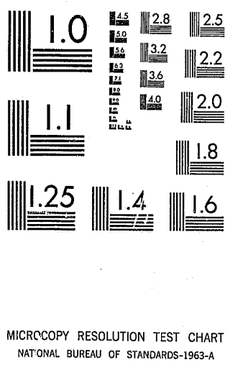

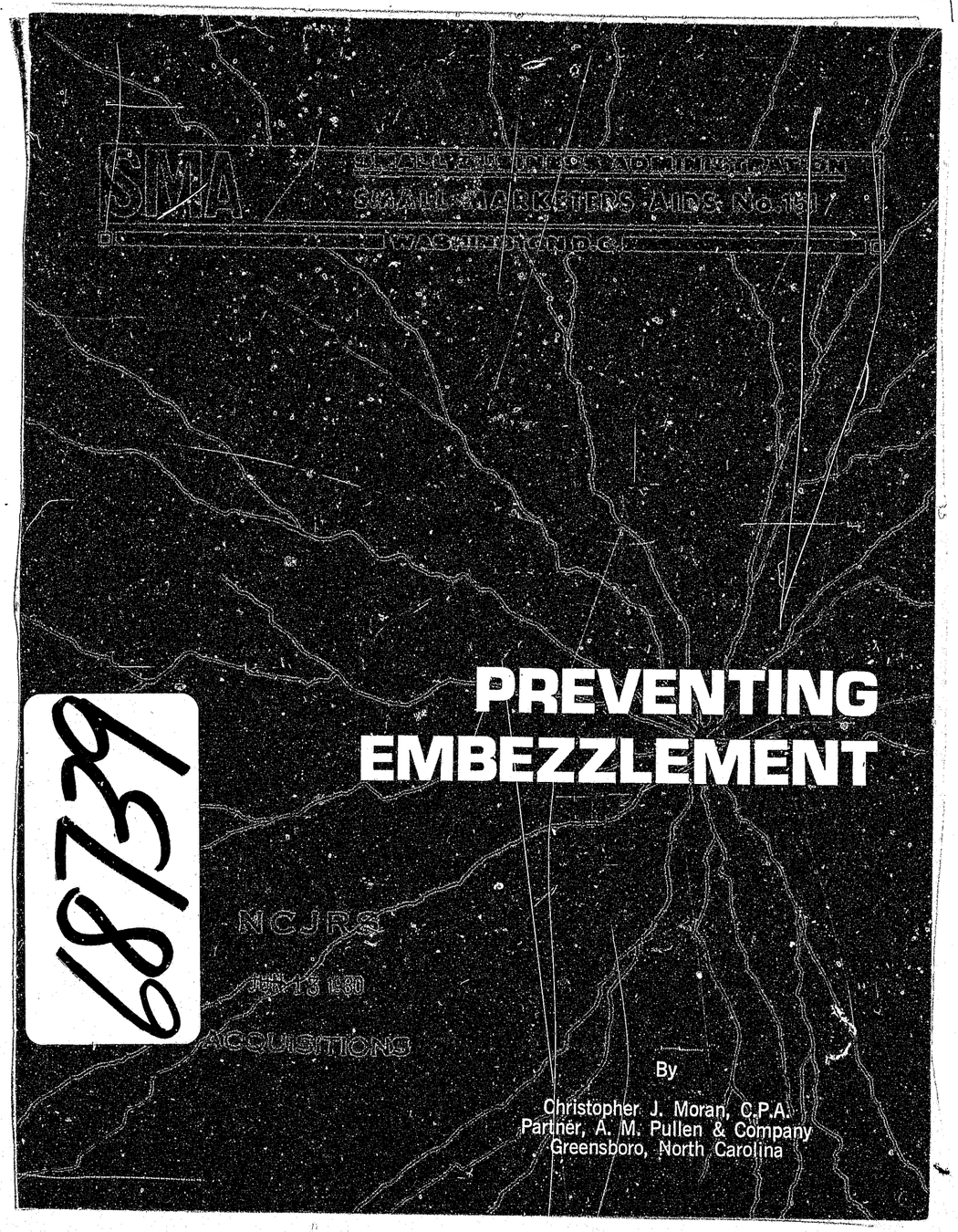

SUMMARY

An owner-manager can lose a great deal of money before even suspecting that embezzlement might be going on. That's because this crime—by definition—is committed by someone in a position of trust. The loss may involve a small amount taken by an employee from the cash register. Or it may be a considerable sum stolen through an elaborate scheme of juggling the books.

Simple controls built into the accounting system can often forestall any such practices in your operation. In any case, the proper internal controls may help document incriminating evidence, without which it is difficult to estimate your loss for insurance purposes or even to prove it resulted from a crime.

This Aid offers suggestions on how an alert businessman can thwart dishonest practices. It also discusses what you should do if it appears that one of your employees has committed the crime of embezzlement.

REVISED
OCTOBER 1977

You may not have had any experience with embezzlers. But many owner-managers have. Every day there are newspaper stories about how some dishonest employee has managed to divert company funds to his or her own pocket. It happens often enough to make it worth your while to give the subject some thought and to examine your recordkeeping and auditing procedures to make sure there are no tempting loopholes.

Embezzlement is "the fraudulent appropriation of property by a person to whom it has been entrusted." The key word is "entrusted." That's what makes this crime different from ordinary theft or larceny. The embezzler is someone in your company that you trust.

You need to have a system of internal control to safeguard money and other property subject to embezzlement. Of course, nobody wants to run his business like an armed camp. But if you have a built-in control system, administer it tightly, and audit it frequently, you may prevent attempts at embezzlement. At any rate, you will have the means to collect evidence that may expose a crime.

The embezzler usually thinks that he is clever—smarter than the owner-manager, and cunnning enough to beat the system. Before you set about to outwit him, it is a good idea to be familiar with some of his methods of operation.

Some Common Schemes

The embezzler is usually a trusted employee who is taking advantage of the confidence his employer has placed in him. In many cases the embezzler has been given more authority than his position calls for. His methods of operation are limited only by the scope of his imagination.

In the simplest situation, cash is received and the employee merely pockets it without making a record of the transaction. A theft of this type is difficult to prevent or detect if the transaction is a cash sale and no subsequent entry is necessary in accounts receivable records. To reduce temptation, prenumbered sales invoices or cash register receipts should be used for all sales regardless of the amount. Spot checks and other monitoring procedures can also help assure you that cash sales are actually being recorded.

A somewhat more complicated type of embezzlement is called lapping. This involves the temporary withholding of receipts such as payments on accounts receivable. Lapping is a continuing scheme which usually starts with a small amount but can run into thousands of dollars before it is detected. For example, take an employee who opens mail or otherwise receives cash and checks as payment on open accounts. He holds out a $100 cash payment made by customer "A" on March 1. To avoid arousing suspicion on "A's" part, he takes $100 from a $200 payment made by customer "B" on March 5. He sends this on, together with the necessary documentation, for processing and crediting to the account of "A". He pockets the remaining $100, which increases the shortage to $200.

As this "borrowing" procedure continues, the employee makes away with increasingly larger amounts of money involving more and more accounts. A fraud of this nature can run on for years. Of course, it requires detailed record-keeping by the embezzler in order to keep track of the shortage and transfer it from one account to another to avoid suspicion. Any indication that an employee is keeping personal records of business transactions outside your regular books of account should be looked into.

Sometimes an embezzler who is carrying on a lapping scheme also has access to accounts receivable records and statements. In this case, he is in a position to alter the statements mailed out to customers. Thus the fraud may continue undetected over a long period of time, until something unusual happens. A customer complaint may spotlight the situation. Or the matter may be surfaced through audit procedures such as confirmation of accounts receivable. One embezzler who also handled the customer complaints was able to avoid detection for many years. The amount of the shortage reached such proportions and covered so many accounts that he dared not take a vacation. He even ate lunch at his desk lest some other employee receive an inquiry from a customer concerning a discrepancy in a statement. The owner-manager for whom he worked admired his diligence and loyalty. His fellow workers marveled that his apparent frugality enabled him to enjoy a rather high standard of living. But the inevitable finally happened. This employee was hospitalized with a serious ailment, and in his absence his fraudulent scheme came to light. One reason many firms require regular vacations is to keep some "indispensable man" from dispensing with company funds illegally.

Sometimes company bank accounts are used for check-kiting. In fact, losses from some large check-kiting schemes have been great enough to cause a company to go broke.

In the usual scheme, the check-kiter must be in a position to write checks on and make deposits in two or more bank accounts. One account could be his

personal account and the other a business checking account. If he has an accomplice in another business, two business accounts may be used. If your company has more than one checking account at different banks, these accounts may be utilized to carry out the fraud.

The check-kiter is taking advantage of the time period (or "float") which is the number of days between deposit of a check and collection of funds. There may be several days between the date when a kited check drawn on bank "A" is deposited in bank "B" and the date the check is presented to bank "A" for payment. Assuming that it takes 3 business days for checks to clear, a simple kite between two banks could be accomplished as follows:

On December 1, a check in the amount of $5,000 drawn on bank "A" is deposited in bank "B". On December 2, the check-kiter cashes a $5,000 check payable to cash and drawn on bank "B" with a teller at bank "B". Since the original kited check will be presented to bank "A" on December 4, the check-kiter on or before that date will deposit a $6,000 check drawn on bank "B" in bank "A" not only to insure payment of the original kited check but increase the amount of the kite. As the process is repeated the kited checks become larger, more cash is withdrawn, and the scheme can continue until the shortage is covered —or until the kite "breaks" when one of the banks refuses to honor a kited check because the funds on deposit are uncollected.

A temporary kite may be used by a dishonest employee to conceal a cash shortage at the end of a period by depositing a kited check in your company account. This brings the bank balance into agreement with the books. C.P.A.'s will request "cut-off" bank statements to detect frauds of this type.

Payroll frauds are yet another source of loss to management. Occasionally an enterprising embezzler has added the names of relatives or fictitious individuals to the company payroll and thus enjoyed several salary checks each week instead of one.

Sometimes, when a company becomes large enough that the owner-manager no longer can exercise personal surveillance of accounting activities, opportunities arise for a dishonest employee to set up a dummy supplier and falsify documentation of fictitious purchase transactions.

Dishonest employees can figure out any number of ways to defraud their employers. Purchasing agents can accept "kickbacks" from suppliers for purchasing goods at inflated prices. Salesmen and others can pad their expense accounts. Personal items can sometimes be bought and charged to the company. Cashiers in retail firms can undercharge relatives or friends for merchandise. False vouchers can be prepared to conceal thefts from petty cash funds. Overtime can be falsely recorded. Moreover, quite substantial amounts of money may be lost through the cumulative effect of such seemingly minor abuses as personal use of company postage stamps, supplies, and equipment, as well as charging personal long-distance phone calls to the business. And so on.

Make Your System Fraud-Proof

The first and one of the most important things an owner-manager should do is to set a good example. Your employees watch what you do and are prone to imitate your habits—good or bad. An employer who pilfers his own petty cash, fudges on his expense account, uses company funds for personal items, or sets other examples of loose business behavior will find his employees rationalizing dishonest actions with the attitude "if it's good enough for the boss, it's good enough for me."

Another important way an owner-manager can discourage embezzlement is by establishing a climate of accountability. Employees should know their jobs and feel trusted. But they should also realize that they are held accountable for their actions. To some people, management indifference in financial administration is a license to steal. That's why it is important for you to examine your procedures and determine what controls can be added to forestall any dishonest practices. And, just as important, the system should be designed to help document evidence in the event someone does try to embezzle your funds. One problem in fidelity loss claims is that of proving the amount that was stolen. The owner-manager has to support his loss claim with evidence—facts and figures that you get from your records.

Reliance for prevention and detection of fraud must be placed principally upon an adequate accounting system with appropriate internal controls that safeguard your assets. Your public accountant can be of great help in setting up a good recordkeeping system. Then it must be tested and evaluated at least annually by the auditor. The purpose of periodic examination is to make sure that there are no loopholes through which an embezzler can manipulate your funds.

One fundamental control is separation of the duties of employees. For example, persons concerned with receiving checks and cash should not also be responsible for the entries in the accounts receivable records. No one person should handle a transaction from beginning to end. If you do not exercise tight control over invoices, purchase orders, discounts, customer credits, and so forth, you are asking for trouble.

You should insist that your accounting system provide you with operating statements issued at least monthly. These will inform you of the operations to date and the firm's financial condition. You can use these documents to compare the figures with prior periods. Any unusual or unexplained variations should be discussed with your public accountant to determine the reason.

Look for Clues

You know how in medicine the symptoms of one disease often resemble those of another. Likewise in business the symptoms, or danger signs, of an embezzlement are often caused by other factors. Here are a few clues which indicate that either an embezzler is at work in your company or certain aspects of the business need more of your attention:

- Increase in overall sales returns could be caused by defective merchandise—or it might represent a concealment of accounts receivable payments.
- Unusual bad-debt write-offs can be due to a number of business reasons—or they could be covering up a fraudulent scheme.
- A decline or unusually small increase in cash or credit sales might mean that business has not been good—or it could mean that some sales were not being recorded.
- Inventory shortages can be caused by error or mismanagement—or they could indicate fictitious purchases, unrecorded sales, or employee pilferage.
- Profit declines and/or increases in expenses can be entirely legitimate—or they could be a sign that cash is being siphoned off illegitimately.
- Slow collections can be caused by business conditions—or they can be a device to mask an embezzlement.

Ounces of Prevention

There are many steps an owner-manager can take to cut down on the possibility of losses through embezzlement. Do you take the following precautions?

1. Check the background of prospective employees. Sometimes you can satisfy yourself by making a few telephone calls or writing a few letters. In other cases, you may want to turn the matter over to a credit bureau or similar agency to run a background check. (Keep in mind that the rights of individuals must be preserved in furnishing, receiving, and using background information.)

2. Know your employees to the extent that you may be able to detect signs of financial or other personal problems. Build up rapport so that they feel free to discuss such things with you in confidence.

3. See that no one is placed on the payroll without authorization from you or a responsible official of the company. If you have a personnel department, require that it approve additions to the payroll as a double check.

4. Have the company mail addressed to a post office box rather than your place of business. In smaller cities, the owner-manager may want to go to the post office himself to collect the mail. In any event, you or your designated keyman should personally open the mail and make a record at that time of cash and checks received. Don't delude yourself that checks or money orders payable to your company can't be converted into cash by an enterprising embezzler.

5. Either personally prepare the daily cash deposits or compare the deposits made by employees with the record of cash and checks received. Make sure you get a copy of the duplicate deposit slip or other documentation from the bank. Make it a habit to go to the bank and make the daily deposit yourself as often as you can. If you delegate these jobs, make an occasional spot check to see that nothing is amiss.

6. Arrange for bank statements and other correspondence from banks to be sent to the same post office box, and personally reconcile all bank statements with your company's books and records. The owner-manager who has not reconciled the statements for some time may want to get oriented by the firm's outside accountant.

7. Personally examine all canceled checks and endorsements to see if there is anything unusual. This also applies to payroll checks.

8. Make sure that an employee in a position to mishandle funds is adequately bonded. Let him know that fidelity coverage is a matter of company policy rather than any feeling of mistrust on your part. If a would-be embezzler knows that a bonding company also has an interest in what he does, he may think twice before helping himself to your funds.

9. Spot check your accounting records and assets to satisfy yourself that all is well and that your plan of internal control is being carried out.

10. Personally approve unusual discounts and bed-debt write-offs. Approve or spot check credit memos and other documentation for sales returns and allowances.

11. Don't delegate the signing of checks and approval of cash disbursements unless absolutely necessary and never approve any payment without sufficient documentation or prior knowledge of the transaction.

12. Examine all invoices and supporting data before signing checks. Make sure that all merchandise was actually received and the price seems reasonable. In many false purchase schemes, the embezzler neglects to make up receiving forms or other records purporting to show receipt of merchandise.

13. Personally cancel all invoices at the time you sign the check to prevent double payment through error or otherwise.

14. Don't sign blank checks. Don't leave a supply of signed blank checks when you go on vacation.

15. Inspect all prenumbered checkbooks and other prenumbered forms from time to time to insure that checks or forms from the backs of the books have not been removed and possibly used in a fraudulent scheme.

16. Have the preparation of the payroll and the actual paying of employees handled by different persons, especially when cash is involved.

If You Suspect a Crime

First of all, be sure that you do not jump to any unwarranted conclusions. What may appear to be an obvious embezzlement may, on further investigation, turn out to have a perfectly valid explanation. A false accusation could result in serious civil liability. There have been cases where employees have been charged by management with embezzlement, dismissed from their positions, and later found to be entirely innocent.

But if you have good reason to suspect embezzling, contact your attorney immediately. Be guided by his advice on how to proceed. Discuss with him the necessity of notifying the bonding company and appropriate law enforcement authorities. Follow his advice in matters regarding prosecution so that you will not subject yourself or your company to charges of false arrest.

Don't subject yourself to criminal charges by helping conceal the commission of a crime. Embezzlers should be prosecuted when the facts so warrant and when there is a sufficiency of evidence. These and other legal questions are best left to your attorney.

Computer-Related Embezzlements

The news media have given a lot of publicity to computer-assisted frauds and embezzlements. The computer crimes receiving this publicity are usually complex and give the impression that computer-related frauds can be committed only by highly skilled technicians using sophisticated computer systems. This could create a false feeling of security for owner-managers who use less sophisticated systems or service centers for processing their records.

A recent study by the U.S. General Accounting Office of Computer-Related Crimes in Federal Programs disclosed that most computer-related crimes were committed by people with limited knowledge of computer technology. Most cases

resulted from preparation of false input data to computer-based systems. Neglect of control on input is a weakness. You should have your outside accountant review your controls and strengthen them if needed.

To Sum Up

There are three principal ways in which an owner-manager can minimize the possibility of embezzlement losses. None is completely effective without the others.

Internal controls are perhaps the most effective safeguard against fraud, but even the best precautions can't make it absolutely impossible.

Independent audits discourage fraud and may uncover it. But they can't, as some people mistakenly believe, guarantee disclosure of all irregularities.

Fidelity coverage can help you recover what may be lost in spite of your best efforts to prevent embezzlement.

FOR FURTHER INFORMATION

Business owners who wish to explore this subject further may consult the following references. The list is necessarily brief. However, no slight is intended toward authors whose works are not mentioned.

Embezzlement Controls for Business Enterprises by Lester A. Pratt, C.P.A. Available free from Fidelity and Deposit Company, Baltimore, Md. 21203.

Computer-Related Crimes in Federal Programs. FGSMD–76–27, April 27, 1976. May be purchased from Government Accounting Office, Distribution Section, P.O. Box 1020, Washington, D.C. 20013.

A Handbook on White Collar Crime. Chamber of Commerce of the United States. 1974. May be purchased from the Chamber of Commerce of the United States, 1615 H Street, N.W., Washington, D.C. 20006.

In addition, the following publications on the subject of crime in business may be of some interest. These *Aids* are available free by writing to the Small Business Administration, Washington, D.C. 20416 (or contacting your nearest SBA office).

"Preventing Employee Pilferage," *Management Aids* No. 209.
"Preventing Retail Theft," *Small Marketers Aids* No. 119.
"Reducing Shoplifting Losses," *Small Marketers Aids* No. 129.
"Preventing Burglary and Robbery Loss," *Small Marketers Aids* No. 134.
"Outwitting Bad Check Passers," *Small Marketers Aids* No. 137.

U.S. GOVERNMENT PRINTING OFFICE : 1979—O-288-728

END