to work with classified documents. The building that stored them was guarded by a number of mean armed guards who delighted in detaining anyone who tried to enter without the proper identification. No one ever forgot his or her ID badge more than once. In an effort to make the place even more secure, the agency that owned the building replaced most of the guards with fingerprint scanners, allegedly because they never got bored and made mistakes. Within the first month, everyone discovered that if you breathed on the glass scanner surface, you could make a fingerprint image appear for a few seconds. (No one ever cleaned the scanner.) If you were quick, you could breathe on the surface, hit the scan button, and have the door open—all without having your own print scanned. "That's fascinating," I can hear you say, "but remind me again why I need to know this?" The moral of this particular anecdote is that there still isn't anything that provides better protection against wrongdoing than the observation of an alert and interested person.

If I could tell you just one thing that would provide the best protection for your library, it would be this: "Pay attention." Pay attention to things that don't look right. Is the check you're signing blank? Is there documentation to support the expense? Is there something odd about the whole transaction, like blank lines or an out-of-sequence purchase order number? Pay attention to whether things are reasonable even if they're correct. Is it normal to pay $5,000 for a trip to the ALA Annual Conference? Why has the training budget doubled since last year?

Many of these items are commonsense things that anyone involved with a library would know about, but there are also common analytical techniques that can help you decide whether payments look reasonable and uncover patterns that are common in frauds.

INVESTIGATING FRAUD—A RISK ANALYSIS MODEL

If you know where to look, it's almost impossible to cover up fraud. The problem is that you don't always know where to look, and you can't go through an entire set of financial records and examine every transaction. It isn't practical, and it defeats the purpose of having an accounting department if you're going to enter every transaction twice. What we do instead is look for symptoms of fraud or perform a set of diagnostic procedures or both. If something looks out of the ordinary, we investigate further. The process is the same one your doctor uses when you go in for a physical. He or she takes your vital signs, draws blood, asks you about shortness of breath, pain, and headaches, and so on. If a combination of symptoms and findings indicates some disease may be present, then more detailed and invasive tests are done.

We follow the same rationale when we look for fraud. We begin with simple, cheap diagnostic tests, examine the organization for symptoms of fraud, and decide if and where there is increased risk of fraud occurring. If the symptoms are strong enough, we examine the financial records in greater detail. Among the most common and easiest diagnostic tests for fraud are vertical and horizontal analysis (either with financial statements or with more informal data), gaps and anomalous results in prenumbered documents, and reconciliations (for bank and other accounts). We'll examine each of these more specifically in the following sections.

Vertical and Horizontal Analyses

As we discussed in chapter 2, some internal controls detect rather than prevent fraud.

In many cases of fraud, particularly billing frauds or frauds that involve the theft of cash, it may not be possible to stop the fraud or observe it while it's happening. Instead, we need to examine patterns of cash receipts or expenses over time to determine if there are anomalies that indicate fraud. For example, in the case of cash thefts, do cash receipts and voids of overdue fines occur more frequently on some days than on others? In the case of billing frauds, are there some expenses that are much higher than anticipated? Two simple yet highly effective techniques for examining expenses over time are vertical and horizontal analyses.

Budgets and expenses change over time. This is not earthshaking, but it creates problems when we try to examine expenses from two different periods. Let's examine the income statements for the Acme Library that are laid out in table 6.1. (Obviously this is simplified for the purposes of illustration. A real library would have more expense categories, but the principle is the same.) Clearly revenue has increased and so have most expenses. Salaries, utilities, subscriptions, training, and travel have all increased. By itself, the situation isn't that unusual. Higher levels of activity, for example, require larger budgets and produce higher levels of expenses. The difficulty is deciding whether the increases in expenses are reasonable given the increase in the budget size. This is where horizontal and vertical analyses are particularly useful.

Two ways to determine the reasonableness of expenses are to examine them as a proportion of total expenses for a given year and to examine the percentage increase from one year to the next. These techniques are called vertical and horizontal analysis, respectively. The techniques convert absolute dollar amounts into percentages, which removes size effects and makes comparisons between and within years easier. Table 6.2 shows vertical and horizontal analyses for Acme Library.

To perform horizontal analysis, we simply calculate the percentage increases for expense and revenue accounts from one year to the next. Thus, in our example, revenue increased 10.4 percent (552,000/500,000), salary expenses increased 16.53 percent, utilities increased 40.05 percent,

Table 6.1

ACME LIBRARY: 20X0-20X1 INCOME STATEMENTS		
	20X0	**20X1**
Revenues	$500,000.00	$552,000.00
Expenses		
Salaries	$251,000.00	$292,500.00
Mortgage interest	$110,000.00	$110,000.00
Utilities	$ 38,700.00	$ 54,200.00
Subscriptions	$ 29,500.00	$ 36,500.00
Training	$ 7,000.00	$ 11,000.00
Travel	$ 5,000.00	$ 7,000.00
Total expenses	**$441,200.00**	**$511,200.00**

Table 6.2

ACME LIBRARY: HORIZONTAL AND VERTICAL ANALYSES						
	20X0		20X1		INCREASE 20X0-20X1 (ABSOLUTE $)	INCREASE 20X0-20X1 (% CHANGE)
Revenues	$500,000.00	100.00%	$552,000.00	100.00%	$52,000.00	10.40%
Expenses						
Salaries	$251,000.00	50.20%	$292,500.00	52.99%	$41,500.00	16.53%
Mortgage interest	$110,000.00	22.00%	$110,000.00	19.93%	$ 0.00	0.00%
Utilities	$ 38,700.00	7.74%	$ 54,200.00	9.82%	$15,500.00	40.05%
Subscriptions	$ 29,500.00	5.90%	$ 36,500.00	6.61%	$ 7,000.00	23.73%
Training	$ 7,000.00	1.40%	$ 11,000.00	1.99%	$ 4,000.00	57.14%
Travel	$ 5,000.00	1.00%	$ 7,000.00	1.27%	$ 2,000.00	40.00%
Total expenses	**$441,200.00**	**88.24%**	**$511,200.00**	**92.61%**	**$70,000.00**	**15.87%**

training increased 57.14 percent, and so on. By itself, there are limitations to horizontal analysis, chief among which is that we still expect increases from year to year if the budget increases. Therefore, a second analysis is usually performed to examine how expenses change within a given year. This is vertical analysis.

To perform vertical analysis, we convert all of the year's expenses into percentages, using the year's total revenues as the denominator. In our Acme Library example, the revenue for the year is 100 percent. Every expense is then converted into some percentage of revenue. In 20X0, for example, salaries are 50.2 percent of revenue, mortgage interest is 22 percent, and so on.

Using the Results of Vertical and Horizontal Analyses

So what do the findings mean? First, vertical and horizontal analyses don't tell us anything about whether fraud has actually occurred. All that they provide are indications that something looks out of the ordinary and needs to be examined more carefully. (The same thing is true during your physical. Elevated blood pressure may mean a chronic condition or temporary fear of visiting the doctor.) Be careful about jumping to conclusions, especially if they involve pronouncing guilt or innocence of an employee.

Having given you that caveat, here's what seems unusual in our example.

EXPENSES THAT INCREASE FASTER THAN REVENUES

There are many reasons for expenses to increase, but in general we expect historical relationships among expenses to hold. In other words, if salaries are roughly 50 percent of total revenues, we'd expect to see roughly the same proportion of expenses as the budget rises. In our example, salaries increased from about 50 percent to almost 53 percent. Alone, this increase wouldn't be so bad, except the increase itself is over 16 percent and more than $40,000 in absolute dollars. If the library hasn't added a new position, it should be investigating why salaries increased so rapidly. Even more dramatic are increases in subscriptions (23 percent), utilities (40 percent), and training (57 percent).

In theory, there are legitimate reasons for any of these increases, but the magnitude of the increases warrants a closer look. This would be true, incidentally, even if there were no fraud. Increases of 40 percent and more should be cause for concern for managers; it's not sustainable growth in the long run. If your costs are rising this quickly, it doesn't matter if they're legitimate. You're going to run out of money.

The increase in training is particularly troubling. The costs have more than doubled in a year. Notice that not only has training increased from year to year, it has increased over 50 percent as a proportion of total expenses in 20X1.

Another troubling aspect of expenses that isn't readily apparent from looking at the unanalyzed income statements is that total expenses in 20X1 increased by more than the increase in total revenue. Total revenue increased by $52,000, but the total dollar increase in expenses was $70,000. The library was able to absorb the increase because it hasn't been spending its entire budget. (Notice that only 88 percent of revenue was spent in 20X0 compared to almost 93 percent in 20X1.) Although the library was able to absorb the increases because it had some slack in its finances, the trend can't continue in the long run without overspending the library's revenues.

LARGE INCREASES IN SERVICE-RELATED EXPENSES

Fraudsters often attempt to cover up their thefts by creating false expenses. Service expenses are easier to fabricate because they don't have any accompanying physical inventory. Notice that there are large increases in travel, salaries, and utilities, none of which creates any tangible assets. In theory, the expenses could be legitimate, but the combination of increased expenses in service-related areas should raise concerns and warrant a closer examination.

Budgets and Vertical and Horizontal Analyses

In the preceding example, we made comparisons between years using actual historical data. Analyses can also be done by comparing budgeted expenses with actual expenses. This has the advantage of allowing the library to make comparisons in real time (month by month, for example) rather than after a year's worth of data is compiled. However, the results need to be examined with some caution. Budgets are predictions of the future. Variance between the budget and actual expenses can mean the library's finances are deviating from what they should be, but it may also indicate a need to revise the budget estimates. That doesn't mean the analyses have no value, only that any conclusions need to be applied with caution.

Vertical and Horizontal Analyses Using the Balance Sheet

In profit-making organizations, it's common to perform analyses on the balance sheet as well as the income statement. Common frauds in profit-making firms involve the creation of false accounts receivable or fraudulent sales returns and voids. Fraudulent entries in both of these classes of accounts can be used to offset the theft of cash. However, because libraries don't rely on sales to generate revenue, there's less chance that frauds will be committed that involve accounts receivable or sales. (Indeed, most libraries don't even have these accounts in their balance sheet.) As a result, analysis using the balance sheet is less important in libraries for detecting fraud. By all means consider analyzing your library's balance sheets over time. There are numerous items that can be of use to library managers, but if your primary goal is detecting fraud, the balance sheet is of relatively little use.

Vertical and Horizontal Analyses Using Data from Sources Other Than Financial Statements

Variance reporting and analysis has a specific meaning within the discipline of managerial accounting. It refers to differences between the actual and expected costs for an activity at some level of performance. (For example, we manufacture one hundred tractors. The expected materials cost is $5,000, but we actually spent $5,125, an unfavorable variance of $125/tractor.) The analysis we'll perform to look for fraud is similar, but more informal. It would be unusual for a library to develop standard costs or revenues for its services, but we can still look for patterns and anomalies over time. In essence, this is simply a more general form of horizontal analysis in which we look for departures from the expected.

The discussion of horizontal and vertical analyses used expenses, but for this application of the technique, let's use revenues, specifically the receipt of overdue fines. The advantage of a more informal variance analysis is that it allows us to track changes over short periods. (There's no reason why you couldn't analyze expenses using variance analysis; that's essentially what an analysis of actual versus budgeted costs would provide.)

For our example, assume that you're simply interested in how cash receipts vary during a month. It's possible you have suspicions concerning an employee's honesty or have casually observed that receipts tend to decline during certain periods, but it isn't necessary to have suspicions to carry out variance analysis. The advantages of the technique are that it's cheap and easy to perform and can be used as part of a proactive fraud prevention program.

For the purposes of illustration, assume you've decided that your heaviest cash collections occur between 4:00 and 8:00 p.m. Table 6.3 is a listing, by date, of the collections and voids for the month of June.

If you're very observant, you may see some peculiarities, but the information isn't in a very useful format. For example, it looks as if the

Table 6.3

SUMMARY OF OVERDUE FINE COLLECTIONS AND VOIDS

	FINES				FINES		
DATE	RECEIVED	VOIDS	WEEKDAY	DATE	RECEIVED	VOIDS	WEEKDAY
1-Jun	$120.51	5	Monday	16-Jun	$105.51	6	Tuesday
2-Jun	$102.27	5	Tuesday	17-Jun	$118.45	4	Wednesday
3-Jun	$110.21	5	Wednesday	18-Jun	$117.42	5	Thursday
4-Jun	$118.45	5	Thursday	19-Jun	$106.09	5	Friday
5-Jun	$106.09	5	Friday	20-Jun	$105.06	5	Saturday
6-Jun	$104.03	5	Saturday	21-Jun	$105.06	4	Sunday
7-Jun	$104.03	5	Sunday	22-Jun	$120.51	5	Monday
8-Jun	$111.24	5	Monday	23-Jun	$116.39	5	Tuesday
9-Jun	$100.24	6	Tuesday	24-Jun	$113.30	5	Wednesday
10-Jun	$110.21	5	Wednesday	25-Jun	$118.45	5	Thursday
11-Jun	$119.48	5	Thursday	26-Jun	$111.24	5	Friday
12-Jun	$110.21	5	Friday	27-Jun	$106.09	5	Saturday
13-Jun	$101.97	4	Saturday	28-Jun	$106.09	5	Sunday
14-Jun	$101.97	4	Sunday	29-Jun	$119.48	5	Monday
15-Jun	$119.48	5	Monday	30-Jun	$102.30	6	Tuesday

collections may vary by weekday, but the arrangement of the data doesn't make it easy to tell. So what happens if we sort the data by days of the week? The results look something like those in table 6.4.

A few things now become much more apparent. Monday, Wednesday, and Thursday have roughly the same volume of receipts and collections. Tuesday, on average, is $8–10 lower. Friday, Saturday, and Sunday

Table 6.4

RECONFIGURED SUMMARY OF OVERDUE FINE COLLECTIONS AND VOIDS

	FINES RECEIVED	VOIDS	EMPLOYEE		FINES RECEIVED	VOIDS	EMPLOYEE
Monday				Friday			
1-Jun	$120.51	5	Brown	5-Jun	$106.09	5	Michaels
8-Jun	$111.24	5	Jones	12-Jun	$110.21	5	Michaels
15-Jun	$119.48	5	Jones	19-Jun	$106.09	5	Mull
22-Jun	$120.51	5	Sanchez	26-Jun	$111.24	5	Nguyen
29-Jun	$119.48	5	Jones	**Average**	**$108.41**		
Average	**$118.24**						
Tuesday				Saturday			
2-Jun	$102.27	5	Smith	6-Jun	$104.03	5	Nguyen
9-Jun	$100.24	6	Smith	13-Jun	$101.97	4	Smith
16-Jun	$105.51	6	Smith	20-Jun	$105.06	5	Nguyen
23-Jun	$116.39	5	Brown	27-Jun	$106.09	5	Michaels
30-Jun	$102.30	6	Smith	**Average**	**$104.29**		
Average	**$105.34**						
Wednesday				Sunday			
3-Jun	$110.21	5	Sanchez	7-Jun	$104.03	5	Nguyen
10-Jun	$110.21	5	Michaels	14-Jun	$101.97	4	Nguyen
17-Jun	$118.45	4	Sanchez	21-Jun	$105.06	4	Michaels
24-Jun	$113.30	5	Sanchez	28-Jun	$106.09	5	Mull
Average	**$113.04**			**Average**	**$104.29**		
Thursday							
4-Jun	$118.45	5	Mull				
11-Jun	$119.48	5	Mull				
18-Jun	$117.42	5	Brown				
25-Jun	$118.45	5	Mull				
Average	**$118.45**						

are also lower, but the three days have roughly the same volume of collections. As weekend days, they also have a plausible reason for being different (although it might still be worth looking at them in detail). There seems to be less logic concerning why Tuesday is lower. The number of voids is also relatively consistent for days of the week, except for Tuesday, which is consistently higher.

When we combine the financial data with the names of the employees who were collecting receipts, the results are even more suspicious. On all of the Tuesdays when Smith worked, the receipts are lower and the number of voids is higher. During the one Tuesday Smith was absent, the receipts returned to a higher level. This isn't to say that Smith is guilty of crime; the results may still be a coincidence or have another, benign cause. However, it's certainly reason for a closer scrutiny of Smith.

There's no algorithmic method for analyzing variances; however, changes in activity (money spent, money received, purchases with specific vendors, refunds with specific customers) related to specific employees, locations, or times are common methods. Spreadsheet software and machine-readable accounting records make it possible and convenient to analyze connections among a wide variety of data. The same caveats that we applied to horizontal and vertical analyses are appropriate here. The analysis only indicates areas that need closer scrutiny, not assumptions of guilt.

Gaps and Anomalies in Prenumbered Documents

I wish this section had a more graceful title, because the concept it's describing isn't that complicated. We have documents that come prenumbered. We use the documents in sequence. When there's a break in the sequence or when the documents seem to have been used out of sequence, we realize that something is missing or that the way the document is being used doesn't make sense. Many managers, however, don't understand how the system should work or what they should do with the information when they have it.

A number of documents such as checks, invoices, and purchase orders use the same system. For the purposes of illustration, though, I'd like to use a purchase order/voucher system to explain what gaps and similar information tell us and how to use this information to investigate potential frauds.

In chapter 2, we discussed purchase orders and vouchers. To recap, a voucher is simply a collection of the documents that are needed to determine that a purchase is legitimate and should be paid. It normally begins with a purchase order (PO), which lists the vendor, description, price, and quantity of the items being ordered and carries the signature of an employee authorized to make the purchase. In addition to the PO, there are documents attesting the order was received in the proper amounts (invoices, receiving reports, etc.) and a check for payment.

That's fine as far as definitions go, but how does the system actually work? Figure 6.1 is a flowchart that outlines how a typical purchase order system is put into practice. The process begins with a sequentially numbered PO. This is usually a multipart form, and copies are sent to several places:

Vendor

Receiving

Accounting office

The PO normally contains wording to the effect that bills cannot be paid without a copy of the PO number to encourage the vendor to include a copy of the PO (or the PO number) with the shipped goods and invoice.

When the shipment arrives, the employee responsible for checking it pulls the Receiving copy of the PO and compares it to the actual shipment. If the shipment is correct, the invoice and Receiving copy of the PO are forwarded to the accounting office. Accounting pulls the Accounting copy and compares it to the invoice and Receiving copy. If the amounts agree, a check is cut and sent to the manager who has check-signing authority, together with all the documents that prove the expense is legitimate and ready for payment (i.e., the voucher).

Most PO systems work along these lines; however, the systems don't ensure proper payments unless the following controls are also operating.

1. Purchases are not made without a PO.
2. The PO is completed and authorized before items are ordered or paid for or both.
3. The person who fills out the PO isn't the same person who authorizes it.
4. The person who checks in the shipment isn't either of the people in step 3.
5. The person who signs the check isn't the same person who prepares the check.

One of the main ways to ensure that all of these procedures are followed properly is through the use of sequentially numbered purchase

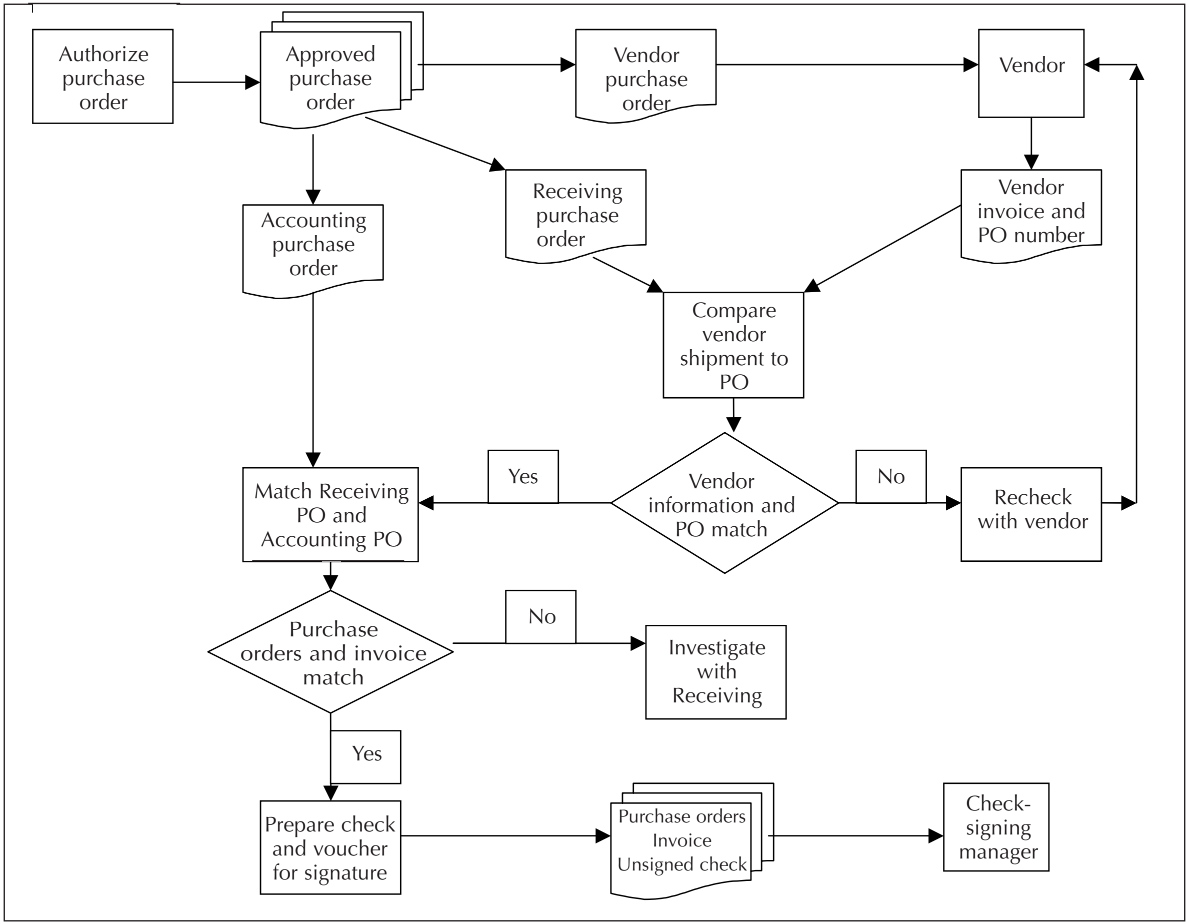

Authorize purchase order
Approved purchase order
Vendor purchase order
Vendor
Accounting purchase order
Receiving purchase order
Vendor invoice and PO number
Compare vendor shipment to PO
Match Receiving PO and Accounting PO
Yes
Vendor information and PO match
No
Recheck with vendor
Purchase orders and invoice match
No
Investigate with Receiving
Yes
Prepare check and voucher for signature
Purchase orders
Invoice
Unsigned check
Check-signing manager

Figure 6.1 **PURCHASE ORDER SYSTEM FLOWCHART**

orders. Here's how the system works. Sequentially numbered documents alert us to situations in which POs are created out of sequence or a PO is missing. The former situation results when a PO is created after an order is placed—in essence, when a purchase is made without proper authorization. The data look something like those shown in table 6.5.

Note that the date on PO 1125 falls before the date on PO 1124, even though the purchase order number is higher in the sequence. Logically, this shouldn't have happened unless 1125 was created later than 1124. However, because the number is higher, PO 1125 was probably created after the order was placed, bypassing the proper procedures for authorization.

Gaps in the PO numbers can provide similar information in tracing purchases. For example, the gaps in the PO number sequence in table 6.6 alert us to several items that may be of interest. PO 1202 has no information associated with it. This could be a voided PO or an oversight in posting, or it could be a fraudulent purchase that the maker wants to keep hidden. In any case, the gap needs to be investigated and resolved. Similarly, PO 1204 has no associated invoice. The order may be pending or was paid without receipt of the purchased item. In either case, the issue should be resolved.

Table 6.5

LIST OF PURCHASE ORDERS

PURCHASE ORDER NUMBER	PURCHASE ORDER DATE
1123	11/07/05
1124	11/11/05
1125	11/09/05
1126	11/13/05

Table 6.6

SUMMARY OF PURCHASE ORDER INFORMATION

PURCHASE ORDER NUMBER	PURCHASE ORDER DATE	VENDOR	INVOICE RECEIVED	AMOUNT	PAID Y/N
1201	6/05/2005	Acme Office Supply	6/11/2005	$287.00	Y
1202					
1203	6/07/2005	Data Products	6/15/2005	$511.00	Y
1204	6/11/2005	Miller Furniture		$600.00	
1205	6/13/2005	Acme Office Supply	6/20/2005	$211.00	Y

An important point to keep in mind concerning sequentially numbered documents is that they don't deter fraud and error by themselves. Their only value is to bring anomalies to the attention of management. If no one looks regularly for missing items in the sequence and, more important, if no one follows up and resolves the missing items, then there's no reason to number the documents. As with horizontal and vertical analyses, gaps tell us only that something is out of the ordinary, not the cause.

Reconciliations

Most of us are familiar with bank reconciliations. This is a procedure in which we take into account differences between our recorded cash account and that of the bank. It reflects deposits and withdrawals that have been made but that have not been recorded in the bank statement.

The bank reconciliation is a specific case of identifying and analyzing gaps and anomalies in sequentially numbered documents. In this case, the checks are prenumbered, and we compare our records to those of the bank. Bank reconciliations have the advantage of being independently prepared statements with which to compare our own records, but reconciliations need not be limited to cash. Reconciliations are a structured technique for examining the disposition of any sequentially numbered documents. We list the documents in order, uncover any with missing or inadequate information, and factor in the effects of any outstanding documents for which we have no final disposition.

If we examine the same record of POs that we saw in table 6.6, we can calculate a more accurate picture of the office expenses for June than if we used only the checkbook. In this case, the outstanding PO (1204) represents an obligation to pay, so the true expense for June is $1,609.00 (all of the paid POs, plus the outstanding one) rather than the $1,009.00 that we get from the check register. A reconciliation also reveals the PO with no information, just as a blank entry would in the check register. Again, there's no indication concerning why the information is missing, only that we need to follow it up.

KNOW YOUR LIMITS AS A FRAUD EXAMINER

Fraud investigation can be significantly more complicated than the preceding section might imply. Many schemes, such as lapping or kiting, are so complicated that it isn't unusual for the perpetrator to maintain two sets of financial records in order to keep the fraud straight. To keep the medical analogy flowing a bit longer, it's like finding something during a self-examination; it should tell you to get to a physician, not perform surgery on yourself.

If you do find something out of the ordinary, and it's anything but the most basic of frauds, I would strongly advise you to bring in a professional to conduct the investigation. You don't want to run the risk of missing something or poisoning the evidence and destroying your case. (See chapter 7 for a more detailed discussion of what to do if you find something.)

Finally, proactive fraud examination is a complement to good internal controls, not a replacement. Any examination is predicated on having reliable and timely financial records, and it's still less traumatic and more cost effective to prevent fraud than to detect it.

~7~

If Fraud Happens: Dealing with the Fallout

EVEN IN THE BEST OF LIBRARIES . . .

One of the things you've probably picked up if you've read this far is that there is no such thing as a completely foolproof antifraud program. It doesn't make economic sense to spend more protecting your assets than they're worth, and frankly, there will always be weaknesses that can be exploited even if you had all the money in the world to spend.

Before we proceed any farther, however, let me disabuse you of the thought that this fact lets a library off the hook as far as instituting good internal controls. It doesn't. I have heard countless times over the years that "if a crook wants to steal something, he or she will." I suppose that's theoretically true, but you'll notice, for example, that muggers don't stand outside military bases trying to rob Navy SEALS or Army Green Berets as they leave. Similarly, criminals rob convenience stores more frequently than they rob armored trucks.

Most criminals are rational about their work. They look for easy, cost-effective targets rather than dangerous ones that require more work and carry a greater risk of capture or injury or both. If the target appears to be difficult to tackle, they look for an easier one. Therefore, even though a financial system can be defeated in theory, if doing so requires more work and risk, that system tends to be left alone. Hence, a moderately effective system is still a better investment than no system.

Of course, there's still a distinct, if reduced, possibility that your library can become the victim of fraud no matter what you do. In the spirit of anticipating problems rather than ignoring them, this chapter is devoted to helping you get through a fraud if the worst actually occurs. Be realistic about what you can do yourself. Some frauds are easy to uncover because no one in the library was paying attention. That doesn't mean all fraud schemes are simple. Nor does it mean that your initial discovery will uncover the full monetary extent of the damage. At some point you are likely to need the services of a professional.

RED FLAGS—WHAT ARE COMMON WARNING SIGNS OF FRAUD?

Fraud is a serious charge to bring against an employee. In making the charge, you almost certainly will be damaging his or her career. Similarly, false or unfounded accusations may leave the library open to legal action. However, neither of these possibilities should mean that you never bring such charges up, only that library management needs to take special care.

It also isn't appropriate or even possible to recheck every accounting entry in the library financial system. That is, after all, the purpose of hiring an accounting manager or a bookkeeper. For those entrusted with stewardship and oversight of library resources, the problem then becomes one of identifying the symptoms of increased fraud risk to know when and where to examine the library finances more carefully. In the auditing profession, these symptoms are known as red flags. Among the more common red flags that library boards and directors should be aware of are the following.

The Library Never Seems to Have Quite Enough Money

A classic symptom of fraud is a normal-looking set of financial statements but very little cash. This is a result of the fraudster stealing cash while covering traces of the fraud by making false entries. If the amount of cash available seems low compared to the level of contributions and appropriations, then the library's finances deserve a closer look. This should be true regardless of whether fraud is suspected because the situation indicates spending in excess of revenues and probably needs to be curtailed before the library runs out of funds. An examination of actual versus budgeted expenses is a good next step (see the Significant Deviations from Budgets section later in this chapter).

Complaints from Creditors

Among the likely outcomes produced by stealing money is unpaid bills. There's some logic to this, because the money in a library is finite and if someone is stealing it, eventually there won't be enough to pay legitimate creditors. Normally, not paying people to whom you owe money is self-correcting. The creditors start clamoring for what they're owed and, given enough time without being paid, stop providing their goods and services. Indeed more than one fraud has come to light (so to speak) when the local utilities cut off gas and electricity.

Although the end may be inevitable, it is often postponed for long periods by the fraudster who intercepts the dunning phone calls and overdue notices. As we've seen earlier, rotating opening mail among employees helps keep this situation from happening. However, the fraudster doesn't always bear full responsibility for keeping the information quiet.

In many cases, board members or employees have received complaints and failed to follow up on them. It isn't unusual, particularly in smaller communities, to know many of the people with whom the library does business and to receive complaints about slow payments. In many cases, the individual passes the complaint along to the appropriate library employee and forgets about it. Only later does the individual experience that sinking feeling of, "If only I'd checked into it more deeply."

This isn't quite as big an oversight as it may first appear, because it's appropriate to refer library financial matters to the director or office manager or both. What is less understandable (or at least less forgivable) is that the individual receiving the complaint never follows it up with both the creditor and the library staff to see how it is resolved.

Significant Deviations from Budgets

The tacit assumptions underlying this red flag are that the library has a budget, that someone reviews it on a regular basis to compare actual with projected expenditures, and that the individual performing the review isn't the fraudster. Assuming all this occurs, the budget can be a valuable tool for diagnosing fraud.

In general, frauds produce higher actual expenses than would be expected from the budget. This may result from paying phantom invoices, overpaying for goods and services actually received, or hiding thefts of cash by making fictitious entries to cover the loss. This is not to say that budget variances are always evidence of fraud. Changes in programs or cost increases outside the control of the library (e.g., for fuel or insurance) may cause legitimate variances. However, large or consistent deviations should be a cause for investigating further.

Excessive Employee Lifestyles

No one expects library management to intrude into the privacy of employees or board members. On the other hand, it's equally bad to ignore the evidence of your own senses. If a minimum-wage bookkeeper comes to work in a new Cadillac Escalade and talks about a vacation to Paris, it's legitimate to wonder how it all gets paid for. Winning the lottery is always possible as is marrying a rich spouse, but significant changes in an employee's finances are worth keeping an eye on. This is an area where managers are uniquely qualified (as compared to auditors, for example) because they see the employees on a regular basis and have a more complete idea of those employees' personal means.

Strange Employee Behavior

For most people who commit frauds, the experience is highly stressful. I assume this doesn't require much explanation. Guilt and the fear of detection and subsequent punishment are common outcomes of committing a crime. This is particularly the case with first-time offenders, as most fraudsters tend to be. These feelings, in turn, cause stress.

High stress levels often manifest themselves with significant changes in behavior such as increases in temper, bullying, withdrawal, or defensiveness. There are, of course, no infallible symptoms of guilt. People suffer stress all the time for reasons that have nothing to do with work. At the same time, as with excessive lifestyles, managers should not discount the evidence of their own observations.

Accounting Anomalies—Particularly Missing or Incomplete Records

Frauds and the subsequent actions to conceal them produce a number of characteristic accounting anomalies. Many of these are technical in nature and of great interest only to auditors, but some are easily observable by anyone in the library. Among these are the following.

Past-due bills or increasing periods before payments are made or both

Documents such as purchase orders with gaps in sequences

Document sequence numbers that don't make sense (e.g., items ordered at a later date have sequence numbers that come before earlier orders)

Documents that are photocopies rather than originals

Documents that are missing (particularly those that authorize purchases or certify that the goods and services were received)

Missing bank statements

Documents that always seem to be locked up or unavailable when the director, the auditor, or board members want to review them

Documents that are kept at an employee's home

Duplicate payments

The preceding list is by no means exhaustive, nor are the items necessarily indicative that a crime has been committed. It's more common, for example, simply to have an employee doing a poor job of bookkeeping than it is to have someone committing a crime. In any case, though, these situations should be cause for concern by the director or board members because they're evidence of poor financial management even if nothing illegal is occurring.

These red flags may also be accompanied by unusual employee behavior. It is common, for example, for employees who have been involved in making fraudulent accounting entries to be highly possessive of the records or unusually sensitive concerning anyone observing them on the job.

Weaknesses Uncovered in Previous Audits

This seems like a no-brainer. If an audit has been conducted in a library and it identified potential control problems (and possibly even suggested the means to correct them), you might expect that the library board and director would regard this as a weakness that needed to be corrected. The truth, however, is that audit recommendations are often not heeded. There are a number of reasons for this. In some cases, no one in the library understands the audit findings or realizes someone needs to do anything about them. (If this sounds as though it could be you, please go back to chapter 2 and reread the section about getting auditors to help you.) In other cases, the advice is simply too difficult to follow. How many of us, for example, have been advised by a doctor to exercise more, eat better, drink less, and so on? We understand the value of the advice but still don't do it for lack of time, lack of discipline, or orneriness. That being said, it can hardly come as a surprise when we have a heart attack or, to extend the example, when the library suffers a fraud.

Previous Fraud

This seems like an even bigger no-brainer, but consider what it means to make changes in the wake of a fraud. The director and board (assuming they aren't the culprits) will be embarrassed. They may feel (perhaps with some reason) responsible. It's natural, if not laudable, under those circumstances to avoid scrutiny. Making changes not only draws attention to a situation they would rather avoid but is a tacit acknowledgment that there were problems to begin with.

New board members or directors should be particularly aware of this situation. Often there are no records kept of the fraud other than the collective memory of staff or other board members. I don't recommend asking about previous frauds the first day you're on the job or the board, but keep your eyes and ears open for hints and the appropriate time to ask the question.

Tips or Complaints of Fraud

A surprising number of frauds are uncovered as the result of tips. What's even more surprising, unfortunately, is the number of organizations that have received tips and failed to follow up on them. We might expect that the receipt of a tip would trigger an immediate investigation, but the same problems are associated with tips as with auditor recommendations—they may be too difficult to deal with or the recipient may not understand what to do with the information.

Many organizations have instituted anonymous tip hotlines to deal with fraud. This may be more than your library needs, but at a minimum you should create an explicit procedure for dealing with tips so they don't fall through the cracks or get ignored. (If you think it would be embarrassing to have a fraud occur during your tenure as director or board member, imagine how much worse it would be if the fraud happened after someone had phoned in a tip that was ignored.)

RESPONSE—WHAT STEPS SHOULD YOU TAKE IF YOU SUSPECT A CRIME HAS BEEN COMMITTED?

Let's assume that you have suspicions that one (or more) of the library's employees are engaged in fraud. In many cases, a poor response by management damages the outcome of the investigation, leaves the library open to legal action for defamation, or increases the damage that results from the fraud. The following are some general steps that the library should take that will protect it from personnel actions, prevent subsequent fraud, and facilitate any investigations.

1. Act Quickly

There are several reasons for taking prompt action once you have suspicions that fraud is occurring. The following are among the most important.

The longer it takes to act, the longer the fraud occurs. Because the crimes are bleeding money out of the library, delays can substantially increase the amount of financial damage that a library incurs.

Delays in acting increase the likelihood that news of the suspected fraud will leak out. This has several adverse effects. The first is that suspicions of fraud damage an employee's reputation. Particularly in cases where an actual finding of fraud has yet to be established, it is important to keep the matter confidential to protect the employee and library. Second, if the information becomes known, the perpetrator has time to cover up his or her actions and destroy evidence. Third, although it is likely that the matter will become known to the public in any case, it is better for the library to control when and how the information becomes public. This is particularly important for maintaining some level of public trust. If a crime has been committed, it is better for the library to appear to have the situation under control and be able to answer inquiries in a competent manner.

The timeliness with which the bonding company is informed of a suspected crime may affect insurance coverage. (See step 5 concerning notification of your insurance carrier later in this section.)

2. Make a Plan

Keep in mind that you will be under enormous pressure to do something. Just for a little while, resist the urge to act; you have more time than you think. If you plan how you'll go about investigating the potential crime, you'll do a better job and minimize liability. At a minimum, lay out how you'll conduct the internal investigation. Normally, a fraud investigation is conducted in the following sequence.

Examine documents. Most fraud investigations begin with documents and work upward to the suspect. Usually, it's possible to complete all or most of the document investigation without alerting everyone in the library (including the suspect). You should have some idea concerning whether a crime has actually occurred, the extent of the damage, and who was involved at this stage. The better you understand, the better the interview part of the investigation will go.

Conduct interviews. Generally, it's better to begin with people who are not directly involved with the fraud and work inward to the actual suspect. Start with witnesses and other people who can corroborate details of the fraud and end with the actual suspect.

The logic behind this sequence is that you need to be as well prepared as possible for any interviews. Reviewing documents first gives you the background necessary to ask penetrating questions and to keep any of the parties from evading your questions by giving you misleading answers. Interviews begin with less confrontational topics and individuals and work up to the suspected fraudster. The same logic applies to gathering background information first to prepare you for the more important interviews.

3. Secure Records

It's rare to catch a fraudster in the act of committing a crime. Therefore, any case you're likely to bring will rely on financial records to demonstrate wrongdoing. If you delay in investigating the case, the perpetrator has time to destroy or alter the records that could be used as evidence. This is especially true in cases where record keeping is primarily electronic. Although a number of techniques allow for the recovery of erased computer files, it is still better to preserve the original records before they're altered. The following are among the steps that the library should continue taking.

a. Secure any storage media such as floppy disks, CDs, data sticks, and the like that have been used by the employee to store data.

b. You may need to make *exact* copies of any hard drives used by the employee to store data. This includes not only the employee's personal computer but also any shared drives on the library network. Be aware that you must do more than simply make a copy of the drive's content. Erased files, for example, may still be found on the hard drive. Similarly, any time you access a file, particularly in MS Windows, you alter the file and potentially compromise its value as evidence.

   The type of copy you need to make is known as a *bit stream* copy (sometimes referred to as hard disk imaging or cloning) and is a bit-for-bit copy, including any deleted, hidden, or password-protected files. Numerous systems can perform this task, but frankly you shouldn't be doing it yourself. Not only does it require significant technical skill but the evidence itself may be compromised by using internal IT people.

c. Secure the originals of any financial records. These may include accounting ledgers, invoices, canceled checks, bank statements, and any other source documents that provide evidence of financial transactions.

d. Search the employee's desk and any associated storage that's under his or her control. In many cases, this is property owned by the library and thus can be searched without the employee's permission. Keep in mind that the situation may vary in circumstances where the employee has a reasonable expectation of privacy (see step 6 concerning employer and employee rights later in this section).

e. Control access to your financial records once you've started the investigation. Specifically, keep the alleged fraudster away from them. This may require locking desks and offices after you've confiscated the keys from the suspected employee. Similarly, physically seize computer hardware or change passwords or do both before you confront the suspect.

4. Deal with the Suspected Fraudster

In general, you have four options if you suspect an employee of committing a fraud.

a. Do nothing and leave the employee alone.

b. Make your initial inquiries without informing the employee.

c. Suspend the employee pending resolution of the suspicions.

d. Terminate the employee. (Summerford and Taylor 2003)

The response you make will depend, in part, on the strength of your evidence and the policies you have in place for dealing with suspected frauds, but obviously some of these responses are more effective than others.

The first option—leave the employee alone and do nothing—is clearly a bad decision. I mention it here merely for the purpose of disabusing you of the idea. It sounds ridiculous and cowardly simply to leave the employee in place and take no action, but an appallingly large number of employers do this. Unfortunately, it has a certain perverse appeal. Doing nothing avoids any messy investigations or painful confrontations. After all, we could be wrong about our suspicions and maybe the problem will simply go away like that pain in my chest. As we know, sometimes the pain does go away, but if we're wrong, the next steps are CPR and bypass surgery. Consider the consequences of taking no action the next time you have doubts about the library's financial well-being.

Option b actually isn't a bad idea. Quietly investigating a suspected fraud has two advantages. It protects the reputation of the employee(s) if they're innocent and deters them from destroying or altering evidence if they're guilty. Remember, though, that any investigation will eventually become public to some degree, and if you turn up anything that uncovers fraud, you'll still need to confront the employee who's responsible.

Deciding between options c and d is a bit tricky. Many employers react strongly to the possibility that an employee has stolen from them and immediately want to terminate the employee. I would advise caution in doing this unless you have unequivocal evidence of fraud. Be sure first that a crime has actually been committed. Snyder's first law of fraud investigation states, "Never assume criminal intent if it can be attributed to incompetence." Many financial systems are simply so badly run that they appear to be criminal. Of course, many fraudsters will hide behind a façade of incompetence, so you may need professional help to untangle the records and decide if a crime has taken place.

If the library is too quick to fire the employee, it may face charges of wrongful termination. Similarly, if the library is part of a civil service system or is unionized, its ability to terminate at will may be constrained. However, even in cases where library employees are subject to employment at will, there are good reasons for suspending rather than terminating the employee.

By suspending employees, pending an investigation, you keep them close at hand and thus able to answer questions. Also, in many states there is a common law obligation on the part of the employee to assist in the investigation by the employer. You may be able to obtain copies of the employee's bank statements and tax returns without a court order.

Ideally, the library should decide on a procedure for dealing with suspected employees before an incident occurs. The grounds for termination and suspension should be laid out explicitly in the library's procedure manual, along with an employee's obligation to assist in any investigation.

5. Notify Your Insurance Carrier

If the library bonds its employees, read the policy carefully. Most carriers require their policyholders to notify them of a suspected crime, and a failure to do so may void coverage. Most policies have thirty- to sixty-day notification periods and may contain other provisions as well, such as the removal of the suspected employee from a position of trust (Summerford and Taylor 2003). Remember that the carrier will usually have some provision for taking criminal or civil action or both against the employee if he or she is guilty. The library will not have the option of collecting on the policy and keeping the matter quiet.

6. Understand Both the Employer's and the Employee's Rights

Employers have the right to conduct fraud investigations if they suspect an employee has committed a crime. (Indeed, libraries have an obligation to the taxpayers or whatever groups support them to ensure that their funds are spent responsibly and are protected from fraud.) At the same time, employers have the obligation to ensure that their employees are treated fairly and are protected from wrongful termination, defamation, and unreasonable invasions of privacy. Although the laws protecting employee privacy rights are complex and the library should consult with legal counsel at the outset of any fraud investigation, there is no reason such laws should prevent a rigorous investigation of fraud. (Please note that a comprehensive overview of workplace privacy law is beyond the scope of this book. The following are some general guidelines, but always consult an attorney before undertaking an investigation.)

The Constitution's Fourth Amendment protects individuals against unlawful search and seizure. However, in order to invoke Fourth Amendment protections, some form of state action must take place. State action occurs any time a governmental agency carries out an investigation, including an investigation of its own employees. State action also occurs when the investigation is done at the request of a governmental agency or under the provisions of state or federal law. The important point for many libraries is that they may be constrained in their ability to conduct employee searches if they are part of a governmental unit such as a municipality or state university system. Proper legal advice is especially important in such circumstances.

If the library is a private employer, however, it has much greater leeway in conducting searches of employee work spaces such as lockers or desks. Such premises are considered the employer's property and are subject to at-will inspections by the employer, provided there is no expectation of privacy by the employee. In practice, this means employees are protected against searches if the area is locked and the employer does not gain prior consent to search. Generally, employers can avoid difficulties with expectations of privacy by establishing a written right-to-search policy and obtaining written consent from employees at the time of hire. Employers are also obligated to be consistent in their treatment of employees regarding searches.

Employees have obligations to assist their employers in resolving allegations of crime in the workplace. How far these obligations extend is a matter of some debate in the investigative community. At a minimum, employees are expected to talk with investigators and answer questions that relate to the crime under investigation. Other aspects of cooperation include the voluntary submission of documents such as bank statements or tax returns. Submission of personal documents is less widely accepted as a reasonable obligation, and its legality may vary by jurisdiction. Once again, the library should consult with legal counsel before attempting to obtain such documents from employees. The library's remedy for employees who refuse to cooperate is usually limited to termination of employment.

7. Consult with Professionals

At a minimum, the library should contact its legal counsel at the outset of an investigation. As the preceding section discussed, numerous legal rights and obligations surround the employer and employee in a fraud investigation. Failing to follow them may compromise the case and leave the library open to damage claims from the employee.

The library should also consider soliciting the services of an auditor or a certified fraud examiner (CFE). Although many frauds are technically uncomplicated, knowledge of accounting and auditing is necessary to fully uncover the extent of the crime. Such expertise usually isn't available within the library itself, and the board or director runs the risk of mishandling the investigation if they try to perform it themselves. Accounting knowledge isn't the only area where professionals can help. Interviewing witnesses and suspects is a skilled practice, and conducting this aspect of the investigation poorly can not only jeopardize the case but leave the employer open to charges of defamation, coercion, and even false imprisonment.

8. Keep Any Investigative Information Confidential

Releasing information to third parties or other employees is a defamation suit waiting to happen. Confidentiality is important not only to avoid litigation but also out of consideration for the lives of the people involved. Fraud is a serious allegation, and you risk damaging an employee's reputation or livelihood by casting premature suspicion. Any information gathered during the investigation should be kept in confidence until the matter is resolved. However, you should avoid blanket promises of confidentiality to interviewees because it may become necessary at some point to turn the material over to police or other investigative agencies.

The library should be particularly careful in making any pronouncements of guilt, because these are matters for a court of law.

FORGET, FIRE, OR PROSECUTE—WHAT SHOULD YOU DO ONCE THERE IS PROOF?

Let's assume that you've done all the work and have solid evidence that an employee of the library has committed fraud. What should you do next? In most instances in this book, I have tried to provide a range of options. In this case, I don't think there are any responsible alternatives except to prosecute. This isn't a universally held opinion; it's estimated that less than one-third of fraud cases are reported to law enforcement. However, if you don't prosecute, you're abdicating your responsibility as a manager and potentially sending the problem to a different organization. Let's examine the alternatives individually.

Do Nothing

As we saw in the previous section, there's a certain appeal to this option: no pain, no embarrassment, no publicity. The problem, however, is that you're letting a criminal employee get away with the crime. Apart from the ethics of the situation, you're sending a message to the guilty employee (as well as any other employee) that you won't act if a crime has been committed. You're setting the stage for future frauds.

Terminate the Employee

This is a better alternative. At least you're removing the original source of the crime from the library. If you decide on this course, I would advise getting a statement from the terminated employee that he or she resigned as the result of committing a fraud. This will help protect you if you plan to be honest when the next employer contacts you concerning the employee's work history. It also acts as a defense if you plan to deny the employee unemployment insurance. But it leaves open a few problems.

First, you're sending the message that there's no downside to committing a crime against the library except losing a job. For many employees, especially at lower levels in the library, this may not be much of a deterrent. (And rest assured, they'll all know about the fraud.) Second, it passes the problem on to a new employer. You've let a criminal go, possibly to commit the same crime in some other location. Ethics aside, this may leave you open to future legal action if a subsequent employer suffers a loss and you failed to notify that employer of the employee's behavior when asked for a reference. Finally, there's a reasonable chance that the incident will leak out and that library management will look inept for allowing the situation to occur and lacking in ethics and responsibility for letting the perpetrator go. (See the Damage Control section below for more discussion of this last point.)

Prosecute

Legal action is messy and uncertain and is bound to bring the fraud to the attention of the public. Nevertheless, it's usually the best course to take if you have evidence that a fraud has been committed. Frankly, you will probably have no choice in the matter if you plan to collect on the employee's surety bond. Most bonding policies contain a clause that gives the insurer the right to take action against the perpetrator to recover losses.

Even if the library is not bonded, prosecution is a good idea for several reasons. First, it sends a clear message that the organization will not tolerate dishonesty. This acts as an immediate deterrent for the perpetrator and for any employees who subsequently consider committing fraud. Second, it reduces the likelihood of passing the problem along anonymously to the next employer. Criminal charges are a matter of public record. Finally, it's the responsible course for the board or director as stewards of public resources. The board and director have an obligation to protect public money from abuse to the full extent of the law.

It will not, unfortunately, be an easy undertaking to bring criminal charges in a fraud case. Criminal charges can only be brought through law enforcement agencies or other officials such as district attorneys. Fraud cases tend to be difficult to understand (compared to, say, holding up a liquor store), and law enforcement officials or prosecutors are sometimes reluctant to take them on. As a result, the library will probably be required to do a significant amount of the investigative work itself.

This doesn't mean that fraud charges are never brought. It does mean that to bring them, you need better proof that a crime has been committed than just suspicion on the part of the employer. The services of a professional such as an auditor or a CFE are useful in making a convincing case of fraud.

DAMAGE CONTROL—HOW DO YOU TELL THE PUBLIC?

Let's begin with a simple premise. If a fraud is committed in your library, the news is probably going to leak out no matter what you do. Even if you do nothing about a fraud, it's likely that your employees will know about it and talk. The best you can hope for under the circumstances is to be dogged by rumors. Worse, if you do nothing, the library may run out of money and shut down, which is about as public an event as I can imagine. If you only terminate an employee, someone in the press will want to know why. If, as I hope, you'll do the responsible thing and prosecute, the matter becomes public as a matter of course. The probability of exposure is even greater if you live in a state with open meeting laws, because you'll probably have an audience for any decisions you make. Even if you go into an executive session, someone will want to know why.

Speaking First: Reasons to Come Clean

The point here is that you can't keep a lid on bad information; the only real question is whether you'll maintain any control of the situation. If bad news is going to become public, it's always better if the public hears it from you. By making the announcement yourself (*yourself* in this case means the management and board of the library, assuming they aren't the perpetrators), you appear decisive and in control rather than reactive and confused. (I hope this is more than appearance and is a reflection of the decisive action you're taking.) Also, by speaking to the issue first, you have the chance to shape the perception of the situation (e.g., decisive board action rather than clueless reaction to probing questions from the media). Finally, by taking responsibility first rather than denying a problem exists, the board and management have a reasonable chance of leaving the situation with their jobs and reputations intact. If the political experience of the last ten years has taught us anything, it's that the American public will forgive mistakes, but only if the people who make the mistakes take responsibility for them.

Breaking the Bad News: A Few Practical Ideas

Congratulations—you're doing the right things, but how exactly do you tell the public? This process is known as Crisis Communication, where *crisis* is defined broadly as any situation that may result in negative publicity for the organization (Hatlestad 2002). In our case, we already know what the crisis is: a fraud. We're probably lucky here in that we're the first people to know about it, so we're left with the opportunity to craft the release of the information. Here are a few general guidelines for doing so.

1. *Take control of the situation.* By now, you have investigated the fraud and gathered evidence and are prepared to take action

against the perpetrator. You should have something to report besides the crisis itself. Remember that in dealing with the fraud and communicating to the public, the longer you wait, the more difficult the problem becomes.

2. *Appoint a spokesperson*. Let a single individual or select group speak for the library and refer all questions to them. The person(s) you choose should be informed, calm, and articulate.
3. *Decide on a message*. Keep your explanations short and coherent and communicate only the approved response. Be especially careful about talking too much in response to questions. Listen first.
4. *Be honest and complete regarding the situation*. Ambiguity is not resolved in favor of the library. It's fine to say you don't know the answer to a question, but follow up and get the answer.
5. *Explain precisely what the problem is and how it will be resolved*. This is an opportunity to demonstrate not only your grasp of the situation but also your ability to deal with it decisively.
6. *Take responsibility*. Taking responsibility for the situation shows courage, not weakness. As we've discussed earlier, it's also the only hope in most situations for obtaining any semblance of public forgiveness and respect (Hatlestad 2002).

The preceding guidelines represent only the briefest of outlines for crisis communication, a detailed discussion of which is beyond the scope of this book. For more information, go to the American Library Association website, which has an excellent discussion of the topic (ALA 2005).

THE LAZARUS LIBRARY—A CASE STUDY OF RETURNING FROM THE DEAD IF THE WORST HAPPENS

The story begins in a medium-sized public library. Over the last five years, the library has received awards for its outstanding community service, and the director has been personally recognized as the force behind this service. What isn't obvious to the community, or even to the library board members, is that financially the library is a shell with almost no money remaining for operations.

Over the course of the last two years, the director has systematically looted the library funds. The means for doing this were almost laughably simple: receiving bogus travel reimbursements, receiving overtime pay when no additional work was done, using library funds for personal expenses such as credit card bills, and subsequently falsifying the recipients of such payments. All of this was possible because the director had complete discretion over how library funds were spent. The board rarely reviewed any of the checks presented to it for signatures, and in any case, financial records were almost nonexistent.

The embezzlement was subsequently discovered, not by the library but by a payroll auditor from the state. When independent state auditors finally examined the library's finances, they were able to prove embezzlement of more than $60,000, but pointed out that it could easily be more. Greater accuracy was impossible given the absence of records.

The Initial Response

The first thing the library board did after receiving evidence of fraud was to suspend the library director and summon the police. In the interim, the assistant director became the acting director and remains director to this day. (I doubt that many management texts discuss this, but one way to get promoted is to have your boss sent to jail.) In due course, the district attorney prosecuted the director, who was found guilty and served a brief stint in prison.

Most expenses in a library are fixed. That is, they remain the same even if the levels of activity in the library decrease. Faced with essentially no operating funds for the rest of the year, the library cut back on the only areas where it did have control: labor and acquisitions. The library was forced to lay off almost all of the staff and was forced to stop buying books for several months. It did manage to reopen with reduced hours after a month, but nearly a year passed before the library's operations approached a pre-embezzlement level of service.

Another management milestone occurred during the post-embezzlement year. The library changed its operating procedures. Changing procedures is also much less common than we'd expect. After all, changing how you do things in the wake of a disaster is a tacit admission that you were doing something wrong. (I know this sounds crazy, but the leadership in many organizations thinks this way. It's often the case that no changes are ever made, even after a serious incident such as this embezzlement.)

The Follow-Up

What changes did this library make? First, the board hired an accountant to create a set of financial records, and, more important, the library used the system. More specifically, the library bought a high-powered accounting program and trained a bookkeeper to use it. It now generates regular financial statements, which are reviewed by the board of directors. (In a particularly nice touch that I would recommend to all of you, the statements also identify those expenses that are incurred directly for public service. It's an effective way to demonstrate that public monies are not being eaten up by excessive overhead.)

A second change was to educate the board members and employees. Boards of directors often constitute the only financial oversight in public organizations, but board members are rarely aware of their oversight duties or recruited for their financial knowledge. Conversely, it is often inconvenient for the library staff to have board members review financial documents. Either scenario can result in the library bypassing normal review processes.

Third, the library embarked on an aggressive training program for both the staff and the board members. Prospective board members are assigned a mentor who briefs them on such points as the need for proper authorizations for payments. Moreover, staff members are trained to insist that board members review their work. As the director has pointed out to me, this requires more time and work by the staff to prepare the documents, and sometimes payments are delayed when documentation is inadequate. However, as the director also noted, the library has changed its management practices to acknowledge that good financial management is worth the extra investment in resources.

This last point is worth emphasizing because it is frequently the case that organizations make procedural changes without ensuring that their employees have adequate resources to carry them out. We can't expect our employees to undertake internal controls seriously if we simply add those controls to their existing job duties. In our case-study library, the director and board revised the staff job duties to take into account the additional workload involved in documentation and actually created a new position to deal with the increased documentation.

It took several lean years, but today the library has achieved its former level of excellence, only this time it isn't just a façade. Recently, the library was successful in passing a bond issue to double the size of the facility: proof of the community's faith in their library's ability to handle funds.

Epilogue: Where There's a Will, There's a Way Out

So where does this leave us? First, I hope this example can help you avoid similar problems. You can always improve the library after something goes wrong, but it's better to avoid the situation entirely. Long after the library corrected its financial problems, the staff and board struggled to reestablish its reputation with the public. But having said that, it's also possible not only to survive disaster but also to prevail, if the will to act is present. After the embezzlement was made public, this library could easily have slipped back to its earlier practices and possibly have invited a second embezzlement. Instead, the new director and board took a hard look at the conditions that caused their problems and changed them. It is always better to avoid mistakes, but acknowledging that this is impossible, we should at least endeavor not to repeat them.

8

A Closing Thought: Getting What You Pay For in Fraud Prevention

UNDERSTANDING THE COST OF PROTECTION

When I first left college, I lived with several roommates in a bad neighborhood in a large city. Burglaries were a regular part of life in our section of town. Our apartment was broken into several times, and each time we replaced our broken locks with more sophisticated and expensive ones. The situation continued to spiral upward until it occurred to us one day that the new locks we were buying cost more than our belongings did. We stopped trying to pay more for protection than the assets were worth and decided it was cheaper to replace the stolen belongings than to buy expensive locks.

The same situation should apply to libraries and internal controls. It doesn't make sense to spend more money on protection than the assets are worth. More precisely, it doesn't pay to spend more on protection than the probable losses that will result if you don't have protection. It isn't simply a matter of the expense that will result from a loss; it's a combination of the expense and the likelihood of occurrence. For example, an earthquake may cause the total loss of your library. However, if you live in an area that hasn't experienced an earthquake since the last ice age, then the expense of earthquake insurance is greater than your probable losses due to earthquakes.

Most organizations never bother to examine their risks in an organized way. The results frequently are a poor investment in risk protection and a concomitant loss that could have been avoided with a little planning.

UNDERSTANDING RISK IN THE NONPROFIT WORLD

In general terms, *risk* can be defined as the uncertainty surrounding any future events that may cause the organization to not fulfill its goals. Put another way, an organization has goals, which reflect some desired state of affairs it wants to attain in the future. A number of events, with varying degrees of likelihood, could intervene between now and the future that would prevent or hamper attaining the goals. Within the context of this book, fraud is one aspect of risk that could prevent the library from reaching its goals.

Risk by itself need not be an insurmountable problem. Although we can't predict the future with complete accuracy, we can still try to anticipate future problems and have plans ready if and when they occur. We won't know with certainty what will happen, but that isn't a fatal condition. Uncertainty can be incorporated into plans and adjusted as new information comes to light. What is fatal is surprise—the unforeseen occurrence. The attempt to anticipate future threats to the organization and have plans for dealing with them is what has become known as risk management.

In the profit-making world, risk management is largely a matter of estimating the costs of future risks and building these into the price of goods and services sold to the public. Nonprofits, however, can't pass the costs of risk along to their public. Moreover, the nonprofit faces a potentially worse outcome from risk than does its profit-making counterpart. Many for-profit businesses have come back from failures to anticipate risks such as dangerous workplaces or toxic spills. The consequences for nonprofits failing to anticipate risk, particularly the risk of fraud, are more dire. Nonprofits exist largely based on the trust they have with their contributors. Once that trust is violated, as in the case of a fraud, the nonprofit may not be able to repair it and can face ruin. As a result, the nonprofit approach has been to reduce or prevent risk before it happens (Alliance for Nonprofit Management 2005).

RISK MANAGEMENT

Risk management encompasses a large number of tools and techniques for uncovering risks, assessing the probability of their occurrence, and estimating the cost of damages if they should occur. Risk management in libraries, as it applies to fraud, need not be this sophisticated. It can be as simple as asking and making estimates for the following questions.

1. What kinds of fraud could possibly occur?
2. How likely are they to happen?
3. What is the potential cost of each occurrence?
4. How do we want to pay for the cost?

Keep in mind the following. First, take into account the full costs of a fraud. These include not only the monetary loss but also the loss of public approval. This becomes particularly important if the library is considering underwriting its fraud losses through insurance. A good bond will help defray any monetary losses, but it won't restore public trust, a potentially greater loss. Second, an organization always underwrites its losses. It can do this through investing in preventive measures, paying insurance premiums, or making the tacit agreement to go out of business if the losses are too large. Even if nothing is ever made explicit, there is an underlying decision. It's important for the library to acknowledge how it wants to handle a loss, even if no antifraud measures are taken.

THE GOOD NEWS—BASIC FRAUD PREVENTION IS CHEAP FOR WHAT YOU GET

A friend of mine is a former all-American cross-country runner. We were discussing training, and he commented that running twenty miles per week would provide 50 percent of the benefit that any amount of running would provide. I have no idea whether this is true (although I have no reason to doubt my friend), but it supplies a useful analogy for internal controls and fraud prevention. That is, most of the benefit that a library gains from fraud prevention comes from relatively cheap and simple measures. Creating an atmosphere of trust and ethics, paying attention, segregating at least some duties, and, above all, creating and maintaining a timely and accurate set of financial records will net the library a majority of the control and protection that any amount of internal controls will provide.

An example closer to the hearts of many librarians is the 80/20 rule. Most of us know from reference classes that a relatively small portion of a collection can supply the majority of all information needs. You could, in theory, run a library satisfactorily with a very small collection. The real questions, though, are how much more service do you need to supply to patrons and at what cost? The same is true for fraud prevention.

Complete protection is more than we can obtain and wouldn't be worth the cost even if it were attainable. But the fact that perfection is unattainable shouldn't preclude looking for some protection at a reasonable price. A small investment in internal controls will yield a large return in protection at a price that's lower than the alternative—a costly fraud.

References

ALA American Library Association. 2005. Crisis communication with the media. http://www.ala.org/ala/oif/iftoolkits/toolkitsprivacy/privacy communication/crisiscommunication/crisiscommunication.htm.

Alliance for Nonprofit Management. 2005. Risk management in the nonprofit sector. http://www.allianceonline.org/FAQ/risk_management/what_is_risk_management.faq.

Association of Certified Fraud Examiners. 2004. *Report to the nation on occupational fraud and abuse*. Austin, TX: ACFE.

COSO Committee of Sponsoring Organizations of the Treadway Commission. 2005. Internal control—Integrated framework. http://www.coso.org/publications/executive_summary_integrated_framework.htm.

Cressey, Donald. 1953. *Other people's money: A study in the social psychology of embezzlement*. New York: Free Press.

Hatlestad, Dan. 2002. No news is bad news. http://firechief.com/mag/firefighting_no_news_bad/.

Hersberger, Julia, and Herbert Snyder. 2000. Internal control and financial misconduct in public libraries. *Encyclopedia of Library and Information Science*, vol. 66. New York and Basel: Marcel Dekker.

Mehren, Elizabeth. 2005. The nation: Alleged thefts disquieting for libraries; A noted researcher is charged with stealing $900,000 in rare maps from a Yale collection; The case is just one that has librarians on notice. *Los Angeles Times*, September 10.

NCNB National Center for Nonprofit Boards (now BoardSource). 2005. http://www.ncnb.org/.

New York Times. 2003. Worker charged with stealing $77,000 from Floral Park Library. July 9.

Oder, Norman. 2005. Budget report 2005—Tipping point. http://www.libraryjournal.com/article/CA491143.html#table1.

Oder, Norman, and Michael Rogers. 2005. Library theft cases in GA, MI. *Library Journal* 130 (April): 24.

Ostrander, Kathleen. 2000. Former head librarian charged with stealing from library: She's accused of taking $6,800 worth of books, CDs, tapes from Edgerton Library. *Milwaukee Journal Sentinel*, May 16.

Rogers, Michael. 2004. Ft. Worth library loses $73K. *Library Journal* 129 (November): 24.

Snyder, Herbert, and Donna Dietz. 2006. Fraud in community health centers. *Journal of Forensic Accounting* 6 (December): 301.

Snyder, Herbert, and Julia Hersberger. 1997. Public libraries and embezzlement: An examination of internal control. *Library Quarterly* 67 (January): 1.

South Bend Tribune. 2002. Ex-library worker sentenced in theft. September 11.

Squatriglia, Charles, and Julie Lynem. 1999. Burlingame library worker charged in $129,000 theft: $20 bills missing from overdue book fines. *San Francisco Chronicle*, December 9.

Summerford, Ralph, and Robin Taylor. 2003. Avoiding embezzlement embarrassment or worse. *Fraud Magazine* (November–December): 38–41.

Tsao, Emily. 2005. Suspicious book leads to arrest in library theft. *The Oregonian*, March 25.

Wells, Joseph. 2005. *Principles of fraud examination*. Hoboken, NJ: John Wiley and Sons.

Index

Herbert Snyder is associate professor of accounting at North Dakota State University and a Certified Fraud Examiner. He has written extensively on financial misconduct in organizations as well as on library finance and accounting. Dr. Snyder's articles on library financial management have appeared in *Library Quarterly* and *Library Administration and Management*. In 2004, he was awarded a Certificate of Achievement by LAMA for his contribution to library management and for his column "Small Change," which ran in *Library Administration and Management* from 1998 to 2003. Prior to entering the academic world, Dr. Snyder worked as a fraud investigator and as an intelligence analyst for the U.S. Army.