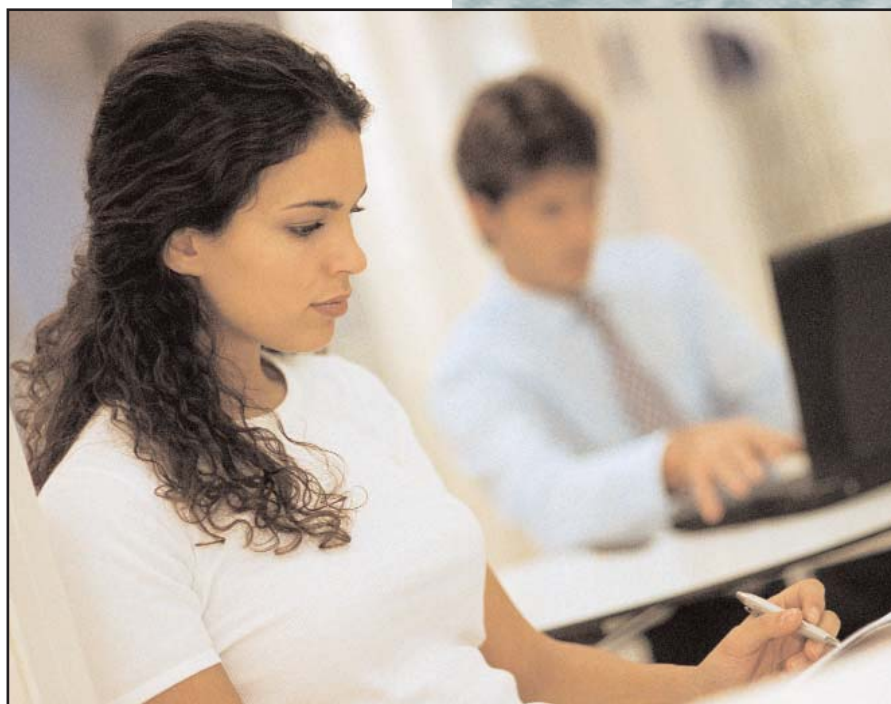


Irwin Siegel Agency, Inc.
Human Service Program
Risk Management Division

Employee Dishonesty



Supporting Those Who Support Others™

Employee Dishonesty

Table of Contents

Prefacei

Employee Dishonesty Mythsii

Prevention1

Management’s Role2

Hiring Staff3

Supervision4

Audits5

Accounting Controls6

Mail Controls12

Controlling Access to Keys13

Payroll Controls14

Corporate Funds and Securities15

Could This Happen to Your Agency?.....18

Conclusion.....22

Sources23

About the Irwin Siegel Agency, Inc.25

Preface

Employee dishonesty can range from theft of petty cash or supplies, stealing money through fictitious vendors or employees and embezzlement, to theft of consumer (client) funds and misuse of the organization's corporate credit card. It can be damaging to any business, but for nonprofits that rely on donations and funding, it can be especially devastating. It poses a threat to the nonprofit provider's reputation, quality of programs and even its viability. Although most organizations prefer to believe that their employees would never steal, some employees do steal, and organizations need policies in place to address this fact.

This resource was created to support human service providers' efforts to guard against and deal with employee dishonesty. It presents best practices against which organizations can assess their policies, procedures and internal controls, and it identifies corrective measures that providers can use to reduce or eliminate exposures relating to employee dishonesty. Armed with the results of their assessments and the 'Best Practices' in this booklet, providers can form their own strategic plans to close gaps and strengthen weak spots that offer the temptation and opportunity for theft. While this resource cannot include every possible situation or control, it will provide a starting point for responding to the most common exposures. As a second benefit, many of these same improvements will also help the user to reduce or catch honest errors that are costly, inconvenient or just plain embarrassing.

Employee dishonesty can range from theft of petty cash or supplies...to theft of consumer (client) funds and misuse of the organization's corporate credit card.



Employee Dishonesty Myths

Before discussing prevention, it might be helpful to dispel some of the myths that surround the subject of employee dishonesty and replace them with useful facts.

Myth	Fact
Only commercial entities are vulnerable to employee theft.	Every organization has financial or material assets that create exposure to the risk of employee theft.
Employee theft is simply a cost of doing business.	Employee theft is a crime that can threaten an organization's budget, reputation and viability.
Employee theft is costly only if it continues for a long time.	Employee theft can reach significant amounts in just a few weeks or months.
New employees are more likely to steal than long-term staff.	There is no basis for this assumption. In fact, long-term staff are just as likely to steal from your agency and are more familiar with your control system.
Beyond pre-employment screening, annual audits and hoping for the best, there is little an agency can do to predict and prevent honest mistakes, theft by fraud or embezzlement.	This resource presents many low and no-cost practices that employers can use to reduce the temptation, opportunity and success of attempts by employees to steal agency dollars.

Every organization has financial or material assets that create exposure to the risk of employee theft.



Prevention

What can you do to prevent employee dishonesty in your agency?

You cannot predict whether an employee will steal from your organization. You can, however, develop certain controls that may reduce temptations, limit opportunities, and make it difficult for attempting thieves to succeed. As an added benefit, these same controls will also help the organization to catch some of the honest mistakes that people may make when handling the organization's funds or materials.

Task Distribution

With high turnover rates, understaffed agencies often fall back on the remedy of assigning multiple related duties to one individual. Unfortunately, this removes one of the strongest barriers to theft, and it has the unpleasant side effect of making it harder to detect discrepancies.

Distributing the steps of each process among several employees accomplishes a number of things. It makes it more difficult for any person to engage in or hide theft, because no individual has sole access to all of the steps. This method will also catch innocent mistakes, because each person will review the previous person's work before proceeding with his or her own. While it may seem difficult to distribute related duties among several people, it remains one of the simplest, least expensive and most effective risk management tools.

More Internal Controls

Each agency can 'manufacture' its own internal controls based on its services and delivery. These should be based on your own assessment of your agency's potential loss areas and may include a combination of management support and supervision, audits, task distribution, restricted/monitored access, Generally Accepted Accounting Principles (GAAP), and any other measures that respond to the particular risks facing your agency.

Each agency can 'manufacture' its own internal controls based on its services and delivery.

Five Keys to Preventing Employee Dishonesty

1. Management support and supervision.
2. Audits.
3. Distribution of tasks among several employees.
4. Restriction/monitoring access to mail, receivables, supplies and other assets.
5. Following Generally Accepted Accounting Principles (GAAP).



Management's Role

This is an ideal opportunity for management to take the lead in promoting a culture of honesty and professionalism. By creating, following and enforcing policies and procedures, management sets standards for integrity and accountability that employees are more likely to follow.

Written procedures for approving and conducting financial transactions are crucial to maintaining efficiency and establishing accountability. Managers also have the responsibility of reviewing reports, questioning negative trends and resolving discrepancies. Many dishonest schemes succeed simply because management does not follow these practices.

Managers should perform best employment practices by documenting the duties that each employee performs. The connection among performance evaluations, job descriptions and risk may be less obvious, but it does exist and it's worth exploring. An employee's duties can change casually for the sake of convenience or because of another employee's promotion, resignation or illness. If an employee is performing a duty on an informal or interim basis, it should not mean that lesser standards of reliability and competence apply. Management must ensure that an employee is trustworthy and capable of completing a task. Management must also follow up by documenting the details of the new task(s) in the employee's file to establish accountability.

Managers must both follow and enforce their organization's policies and procedures. When policies are violated, disciplinary actions need to follow. This could include suspension, termination, additional training and supervision, etc. Be certain that the discipline fits the violation, is stated in the employee handbook, and is applied to all employees consistently.

Establishing a written Code of Ethics for your organization is also a good measure to reduce employee dishonesty. It should include how and when to report improprieties or conflicts of interest, what the appropriate uses of company assets are, what appropriate gifts are, and should specify the maximum value of any gifts. Also, be sure to outline the consequences for breach of policy and distribute it to all employees.

Managers should perform best employment practices by documenting the duties that the employee performs.



Five Management Behaviors that Promote Honesty

1. Lead by example in setting standards for integrity.
2. Review reports formally and at random to spot discrepancies and to maintain a trail of accountability.
3. Review job descriptions and performances to keep employees accountable and their records current.
4. Enforce all policies, procedures and disciplinary actions consistently and in accordance with the Employee Handbook.
5. Establish and reinforce a written Code of Ethics.

Hiring Staff

Facts:

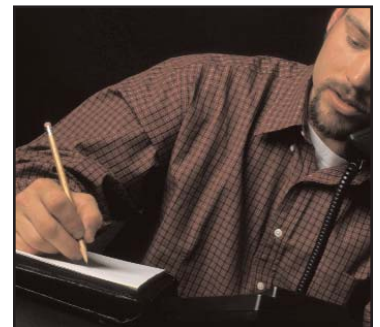
30 percent of all employment applications are falsified and 45 percent of all resumes contain deceptive information regarding education, skills and accomplishments. One in 20 applicants concocts a name, social security number and/or driver's license number to hide previous convictions. To avoid the risks to staff and consumers, related legal expenses and damage to reputation, employers must complete background checks.

Care needs to be taken in the hiring of or transferring of staff to positions of care, custody or control of agency funds or assets. Have every prospective employee fill out a job application that authorizes you to perform a thorough background check and follow through on it. Most employers ask applicants for personal and work references but skip the crucial step of verifying them. When calling former employers, call the main number instead of direct lines that may be inaccurate. It is equally important to verify credentials, such as degrees and certificates, at the source.

You should conduct multiple interviews that include more than one supervisor or manager. This will give you different perspectives from which to evaluate the candidate's demeanor, attitude, responses and other 'intangible' but important elements in determining whether or not to hire the person.

When considering applicants who will have access to checks, purchase orders, company credit cards and other high-risk areas, it is better to be overly cautious

Have every prospective employee fill out a job application that authorizes you to perform a thorough background check and follow through on it.



than too lax. Perform background, criminal and credit history checks for applicants who are under serious consideration for hire. If the job involves access to high-risk areas, it may be worth hiring a professional who specializes in performing such investigations. Finally, use caution regarding applicants who are overqualified, have a declining salary history, or have gaps in residence or employment.

Five Best Hiring Practices

1. Use applications that include authorization to check references and follow through on them.
2. Verify credentials.
3. Conduct background, criminal and credit history checks.
4. Interview candidates more than once and have input from at least one other manager/supervisor.
5. Be cautious of applicants who are overqualified, have declining salary histories, or have gaps in their places of employment or residence.

Supervision

Providing employees with adequate supervision is essential to the accuracy of the tasks that they perform and to agency accountability and loss control. Train employees on policies, procedures and approval processes for all transactions related to the organization's funds and other assets to reduce mistakes. No one wants to follow instructions blindly. Telling staff why a particular policy exists is as important to good training as telling them what to do and how to do it.

Train employees on policies, procedures and approval processes for all transactions...



Cross training allows employers the flexibility to rotate duties among several employees, to improve accuracy, and to avoid the trap of the 'indispensable' employee. In addition to the obvious problems and mistakes that will occur when this person is absent, consider this: if no one else knows how to do this employee's job, how can anyone else be sure that (s)he is doing it honestly, or even correctly?

Require employees, particularly those who have care, custody or control of the organization's funds or assets, to take vacations of at least five consecutive days. This practice may deter employees from becoming involved in dishonest schemes, and it provides a chance to rotate duties and conduct audits.

Employees are often aware of theft, fraud, abuse or noncompliance, but are afraid to report it for fear of repercussions. Establish reporting procedures that provide staff with at least two means of reporting dishonest acts, and notify all staff of the procedures. When reports are received, document and investigate them. Ask your legal counsel for advice on how to proceed with any confirmed dishonest acts.

Five Supervisory Practices to Reduce the Risk of Employee Dishonesty

1. Train and Explain - Tell employees what, how and why.
2. Cross train.
3. Review reports and resolve discrepancies.
4. Require vacations of at least five consecutive days.
5. Establish and inform employees of at least two ways to report dishonest acts.

Audits

Prevention and detection of dishonest acts require adequate accounting systems with appropriate internal controls. Those controls include a system of checks and balances to discourage dishonesty. Audits are a control and a way of measuring the success of other controls. Provider organizations should conduct internal and external audits of their funds, products, materials and services.

External Audit

An independent, certified public accountant should conduct an audit every year. As (s)he audits each department, (s)he should consult with the department head and make a final comprehensive report to the Executive Director, Fiscal Officer and Board of Directors.

Keep in mind, however, that external audits only show errors or irregularities that are material to the auditor's review. If internal controls are insufficient, even an outside auditor may fail to identify a fraudulent transaction. The auditor may notice and investigate questionable transactions, but if there are no internal policies and procedures against which (s)he can check them, the fraud or mistakes could continue undetected. You should ask your external auditor to identify deficiencies in your controls and suggest corrections. If (s)he makes recommendations, review and act on them. Be sure to have someone accountable for the implementation and documentation of the controls.

Audits are a control and a way of measuring the success of other controls.



Internal Audit

The organization should develop a written, internal audit program to promote efficiency and protect corporate assets from misappropriation. Organizations with enough staff can assign officers from different departments to periodically spot audit each other's records. Internal auditors should report to an Audit Committee or the Board of Directors. The internal audit should include monthly reconciliation of accounts receivable and accounts payable by someone other than the person(s) normally responsible for maintaining these records. Confirm that cancelled checks are in chronological order, none are missing, none violate signature or other policies, and that the endorsements are correct. Audit daily cash receipts and deposits, payroll, physical inventory and stock records monthly. Review samples of each type of transaction to ensure that they were appropriately approved and documented. Review invoices and contracts to certify that service or merchandise was authorized and the charges were fair. Scrutinize reconciliation documents for any unusual transactions. In addition to scheduled auditing activities, conduct unannounced spot checks and visits to all locations at regular intervals.

Accounting Controls

The foundation for good internal accounting controls is segregation of duties. This means that different employees handle each of the individual steps of any transaction. For example, if it takes four steps to issue a payment, there should be four people involved. The first person requests payment, the second person approves the payment, the third person draws the check, and a fourth person signs it. A fifth person, who has no part in the first four steps, should reconcile the accounts. If the organization is small, this could mean separating duties between a few people. For large organizations, this could mean spreading the duties out among several departments, committees and/or an outside consultant.

Audit daily cash receipts and deposits, payroll, physical inventory and stock records monthly.

Checks

Restrict the authority to request checks to certain person(s) in each department, subject to approval. The authority to draw checks should be limited to just a few people and none of them should have signatory authority. When an employee exceeds his/her authority in any of these areas, document and investigate it.



The person who issues checks should be different from the people who approve the payment, sign the check, and reconcile the account. On each check stub, write the invoice or other reason for payment and on every invoice, write the check number. This cross-referencing will prevent duplicate payments for the same invoice.

Require two signatures on all agency checks. Consider using three signatures for checks over a certain amount. If additional signatures are not possible, agencies can use a voucher system where payment requests must be approved before payment.

Arrangements with financial institutions should include written notices, samples of authorized signatures, and instructions not to cash checks that do not carry the required signatures. Secure check writing machines, facsimile signature plates and signature stamps to prevent misuse.

Unissued checks should be pre-numbered and stored in numerical order in a locked file cabinet or similar secured box. Inspect checkbooks to ensure that checks are not missing from the back of the book. Tear off the signature areas of voided checks and retain them along with a log to record the reason for the void, and audit both periodically.

Periodically review cancelled checks to confirm that they are in sequential order and have authorized signatures and endorsements. Report alterations or improprieties internally and to the bank, and investigate outstanding checks and deposits that have not cleared. Policies should include steps to verify that outstanding checks have not been cashed and to place stop payments on them when necessary.

Check Controls

1. Restrict authority to request, approve, draw and sign checks.
2. Segregate these duties.
3. Investigate and respond to instances of exceeded authority.
4. Cross-reference invoices and check numbers.
5. Require two signatures and file them with the bank.
6. Secure unused checks and signature stamps.
7. Review cancelled checks for correct signatures and endorsements.
8. File and log voided checks.

Inspect checkbooks to ensure that checks are not missing from the back of the book.



Incoming Receipts and Bank Deposits

When mail is opened, stamp all checks “For Deposit Only” immediately and record all checks in the agency’s accounting books. Deposit all receipts to the organization’s bank account promptly. Use pre-numbered deposit tickets or logs when processing cash receipts and require the processing person to initial or sign the ticket or log. Consider writing the deposit number (or the last four digits) on

every check to help resolve incorrectly posted payments or other errors. Limit access to the agency's signature stamp.

Deposit all cash receipts in full without any adjustments. Make any reductions or withdrawals for petty cash, etc. as separate transactions and document them accordingly.

Six Procedures to Bank on for Incoming Receipts and Deposits

1. Stamp all checks 'For Deposit Only,' log them and deposit them promptly.
2. Write the deposit ticket number on each check.
3. Limit access to the agency's endorsement and signature stamps.
4. Secure the deposit until it is delivered to the bank.
5. Assign a different person to verify the bank's deposit receipt against your log.
6. Resolve errors immediately.

Store receipts awaiting deposit in a locked file cabinet or similar safe box to prevent theft, loss or accidental destruction. Compare the bank's deposit receipt with your deposit slip or log, and require the person making the comparison to initial or sign the deposit sheet. Immediately investigate and resolve rejected deposits and require that the investigator be someone other than the person who posted the payments or prepared the deposit.

Disbursements

Match packing slips and other shipping and receiving documents to their respective invoices to confirm that purchases are appropriate and that billed goods or services have actually been received.

Immediately investigate
and resolve rejected
deposits...



The Board of Directors should periodically review the authority limits for payments to ensure that they meet the needs of the organization. Those authorized to sign payments should review such transactions to ensure that both the purchase and the payment have been appropriately authorized. The reviewer should also verify that disbursements are made in the correct amount, for the correct period, to the correct account, and that all information is recorded properly.

Payments and Disbursements

1. Match shipping/receiving documents to invoices.
2. Confirm that purchases are appropriate and properly authorized.
3. Have the Board of Directors review limits of authority.
4. Verify amount, time, account numbers and authorization for payment/purchases.

Cash

Secure cash and petty cash in separate, locked boxes and store them both in a locked filing cabinet or other secure area. Establish a petty cash fund with a low dollar amount and use it only for minor purchases. Minor purchases do not necessarily have to be inexpensive, and in the same respect, major purchases may not be expensive. For this reason, a statement of use for petty cash should be established that describes its proper use. A statement would prevent misinterpretation of what petty cash can and cannot be used for. For example, a signature stamp may not cost much more than a book of ordinary postal stamps, but from a risk management standpoint, it is a major purchase and no one should be able to buy one from petty cash funds. **Short-term lending or cashing of personal checks should be prohibited.**

Employees should support every request for petty cash with documentation such as a sales receipt and a petty cash voucher signed and dated by the person who requested payment and the person who disbursed the funds. Mark vouchers and cash requests 'cancelled' to prevent re-use and record the transactions in a ledger.

Replenish petty cash through an established procedure that includes documentation and signatures. Monitor the frequency of petty cash replenishment to confirm that the fund is reasonable and being used as intended. Someone other than the petty cash supervisor should check the fund and balance the records. When transferring funds from one location to another, two employees should be assigned to signing the funds in and out of each location.

Corporate Credit Cards

Use caution and logic when creating your credit card policies. **Provide cards only to those employees who need them and follow the best practices mentioned earlier in this booklet for hiring employees who will be using corporate cards.**

A statement of use for petty cash should be established that describes the proper use of petty cash.



It may seem obvious, but state in the policy that the agency's credit card is solely for business-related expenses, that all other expenses are the responsibility of the employee, and that the agency and the employee using the credit card should keep card numbers and expiration dates confidential. It is also a good idea to specify the consequences of violating the policies.

Enforce an approval process for expenses, such as pre-authorization of expenses, and give a specific time limit for receipts and authorization forms to be turned in to the person responsible for reconciliation of the account statement. This person should reconcile credit card statements each month against the receipts and expense authorizations.

Managing Cash

1. Keep petty cash secure and separate from other cash.
2. Keep the petty cash fund small and use it for minor purchases.
3. Don't use petty cash as a personal loan fund or personal check cashing service.
4. Require documentation for all petty cash payments or cash advances.
5. Follow a process for replenishing the funds.
6. Someone who is not responsible for maintaining the funds should conduct scheduled and random reviews.
7. Use two employees to sign cash in and out of each location.

Assign someone else to monitor the use of corporate credit cards and look for any unusual items and personal usage. Give both these employees a procedure for reporting and resolving discrepancies.

When an employee resigns or is terminated, confiscate and destroy his/her credit card(s) and notify the issuer of the card immediately, so that they may cancel the card number. Use the same procedure for lost or stolen cards. Secure unassigned cards in a locked file cabinet or other secure box with limited access.

...separation of duties is a best practice.



Account Reconciliation

Again, separation of duties is a best practice. The person who reconciles the account should be different from the person who approves the payment, issues the check or signs the check. Reconcile accounts as soon as bank statements arrive and promptly investigate and resolve any differences between statements and internal records. Any necessary adjustments should be documented, authorized and recorded.

Seven Steps of Credit Card Logic

1. Issue cards only as needed and screen all employees who will have access.
2. Have and follow clear-cut policies. Make sure employees know the policies.
3. Require documentation within 30 days for all charges.
4. Reconcile credit card statements against documentation before making payment.
5. Monitor card use for unusual or personal expenses.
6. Secure and limit access to unassigned cards.
7. Confiscate cards of employees who resign or are terminated. Notify the credit card company to invalidate the card. Do the same for lost/stolen cards.

Maintain a list of current cash accounts, including the name, address and telephone number of the financial institution, the type of account, names of authorized signatures for the account, and any restrictions, such as the number of signatures needed on checks. Match monthly statements to this list. If a bank or credit card statement is missing, contact the financial institution immediately.

Account Reconciliation

1. Reconcile bank statements when they arrive.
2. Resolve and document discrepancies.
3. Verify that all monthly statements are received. If one is missing, contact that financial institution.

Property

Risk of loss from inventory can be very high, especially when your agency warehouses or manufactures items. Loss can occur through employees, truck drivers and vendors. Providers will find, however, that best practices for this area are simple and effective.

Schedule deliveries and place inventory in secure locations. Investigate discrepancies and inexplicable trends in inventory levels, such as an unusual increase in the number of items reported damaged, and institute random inventory checks. Remember to screen employees who will be responsible for counting goods, both on the shipping and receiving sides. Someone who does not have control of the property should conduct a complete annual inventory and periodic spot checks of the agency's raw materials, goods in process, finished

If a bank or credit card statement is missing, contact the financial institution immediately.



products, machinery and equipment. (S)he should have clearly defined avenues for reporting discrepancies.

Five Inventory Controls

1. Restrict access to property, deliveries and inventory.
2. Investigate trends.
3. Perform random and scheduled inventory checks.
4. Screen employees in shipping/receiving.
5. Assign someone not involved in inventory to conduct annual inventory and random spot checks.

Mail Controls

Assess your procedures for handling mail; how your organization processes its mail can either increase or decrease exposure to risk in this vulnerable area. It is easy to perpetrate and conceal dishonest schemes by intercepting mail as it moves through your facility. **The best risk management tools are ensuring accountability, limiting access, and choosing mail handlers with care.**

Use a post office box to limit access and establish accountability for incoming mail right at the source and assign one trustworthy person to pick up incoming mail from the post office. Use the same strategy when delegating the job of sorting and delivering incoming mail throughout the building, and do the same for outgoing mail. **Include these responsibilities in job descriptions and assign alternates for these tasks to avoid a casual “substitution.”**

Use a post office box to limit access and establish accountability for incoming mail...

As mail is opened, one person should list all the cash and checks received and a different person should review the list and the accompanying cash and checks. Divide the tasks of posting payments, proving deposits to the original list, and preparing the banking in the same way.



Arrange for bank statements and other bank correspondence to be sent to the post office box. If a statement is missing, contact the bank immediately for a new copy.



Triple Ifit Mail Controls

- Assessment:** Know what kinds of mail you receive, who has access to it, and how it is processed now.
- Accessibility:** Limit access by using a P.O. Box and assigning one person and one alternate to each step in handling and processing mail.
- Accountability:** Ensure accountability by including these responsibilities in job descriptions.

Controlling Access to Keys

It is crucial to know who can gain access to offices and how. The more people who have keys, the less control you have over security. Issue keys only to those who *require* access. Keep unassigned keys in a locked box and follow a sign in/sign out system for keys that are not routinely kept by specific staff members. Change combinations and locks at least annually and whenever an employee with access is suspended or terminated.

Designate at least one staff person to maintain an inventory of all keys and review it on a regular basis, at least annually. The inventory should include the key number, name of person to whom the key was issued, his/her position and date of issue. Also keep a list of who is authorized to order replacements. This should be a short list!

Instruct staff never to leave keys out, in a drawer, purse or coat pocket, and instruct them to report lost or missing keys immediately. If any key is missing and cannot be found, replace the lock, even if there is a spare key on hand. Investigate and document the issue.

Designate at least one staff person to maintain an inventory of all keys...



Eight Ways to Keep Keys Secure

1. Know who has access to offices.
2. Keep keys in a locked box.
3. Have a sign out/sign in procedure.
4. Inventory keys regularly.
5. Know who has authority to order replacements.
6. Change locks and combinations when someone who had access is terminated or suspended.
7. Remind staff to keep keys in a secure place at all times.
8. Replace the locks if a key is missing, even if you have a spare key.

Payroll Controls

Because handling payroll accounts is so complex and requires specialized knowledge, the opportunities to act dishonestly and to make innocent errors are both increased. There are several steps organizations can follow to reduce the chances of either happening, and the wise risk manager will initiate as many as possible.

Begin by making sure payroll receives accurate information from the start by requiring employees and the appropriate supervisor to approve and sign time sheets and attendance records. **Supervisors should review time sheets to ensure they accurately reflect use of vacation, sick leave or other time off, before forwarding them to payroll.** Note that the supervisor, rather than the employee, submits approved time sheets to payroll, where they are reviewed for errors or illicit alterations. Payroll staff will investigate and resolve any errors before they pay the employee.

Payroll staff will investigate and resolve any errors before they pay the employee.



Within the Payroll Department, different people should handle attendance and time records, payroll preparation, the signing of payroll checks, and reconciling payroll accounts. The appropriate supervisor should pre-approve requests for overtime pay, and the checks for bonuses, overtime, etc. should be made out only to the persons for whom they are intended, never for “Cash.” Secure unclaimed paychecks in a limited access file cabinet or safe.

Know who is responsible for preparing payroll forms, properly documented time sheets, attendance records and other approved time reporting records and have a review system in place for these items. This system should require employees with access to payroll records to take annual vacations lasting at least five working days during which you can audit records. Reviews should also include periodic head-counts to prevent payroll padding, overstating payroll checks, or issuing unauthorized checks to nonexistent or terminated employees.

Notify the Accounting Department or payroll service promptly of all additions or deletions from payroll. On the executive level, the Director should review and approve all changes to payroll, and the Board of Directors should review and approve any changes in staffing levels and overall compensation scale.

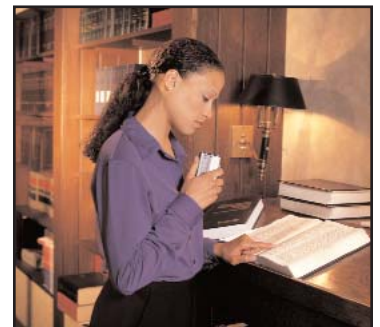
Seven Payroll Controls

1. Supervisor reviews straight and overtime hours and vacation/sick time.
2. Supervisor and employee sign timesheet; supervisor forwards to payroll.
3. Payroll duties are separated; accountability for each task is documented.
4. Payroll staff members take at least one, five-day vacation yearly.
5. Payroll receives prompt notice of payroll changes.
6. Executive Director reviews/approves payroll changes.
7. Board of Directors reviews/approves changes to staffing levels and compensation.

Corporate Funds and Securities

A designated committee should make decisions regarding purchases, sales and transfers of corporate investments and assets. The person who executes the transactions has to be trustworthy and held accountable. Several times a year, conduct inventories of securities under the joint control of several officers and/or employees. **Persons involved in the joint control of securities should not conduct the inventory.**

...the Director should review and approve all changes to payroll...



Corporate Funds and Securities

1. Committee decides all transactions.
2. Employees are screened and held accountable.
3. Annual inventories performed by several officers/employees other than those who control the securities.

Handling Consumer (Client) Funds

Control of Funds and Informed Consent

Clients/consumers should control their own funds to the greatest extent their abilities permit. The consumer and his/her interdisciplinary team should participate in assessments that will determine that ability. The consumer and his/her interdisciplinary team should also participate in any decision regarding the handling of the consumer's funds. Consumers should receive money management training that supports their abilities and have access to facts about their finances so they can make informed decisions.

If it is determined that the consumer is not capable of full financial control, provide support as needed to protect the consumer's best interests and involve the consumer and interdisciplinary team in any decisions. Provide full support in controlling consumer funds if the determination is made that the consumer is not capable of any control.

Accountability

Someone other than the person who provides money management support or has direct access to consumer funds should reconcile all consumer fund accounts.

The Bookkeeping/Accounting Department should reconcile all consumer funds quarterly. All employees who are responsible for handling consumer funds should submit expense/financial reports regularly, which should include receipts to validate each expense.

Consumers should receive money management training that supports their abilities...



Handling Consumers' Funds

1. Consumer Control

Consumers should have as much control over their own funds as their abilities permit.

The consumer and his/her interdisciplinary team determine those abilities and agree on appropriate supports.

2. Informed Consent

Consumers should have the facts they need to make informed decisions about their finances.

3. Accountability

Staff members who have access to consumer funds must submit financial reports/receipts regularly. The individuals who reconcile consumer accounts are not the same ones who provide money management support or have direct access to consumer funds.

The Bookkeeping/Accounting Department should reconcile all consumer accounts quarterly and address discrepancies.

Think It Over

No agency can guarantee that it will never have a dishonest employee in its midst, but agencies that implement appropriate controls can say with confidence, "We took all possible steps to protect our organization and monitor our employees' actions in order to prevent thefts and correct honest mistakes promptly." Beyond protecting your organization's reputation and fiscal health, there are other reasons why nonprofit organizations need to follow best financial management practices. For example, in cases of employee theft, the organization must be able to support any administrative/disciplinary actions it takes based on allegations of dishonesty. Remember, that the ability to make the above statement and back it up with documentation will be vital to your defense if your agency is sued because of your employee's alleged financial mismanagement or wrongdoing.

The truth is, nonprofit human service providers don't need to ask if they are vulnerable to employee dishonesty; they need to ask where and how theft might occur, and what they can do to protect their agencies from that risk. Any successful risk assessment begins with asking the right questions and finding the correct answers. The following case studies are based on facts from actual claims and are intended to give providers a strong start in managing employee dishonesty.

Any successful risk assessment begins with asking the right questions and finding the correct answers.



Could This Happen to Your Agency?

Case Study #1

Consider the case of the ABC Agency, Inc., a provider agency whose Accounts Receivable Manager embezzled several hundred thousand dollars from the organization.

Background

The ABC Agency, Inc. hired Denise Estgal as the head of its Accounts Receivable Department in September. The provider agency conducted a background investigation using the name, social security number and driver's license number that Denise Estgal supplied. The agency also checked her references. Both the references and background checks were so satisfactory that it didn't bother with a criminal investigation. ABC hired Ms. Estgal, but within four weeks the agency terminated her because of poor work performance.

What Happened

After being hired, Ms. Estgal opened a bank account with Dupe Bank, a bank with which the provider agency did not do business. She did this by using an altered version of the agency's legal name, a fake Federal ID Number and a forged Corporate Resolution Charter. With all that in place, it was easy for her to buy signature and endorsement stamps. As Ms. Estgal processed payments from the agency's customers, she endorsed the checks with her stamp and deposited them into her account at Dupe Bank. Later, Ms. Estgal would make untraceable cash withdrawals from that account.

No agency can guarantee that it will never have a dishonest employee in its midst...



Soon after Ms. Estgal was terminated, the ABC Agency began sending out past due notices to its customers. When the customers replied with copies of their cancelled checks and a few sharp requests that the agency 'get its act together,' the agency began combing its records for some explanation. It soon realized that the embezzlement occurred over a one-month period - the month that Denise Estgal had been employed.

Digging a little deeper, the agency learned that Ms. Estgal had provided a fake name, social security and driver's license numbers and fake references. Denise Estgal turned out to be Judy Smith, a professional con artist with a dismal history of embezzlement, armed robbery and attempted escape from prison.

The Lesson

ABC's first mistake was skipping the criminal background check. A professional investigator might have discovered Ms. Smith's identity and history. Second, because Ms. Smith had unchecked access to all steps in the accounting process, she was free to process, record and deposit payments as she chose and then cover her tracks by "forcing" reconciliation of the bank statements. If her employer had followed the best practice of assigning each step to a separate individual, this fraud would have been impossible to commit. As a Department Manager, Ms. Smith would still have access to all of these functions, but she would not have had sole responsibility for them. There would have been at least four other "pairs of eyes" involved - one to log payments, one to post them, another to do the banking and a final person to reconcile the accounts. One or more of these individuals would have caught and questioned the discrepancy.

The Cost

This lesson had a painful price tag of \$363,000 compounded by loss of funders' support and consumers' good will. After Ms. Smith was apprehended, someone from the agency had to participate in the criminal court proceedings if Ms. Smith was to be prosecuted successfully. While the agency could stand a good chance of winning a criminal case against Ms. Smith, there would be little or no hope of the funds being recovered. All of these legal proceedings added substantially to the loss in the form of legal fees and hours lost.

Case Study # 2

Another high risk of theft comes with the handling of client funds. Provider agencies often entrust an individual with the responsibility of overseeing these funds, and in the case of FGH Agency, a group home manager stole \$50,000 from the clients.

Background

Bill Brown was hired as a Group Home Manager for the FGH Agency and worked for the agency for many years. Before hiring Bill, the agency conducted a background check and criminal investigation that showed no prior convictions.

What Happened

Bill was responsible for collecting payment for room and board fees from the consumers living in his group home. He was supposed to forward the payments to FGH. Bill also had check writing authority for the consumers' checking accounts, and he maintained all records relating to those accounts.

Another high risk of theft comes with the handling of client funds.



The agency began investigating when the consumers' housing accounts went into arrears, and Bill refused to submit his records to reconcile the accounts. He later admitted to writing checks from the consumers' accounts and cashing them for himself. He also confessed to pocketing the consumers' room and board money. He told the agency that he was "normally an honest person" but that he had gotten heavily into debt.

The Lesson

Employers must rely on a system of checks, balances and reviews in order to minimize the possibility of employee dishonesty. No one should have uninterrupted responsibility for any financial task, particularly when handling funds belonging to a vulnerable population, many of whom rely on their service provider for partial or significant assistance to manage their funds and guard their interests.

The Cost

FGH's risk management lesson cost the agency \$50,000, diminished consumer confidence and damaged reputation. The agency could have filed a civil suit and obtained a judgement against Bill, but the costs would have been high compared to the amount he stole, and the case would be one of many waiting in line. If FGH prosecuted him and he went to jail, he wouldn't be able to pay anyone back. Instead, the agency had him sign an agreement to repay or face criminal and civil action, while they hoped for the best.

Case Study #3

Corporate credit cards offer another venue for theft and fraud if they are not properly controlled. In the case of the XYZ provider agency, its Fundraising Director committed fraud in this way.

Employers must rely on a system of checks, balances and reviews...



Background

John Smith worked for XYZ for a number of years and was provided with a corporate credit card for expenses that he would incur while trying to raise funds for the agency.

What Happened

XYZ's credit card company called to say that it was closing the corporate account for non-payment. When the agency discussed the situation with the credit card company, it learned that someone had charged over \$150,000 in

unauthorized expenses to the account during the previous three months. As the agency continued to investigate, it found that the fundraiser, John Smith, took family and friends on vacations at expensive hotels and treated them to a variety of hotel extras. The XYZ Agency also learned that John had hid his deceptions by intercepting and discarding the credit card bills as they arrived. John might have continued his improprieties indefinitely, had the credit card company not called to tell XYZ Agency that the credit card account was being closed.

The Lesson

Clearly, no one at XYZ was logging and date-stamping mail or reviewing credit card statements and expense accounts on a regular basis. If XYZ had followed these best practices, it would have caught John within the first month.

The Cost

At \$150,000 plus interest and a blotted credit rating, this was another expensive learning experience.

You may find that your
risk management
processes are erratic.



Conclusion

As the case studies show, two things can limit the opportunity for theft. The first is your ability to recognize and manage exposures, which is very much under your control. The second is the thief's imagination. You cannot control this, but you can, and should, try to anticipate and respond to its output.

While this resource presents best practices related to employee dishonesty, each user must modify them to manage the risks of employee dishonesty within his/her organization. As you decide how and where to apply these practices, consider the flow of dollars, materials and other assets going into and out of your agency. Note the steps involved and who is responsible for each one. You may find that your risk management processes are erratic. For example, many agencies pay close attention to obvious risk areas, such as depositing checks and cash and the ordering and payment of goods received, but may give less thought to areas that seem less vulnerable, such as knowing where keys are, reviewing bank deposits or tracking inventory.

Another way to identify gaps that allow, or even invite theft is to include the following drill in your assessment: ask yourselves how someone might be able to steal from your agency. In other words, try to "think like a criminal." In the case of Judy Smith, her scheme was not really that complex; it was just the product of a creative and criminal mind. Someone like Judy Smith could readily spot an opportunity that might never occur to the law-abiding majority. You may be surprised at the risks you and your colleagues identify during this brainstorming exercise. As a second benefit, you may invent new ways to reduce and detect honest mistakes. Ideally, the results will leave you even more determined to adapt the protective measures suggested in this resource to your own use.

You may be surprised at the risks you and your colleagues identify...

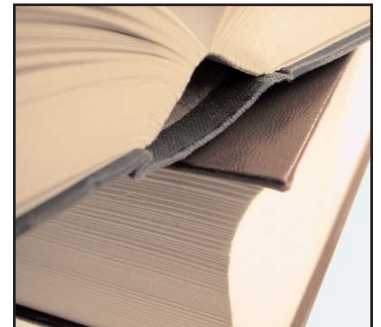


Sources

Healthy Nonprofits: Conserving Scarce Resources Through Effective Internal Controls, NonProfit Risk Management Center, 1996.

Zach, Gerard M., Fraud and Abuse in Nonprofit Organizations, John Wiley & Sons, June 2003.

Some information and case studies were taken from actual ISA claims and were interpreted for this resource.



About the Irwin Siegel Agency, Inc. (ISA)

ISA is a leading insurance and risk management organization within the Human Service field, insuring service providers across the United States. The insurance programs offer comprehensive coverage and specialized risk management for organizations in the Addiction Treatment, Community/Social Service, Developmental Disabilities, Medical/Physical Rehabilitation and Mental Health Care fields.

ISA has produced several other resources that deal with workforce issues such as The Exit Interview and Employment Related Liability, which can help agencies improve staff retention and reduce their risk of liability for employment practices. ISA's risk management resource collection includes a host of publications, videos and interactive, online trainings that cover vehicle, driver and consumer safety, disaster preparedness, incident management and more. Please visit www.siegelagency.com or call 800-622-8272 to find out more about ISA's unique insurance programs and risk management services.

While the information in this document may be helpful in identifying ways to minimize the risks related to employee dishonesty, do not regard this document as a substitute for the advice of legal counsel. This information is offered to increase understanding among its users of the ways in which organizations may be vulnerable to employee dishonesty, the risk management practices employers may use during the ordinary course of business to reduce/prevent this risk, and how and why basic risk management actually works. It does not purport to be a complete discussion of the subject, nor is it intended to provide a guarantee that compliance with its suggestions will avoid employee theft-related liability. Consult an experienced risk management professional and/or attorney for further advice on this topic.

Information contained in this publication has been obtained from sources believed to be reliable. The Irwin Siegel Agency assumes no responsibility for the accuracy or completeness of the information and recommendations. If you would like additional information, please contact our Risk Management Department at 800-622-8272 or by email at siegel@siegelagency.com. You can also visit ISA at www.siegelagency.com.

Some pictures copyrighted by photos.com



irwin siegel
agency inc.

insurance & risk management
human service programs

po box 309, rock hill, ny 12775
ph: 800.622.8272 / www.siegelagency.com