Guide to Preventing Workplace Fraud

Taking Action to Reduce Business Crime Exposure

KPMG

Chubb

It's Chubb. Or it's Chance.

GUIDE TO PREVENTING WORKPLACE FRAUD

TAKING ACTION TO REDUCE BUSINESS CRIME EXPOSURE

"Honesty pays, but it doesn't seem to pay enough to suit some people."

—F. M. Hubbard

PREFACE

Regardless of size, all organizations are vulnerable to workplace fraud. Fraud can take many forms—including embezzlement, forgery, theft of inventory and other assets, and computer crime—and can continue unchecked for years. The financial impact on an organization of these so-called "white-collar" crimes can be devastating.

As a leading provider of crime insurance (sometimes known as fidelity bond), the Chubb Group of Insurance Companies believes the most cost-effective way to deal with fraud is to prevent it. Although insurance can help recoup some monetary losses resulting from fraud, other losses can never be recovered, such as losses resulting from adverse publicity, the disruption of operations, and time spent with law enforcement officials and others. However, the consistent application of sound risk management practices can minimize opportunities for white-collar crime, helping to spare an organization the financial loss—and humiliation—that can result from a determined employee's fraud scheme.

We asked KPMG Forensic℠, a firm that specializes in fraud detection and prevention, to prepare the *Guide to Preventing Workplace Fraud* to help our Crime Insurance customers develop loss prevention strategies designed to reduce their exposure to white-collar crime. This booklet discusses the threat posed by various types of fraud, reviews common types of fraud schemes, and suggests specific risk management strategies.

Although we believe the *Guide to Preventing Workplace Fraud* is a good starting point for companies that want to develop or review their loss prevention strategies, it is not a substitute for expert advice. We encourage the reader to seek appropriate professional advice for any specific issues that arise when designing and implementing loss prevention strategies.

CONTENTS

INTRODUCTION

Understanding the impact of workplace fraud, and the potential losses associated with fraud and establishing effective loss control measures are critical for companies from cost, cultural, and risk management perspectives.

- **Workplace fraud is a common, everyday occurrence. Every business—large or small—is vulnerable to these crimes.**

- **Workplace fraud can have a substantial impact on a business's "bottom line" and even on its continued survival and success.** The financial impact of workplace fraud can be significant and can occur in the form of direct, indirect, and/or intangible costs. In addition to direct losses of tangible assets, such as cash, inventory, and securities, loss of competitive advantage, reduced ability to meet customer needs, reputation impairment, and disruption of business operations are some of the potential indirect and/or intangible costs to a business.

- **The challenge of combating fraud directed against a business is increased by the diversity and deceptive nature of those crimes.** Deception is a key element of workplace fraud, and a company may realize too late that it has been victimized.

- **An appropriate response to the threat of workplace fraud requires understanding potential areas that are "at risk," recognizing the fraud-related threats, and understanding the potential fraud-origination points, both internal and external.**

Although it is not possible to completely eliminate fraud risk, it is possible to reduce the risk and to minimize fraud-related losses and other consequences through effective loss control measures. Reduction of fraud risk requires a thoughtful, comprehensive, and proactive approach. Fraud risk management includes establishing effective loss control measures that

focus on prevention, detection, and response. Given the potential costs of workplace fraud, proactive fraud risk management makes good business sense.

THE THREAT OF FRAUD

Bottom line: Businesses are targets for crime because they have something of economic value. Fraud perpetrators believe that they can successfully steal, compromise, or use some of that value.

There is virtually no limitation to the means that may be employed to accomplish a criminal objective. The criminal mind is ever alert to seemingly new and unique ways to separate a business from its assets. Crimes that businesses face generally may be categorized as:

- "Street crime," such as robbery and burglary.
- "White-collar crime," such as fraud, misconduct, and related financial threats.

The focus of this booklet is on the white-collar fraud threat.

Defining Fraud

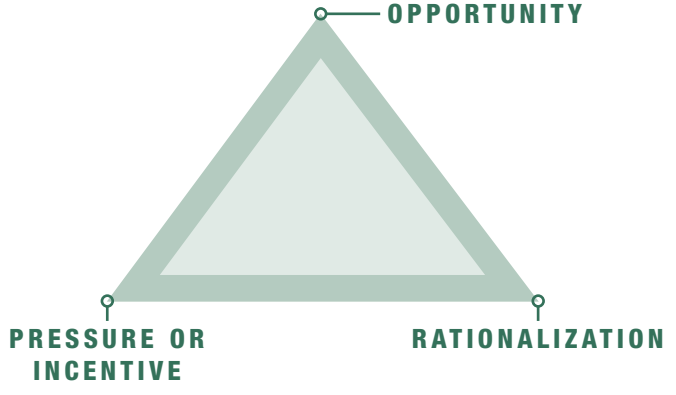
Anti-fraud professionals agree that fraud (and misconduct) encompasses activities involving dishonesty and deception that can drain value from a business, either directly or indirectly, whether or not the perpetrator(s) benefit. Fraud involves the *intent* to defraud; that is, the perpetrator relies on his or her deception to accomplish—or hide—the fraudulent activity. Fraud is not accomplished via honest mistake or error.

Fraud can manifest itself in a wide variety of ways and originate from a number of different sources. Fraud that is perpetrated by employees, consumers, and vendors dominates most instances of fraud experienced by businesses.

Understanding the fraud threats against your business, as well as why fraud typically occurs, are first steps in analyzing fraud risk and developing an appropriate plan for managing that risk.

The Fraud Triangle

What motivates people to commit fraud? Criminologists have identified three elements that are often present when fraud occurs. These three elements form the "fraud triangle."[1]



The Fraud Triangle

"Opportunity" refers to the situations and circumstances that make it possible for fraud to take place. For example, an employee with uncontrolled access to company funds has the opportunity to misappropriate those funds.

Opportunity is, generally, the element that a business can most effectively influence, impact, and control. An important action a business can take to reduce crime exposure is to *assess the opportunity* for fraud and respond accordingly. Responding to fraud risk includes development and use of effective internal controls to reduce, mitigate, or even eliminate opportunities for fraud.

"Pressure or incentive" helps explain why and when fraud occurs. Fraud takes place when fraud pressures or incentives outweigh, and ultimately

1 Dr. Donald R. Cressey is generally credited with developing the concept of the fraud triangle, according to the *2005 Fraud Examiners Manual* (Association of Certified Fraud Examiners).

overcome, the pressures or incentives to act honestly. Thus, pressures or incentives can become the *motivation* to act fraudulently. Pressures and incentives to commit fraud are often associated with:

- Lifestyle issues (living beyond one's means).
- Personal debt (e.g., excessive credit card use, gambling losses, use of drugs or alcohol).
- Business results (e.g., poor operating results, desire to avoid business failure, meet requirements of lenders).

If a company can recognize when and where excessive pressure/incentives may be present, it can use that information in fraud prevention and detection efforts and take action to mitigate business-related pressures/incentives in order to reduce fraud risk.

An effective fraud prevention program can *increase pressures and incentives to act honestly* by emphasizing a "perception of detection," underscored by the company's demonstrated, consistent commitment to taking appropriate and certain action once fraud is discovered.

"Rationalization" refers to the need for people to somehow justify their fraudulent actions in their own minds. A person involved in a fraud attempts to psychologically accept his/her own actions and emotionally "shift the blame" to anyone or anything other than him/herself.

Common rationalizations include:

- Entitlement: "They don't pay me what I'm worth. I have this money coming to me."
- Anger or revenge: "The company has treated me poorly; now they're going to pay."

- Minimization: “I’m not taking very much. The company can easily afford it.”

- Moral justification: “Everyone else is doing it, so it must not be so bad to do this.”

Rationalizations are not generally known to others and therefore are usually difficult to detect. In addition, persons with low moral integrity may feel little need to rationalize their behavior.

THE TYPES OF FRAUD

The Association of Certified Fraud Examiners (ACFE) categorizes fraud threats to businesses in the following ways:

- Asset misappropriation,
- Fraudulent financial statements and records, and
- Corrupt or prohibited practices.

Asset Misappropriation

Simply put, asset misappropriation can be thought of as a theft of something of value that belongs to your business. When it comes to asset misappropriation, "cash is king." In other words, cash is the most frequently targeted asset.

Consider:

- According to a 2004 national survey by the ACFE, 93% of the asset misappropriation cases studied involved cash, and the median loss was $93,000.
- "Cash" targets include currency and coins, checks, electronic funds, financial instruments, rebates, credits, discounts, and virtually any other device or means of financial exchange or enrichment.
- Cash is targeted for obvious reasons—it has a clearly known value, is easily transferable and transportable, is difficult to trace, and may even be diverted before any record exists on company books.
- Cash may be targeted by external or internal perpetrators or even by both via collusion.

Cash-diversion schemes range from simple skimming of sales receipts to complex frauds involving:

- Billing,
- Payroll,
- Expense reimbursement,
- Checks, including alteration and diversion of legitimately issued checks, and
- Sales and remittances, including point-of-sale "till tapping."

Other common targets of asset misappropriation include merchandise and/or other inventory, equipment and supplies, and even waste, scrap, salvage, or surplus property.

Generally, high-value assets that are easy to transport and to dispose of are at highest risk. Prime examples of high-risk assets include laptop computers, which pose the additional risks of confidential data disclosure and possible facilitation of unauthorized information-system intrusion.

Experience indicates that virtually any type of asset can be targeted. Company *services* may also be appropriated. For example:

- A manager of a construction firm uses "on the clock" company employees to remodel his home, or perform landscaping and/or maintenance work.
- An administrative assistant uses her employer's express mail delivery service account to routinely send packages to members of her family in other parts of the world.

Fraudulent Financial Statements, Books, and Records

The financial statements (internal and external), books, and records of a business may also be targets for fraud. Specifically, they may be:

- *Manipulated to hide* fraud (e.g., to prevent discovery of an asset misappropriation), and/or

- *Falsified* to *accomplish* a fraud (e.g., to cause unjustified financial rewards, such as executive bonuses based on falsified financial performance data).

Corrupt or Prohibited Practices

Corrupt and prohibited business practices include the following closely related concerns:

- "Side agreements" involving undisclosed rebates or kickbacks, and

- Bid-rigging, bribery, and extortion.

Corrupt and prohibited practices often involve hidden arrangements with customers and suppliers of goods and services to a company. In many cases, these arrangements directly and dishonestly benefit the individual employee(s) involved.

FRAUD RISK MANAGEMENT– LOSS CONTROL CONSIDERATIONS

Developing a fraud risk management program that includes loss control measures is critical to the *detection, mitigation,* and *prevention* of fraud-related risks.

Loss control measures need to take into account the company's industry, corporate structure and organization, geographic locations, customer base, vendor relationships, and regulatory environment.

Although not exhaustive, an effective risk management program may include the following types of internal controls:

Employee background screening, especially for employment applicants for positions involving trust, such as handling cash, inventory, and financial statements and records. Screening of potential employees should involve checks of criminal history, credit reports, verification of employment and education, and drug testing. An employee screening program should be commensurate with the company's fraud risk and take into account applicable legal considerations.

Customer feedback, reports, and complaints. Companies often pay little attention to feedback from their customers, vendors, and other external sources. Yet ignoring this feedback can result in a failure to detect and respond to possible fraudulent activity.

Effective oversight. Monitor, review, and supervise financial-related activities on a regular basis at multiple levels, including account reconciliations, exception reports, trend analysis, budget and/or plan variance analysis, and audits.

Mandatory vacation policies. Require employees who hold financial positions to take regularly scheduled vacations, and do not allow them to conduct company business while on vacation.

Fraud reporting programs. Have a program for facilitating the reporting of suspected fraud by employees and others.

Fraud awareness programs. Include training employees, and even vendors, in the fraud risks that threaten your business. This training should focus on identifying warning signs ("red flags") of potential fraud.

Fraud deterrence programs. Create a "perception of detection." A reputation for aggressively investigating indications of fraud can have a strong deterrent effect. On the other hand, a reputation for ignoring possible fraud may prove to be an invitation for perpetrators.

Effective follow-up and/or investigation. Establishing written policies and procedures, and assigning responsibility for implementing them, for follow-up and/or investigation when "red flags" are noted, policy and procedure violations occur, and allegations of improprieties surface is critical to ensure that investigation and remediation occurs.

"Zero-tolerance" fraud policy. One fraud deterrence strategy is to announce, communicate, and enforce a "zero-tolerance" fraud policy.

Cooperation with prosecution efforts. In the event of fraud, execute all required affidavits of forgery, provide requested documentation, make company staff available as a witnesses, etc. It is important that a company consistently demonstrate its commitment to a zero-tolerance policy with support for prosecution of any person found to have been engaged in fraudulent activity.

Internal audit/internal investigative units. Internal audit and/or internal investigative units are mechanisms for companies to monitor and look for violations of corporate policy and breakdowns in internal control. Companies should evaluate whether to establish these units separately or to combine them.

General fraud detection practices. Fraud detection can be practiced within various areas of a company and often may be part of the role of the internal audit or investigative unit. Some fraud-detection practices that businesses should consider include:

- Variance analysis, performed to evaluate variances from budget or other expectations.

- Data mining of financial transaction information to identify patterns and trends.

- Analysis of data correlations to identify anomalies in the expected relationship between related or dependant financial report account balances or other data.

- Computerized tracking and analysis of employee expense accounts performed on an ongoing basis in order to detect and respond to anomalies (such as an employee with abnormally high travel expense patterns).

- Review of supporting documentation to identify instances where that documentation is inadequate or suspect.

- "Fraud audits" specifically targeting possible fraud in specified processes or business units.

Vendor management. A company can protect itself from vendor fraud by using an effective vendor screening program.[2] Such a program can:

- Verify that a vendor actually exists and that the identification data provided by the vendor (address, for example) is accurate.
- Verify a vendor's ownership and the identity of key management personnel (and screen for potential conflict-of-interest concerns).
- Determine if a vendor, its owners and affiliates, or its key management personnel have a history of criminal activity.
- Determine if a vendor, its owners and affiliates, and its key management personnel have an acceptable business reputation.
- Verify that a vendor has the requisite qualifications, licenses, certifications, permits, and insurance coverage.

A company may also wish to include the following in its vendor fraud program:

- Procedures for approving orders, authorizing payments, issuing checks, and reviewing vendor payments, bearing in mind appropriate segregation of employee duties.
- Prepayment review of vendor invoices, including reconciliation with company orders and authorizations, receiving reports, returns, and adjustment records.
- Internal audit of the accounts payable function.

2 Always obtain competent legal advice before implementing vendor screening programs. For example, screening programs that include credit history checks must be properly administered in order to maintain compliance with applicable laws.

- "Vendor audits," which typically include examination of a vendor's records and documentation that support the billings made to your company.

- Publication of a company policy for regular vendor reviews and audits.

Cash and check management. Policies and procedures for handling cash need to address fraud risk. The tangible value of cash and the potential for misappropriation is a "real" risk that warrants several loss control measures.

- Assess the need for manual checks. Unless there is a genuine business need for manual checks, get rid of them.

- Strictly control the number of people who can authorize issuance of a manual check; require double signatures where appropriate and feasible.

- Safeguard and strictly limit access to blank check stock.

- Conduct a regular inventory of blank check stock, and promptly investigate missing/destroyed blank check stock.

- Monitor and enforce mandatory data entry of all manually issued checks within a prescribed time period. Require periodic reports of all manual check use, including negative balance reports and check-stock inventory verifications.

- Audit/review manual check use regularly, including examination of a sampling of cancelled checks to determine if payee, address, and amounts are consistent with company records. Review endorsement information on the reverse side of the checks; determine if endorsements are suspicious in any way.

- Reconcile bank statements, and clear exceptions and identified differences. Exceptions and unresolved differences should be promptly brought to the attention of the appropriate level of management and resolved. Report all discrepancies and issues to your bank, both to alert your bank and to protect your legal rights and remedies.

- Use checks with adequate security features. (Consult with a commercial banker regarding security features.)

- Examine cancelled checks returned for indication of alterations, duplicates, or counterfeits. For example, counterfeit checks typically do not have the micro-encoded features. Any cancelled check where the bank has manually encoded the bank account and routing information should be considered suspect.

- Consider the use of "positive pay" or "reverse positive pay" protection.

- Cooperate with prosecution efforts.

"Positive pay" and "reverse positive pay" protection. "Positive pay" may be thought of as an anti-check-fraud process where you and your bank compare notes about the checks issued on your account before they are "paid" into the banking system. Essentially, positive pay works as follows:

- The company prepares an electronic listing of the checks (drafts) issued (a "checks issued" list) and submits this list to its bank each day. Key information included on this list includes the check number, check amount, and date.

- The bank compares the "checks issued" list to the information on the checks presented for payment on account.

- The bank identifies presented checks that do not match the company's "checks issued" list and reports discrepancies to the

company. Checks with identified inconsistencies are not honored by the bank unless the company specifically authorizes payment. Instead, these checks are returned through the banking system and are not charged to the company's account.

- Other presented checks are routinely paid through regular banking procedures.

"Reverse positive pay" works much the same way but involves the company's reviewing a list of checks prepared by the bank (a list of "checks presented") rather than a list prepared by the company. The company would compare the "checks presented" list against internal records of the checks the company has issued. In the "reverse positive pay" process, the company would typically need to notify the bank as to which checks to pay and which to reject.

Additional information about "positive pay," "reverse positive pay," and other check-fraud protective measures may be obtained from commercial bankers and other financial institutions. Bankers are also an excellent source of information concerning the types of fraud currently being experienced by businesses. Take the time to meet with your banker concerning check fraud.

Asset management and disposal. Companies should have a comprehensive asset management program in place. Generally, this means that assets valued above an established amount are tracked by the company from the date of receipt to the date of final disposal. Although asset management programs will vary according to individual circumstances, these programs typically incorporate many of the following features:

- Detailed inventory records.

- Tamper-resistant asset identification tags.

- Physical security measures and building-access control.

- Periodic physical inventories of assets. Inventories of assets in dispersed locations should be conducted simultaneously to prevent double-counting or "ghost inventory."

- Investigation of inventory discrepancies.

- Tracking of "retired," obsolete, scrap, and salvage assets/inventory and sales proceeds. Companies often lose sight of these assets when they are retired from use, written off, or otherwise removed from their financial books.

Payroll. Payroll is a common area of fraud, thereby making fraud controls critically important. A payroll fraud program should enable management to:

- Compare employee termination dates and payroll dates. For computerized pay systems, such comparisons could be automated with exception reports generated for follow-up by internal auditors or others.

- Monitor changes in employee payroll mailing addresses, direct deposit accounts, or check deposit instructions, particularly if changes occur more than once in a short span of time (particularly if the end result is a change back to the original information).

- Review employee pay for sharp increases for one or more pay periods or for the very last pay period spent with the company.

- Review employee pay for similarly situated employees.

- Review for employee names found in payroll records but not in company rosters, email address directories, or telephone lists.

- Ensure that commonly expected deductions are made for all employees.

- Investigate Forms W-2 and 1099, as well as other correspondence sent to the home address on file for an employee, a contractor, or a vendor that is returned as undeliverable.

- Review employee mailing addresses on file for suspicious addresses (e.g., a "mail drop" address, an address for an unrelated employee, or an inconsistent work location).

- Determine if more than one paycheck is issued to the same name, Social Security number, address, and/or direct deposit bank account.

Conflicts of interest, kickbacks, bribes, and employee corruption. Businesses also need to ensure a culture of honesty and integrity. Measures to consider:

- Develop, document, and regularly communicate high ethical standards for all business dealings and activities.

- Provide ethics training to employees. Ensure that ethics training and manuals include practical guidance for "real world" situations faced by employees.

- Insist that company leadership set a high ethical example ("play by the rules").

- Develop a culture that supports, and expects, reporting of ethical lapses.

- Take appropriate and consistent action when issues arise and violations occur.

- Accept only *original* documents (i.e., photocopies are not acceptable).

- Incorporate prepayment review of employee expense reports, by a business unit supervisor or manager and someone from finance or accounting, for appropriateness and reasonableness.

- Conduct random audits of paid employee expense reports.

Segregation of duties. Establishing effective segregation of duties involves understanding employees' roles, responsibilities, and access to financial records, assets, and systems. A company needs to evaluate its business operations, including:

- Incoming payment *receipt* and payment *recording* (bookkeeping) functions. Incoming mail from customers should be opened by someone other than the person recording customer payments in the company's records. All receipts contained in incoming mail should be individually listed by the mail opener for later comparison with the recorded receipts.

- Disbursement *recording* (bookkeeping) and *disbursement authorization* functions. The person responsible for recording a disbursement should not be the same person who has the ability to authorize the disbursement.

- *Disbursement authorization* and *disbursement issuance* functions. The person with authority to authorize a disbursement should not be the same person who issues the actual payment.

- Segregation of the authority to *authorize* account adjustments (including account write-offs) from the ability to *perform* account bookkeeping/account adjustment functions.

- Account *reconciliation* and account *recording* (bookkeeping) functions. Although bookkeeping may prepare a preliminary reconciliation for operational needs, financial controls reconciliation should be performed by someone separate from the recording function.

Segregation of duties may be difficult to achieve in smaller businesses where sufficient staff may not be available to handle separate task assignments. In these cases, businesses may need to rely on other controls, such as closer oversight by owners and managers, more frequent reconciliations and account balance confirmations and, if possible, more frequent rotation of financial assignments.

COMMON FRAUD SCHEMES

This section offers illustrations of common fraud schemes for consideration in assessing your business risks. All names are fictitious and not intended to be or imply real persons or companies.

Vendor Schemes

Payments to outside vendors represent a significant outflow of funds for most companies. Therefore, it is important to understand vendor fraud risks.

Vendor Management

Toni, a human resources manager for ABC Company, has authority over an annual training budget of $3.5 million. She routinely contracts with new vendors for training programs and approves payments to those vendors. Toni asks Accounts Payable to establish a new vendor account for "XYZ Consulting Services" and authorizes payments to XYZ amounting to $300,000 over a six-month period. A subsequent inquiry about XYZ results in discovery that:

- XYZ Consulting Services is a shell vendor operating out of a mail drop address. Toni is the only person associated with XYZ Consulting Services.
- XYZ Consulting Services never provided goods or services of any kind to ABC Company. The invoices provided to Accounts Payable by Toni were never challenged, even though the service description was vague and no service agreement, nor any other documentation, was present in the company files.

"Ghost" vendors represent a common fraud device used by company insiders who have the abilities to approve new vendors to receive payments and to authorize such payments. In these types of schemes, a dishonest employee may establish a phony vendor account(s) that he or she controls and then direct fraudulent payments to that account(s).

In many companies, vendor payments above a certain dollar amount are subject to closer scrutiny, higher level approvals, or special reporting. In these cases, to avoid detection, an employee may set up multiple ghost vendors and make only one or two smaller fraudulent payments to each. Companies should be alert to suspicious patterns of vendor payments, including those that are "just under the radar" in terms of required approvals, reporting, or other company procedures.

Similar to a ghost vendor scheme is the dishonest employee who "takes over" a legitimate vendor account. In this case, the employee may simply change the mailing address shown in the vendor profile for an inactive company to one the employee controls. Of course, invoices begin to arrive from the formerly inactive company.

Ghost-vendor schemes may also utilize company names that are intended to be similar to well-known, established vendors (e.g., a legitimate vendor named "Robert Smith & Co." may be reestablished as a ghost vendor under the name "Bob Smith" or "R. Smith"). A perpetrator's goal for establishing ghost vendors is to use name alignment as a tactic to reduce the chance of detection. Of course, the phony vendor names are typically associated with a mailing address that is controlled by the perpetrator. While this type of scheme may sound simple, it often works.

A dishonest employee may also set up, or be associated with, a real vendor doing actual business with the company (i.e., actually providing goods or services). In this circumstance, an employee's association with the vendor may be kept hidden for a variety of reasons, including:

- Company policy prohibiting conflicts of interest.

- An employee's desire to profit from a vendor arrangement (e.g., reselling marked-up goods to the company at a profit, obtaining a kickback for steering business, or sharing in otherwise fictitious billings or overpayments).

- An employee's desire to personally benefit through collusion with a vendor. These types of schemes typically involve kickbacks, bribes, or other financial incentives paid to (or for the benefit of) an employee who assists a vendor in defrauding the company.

A key preventative measure for a company to take to protect itself against vendor fraud is to ascertain that its vendors each have a reputation for integrity. Businesses should consider the use of a vendor-screening program, the key components of which may include:

- Ensuring that identification data provided by the vendor is accurate, including verifying the ownership of the vendor enterprise and the identity of key management personnel.

- Conducting criminal, financial, credit, and other background checks.

- Verifying that the vendor has the appropriate credentials, licenses, certifications, and permits to conduct business.

If a vendor misrepresents its credentials, this is a strong indicator of a lack of integrity.

In addition, businesses should consider:

- Establishing procedures for approving orders, authorizing payments, issuing checks, and reviewing vendor payments, all on a segregated-duty basis.

- Prepayment reviews of vendor invoices, including reconciling company orders, receiving reports, returns and adjustment records, and any related documentation.

- Internal audit of accounts payable.

- "Vendor audits," which typically include inspection/examination of a vendor's records and documentation that supports the billings made to your company.

Cash-Skimming Schemes

Cash Handling

Todd worked as a clerk in a large retail store. The point-of-sale scanning equipment he used to ring up customer purchases automatically captured the price of each item sold. Per company internal controls, all "till" was routinely counted and balanced at the end of each shift and discrepancies were not tolerated.

Despite the apparent controls, Todd found opportunities to defraud his employer.

- Cash skimming: Todd often pocketed the cash paid by customers. In order to prevent detection and make sure that his till balanced at the end of his shift, Todd substituted large quantities of coupons that he clipped from the local paper for the cash he stole.
- Skip scanning: When Todd rang up purchases for his friends and family, he often skipped the scanning of the most expensive items. These items went into the shopping bag, and out of the store, without payment.
- Unauthorized discounts: Todd provided friends and family with unauthorized "discounts" on merchandise by overriding the scanned price and manually entering a reduced figure.
- Fake refunds: Todd also took cash from the register till and covered for the shortage by falsely reporting cash purportedly paid out to customers as refunds for returned merchandise.

The company's internal controls should have been sufficient to detect that Todd's redemption of coupons, price overrides and related manual price entries, and refund pay-outs all exceeded established norms. These warning signs should have been noticed when the till was counted and balanced and

also evident from trends shown in managerial control reports on key activities such as coupon redemption and returned merchandise payouts. Further, the company's returned merchandise program controls were apparently deficient as, at a minimum, customer identification and return documentation requirements should have been required, as well as reconciliations of returned items and refund payments.

The skip-scanning scheme could have been detected by physical security measures, such as store camera surveillance of point-of-sale activity or managerial oversight and observation of point-of-sale operations.

Frauds Related to Company Checks

Fraudulent schemes involving company checks are often directed against companies. The following scenarios illustrate fraud risk associated with company checks.

Check-Issuance Procedures

ABC Small Company uses a popular off-the-shelf computerized bookkeeping program. All company checks are issued via this system.

When a payment is properly authorized by one of the company's managers, the information needed to issue a check is provided via email to David, the company's computerized bookkeeping systems "expert." David enters the payment information into the computerized bookkeeping program, which causes a company check to be printed. The bookkeeping program automatically creates a record of the check issuance and makes the appropriate accounting entries. The completed check is then sent by David via interoffice mail to the manager who originated the payment request. Periodic reports of company payments are generated from the computerized bookkeeping system by David and are sent to company managers for review. For example, every manager gets a monthly itemized listing of the payments he or she has authorized, which includes payee name, payment amount, etc. If any questions arise, David is consulted and/or asked to provide additional reports from the computerized bookkeeping system.

The above scenario presents a number of fraud risks related to lack of segregation of duties, including:

- The bookkeeping systems "expert" appears solely to have the ability to input and edit bookkeeping system information, issue checks, distribute checks, produce and distribute related reports, and resolve payment questions and discrepancies.

- The check authorization procedures are deficient in that the person requesting the payment is the same person who receives the issued check for review and is then responsible for mailing the check to the payee.

- The check requestor/issuer is also responsible for reviewing system-generated payment reports and presumably for initiating action if discrepancies are noted.

The level of systems security protection provided by an application is an important consideration with any "off-the-shelf" bookkeeping product. Companies should not assume that a "well-known" application is secure but instead need to assess whether access and authorization levels that are set to acceptable default values.

Manual Checks

ABC Company recently determined that a number of "manual checks"[3] had been fraudulently issued by Bill, a dishonest accounting manager. This accounting manager accomplished this fraud by:

1. Not recording all of the manual checks and
2. Recording some of the manual checks in the company's bookkeeping records with a fictitious payee name and mailing address.

Accounting reconciled the bank statements monthly and unreconciled items were identified. Company policy required follow-up on all unidentified amounts or differences greater than $5,000.

The above fraud scheme illustrates a lack of segregation of duties. Key items of note include:

- The manager was able to alter the manual check payees to include his own name and the names of family members. This enabled the manager to use his or a family member's existing bank account to negotiate the manual checks.
- Fictitious payee names included legitimate addresses of family members.
- The accounting manager was knowledgeable about "threshold" triggers for follow-up.

It is not uncommon for a company to use manual checks to supplement an automated (computerized) check-issuance system. Problems arise, however, when a company fails to take into account that the manual checks are not

3 "Manual checks" are checks written out by hand, as compared to checks that are printed using a computer program or system.

part of computerized records and are, therefore, not included in any automated system checks and balances.

Manual check issuance systems require discipline to safeguard against the entry of fictitious information into company records for an issued check. Additionally, it is important that periodic inventory counts be conducted of blank-check stock to ensure all checks are accounted for and "out-of-sequence" check usage does not occur or go unnoticed.

- Tracking manually issued checks is not always the same as tracking checks generated by an automated system. As such, it is critical to maintain a record of manual checks, to establish a policy for recording manual checks in the bookkeeping system, and to reconcile these records.

- Reconciliation thresholds may also need to be adjusted for manual checks.

Loss controls related to manual checks should:

- Assess the need for manual checks.

- Limit and control the number of people who can authorize issuance of and sign a manual check.

- Safeguard, limit access to, and periodically inventory blank-check stock.

- Monitor and enforce mandatory data entry of all manually issued checks.

- Regularly audit/review manual checks.

- Reconcile bank statement information on a consistent, regular basis, including follow-up and resolution of all identified differences.

Altered, Duplicate, and Counterfeit Company Checks

An accomplished "check artist" who obtains a legitimate company check can easily and expertly:

- "Wash" (chemically erase) information on the check face so that new information can be inserted,
- Enter or alter the check payee name and address to match false identities,
- Change the check amount to any amount, and/or
- Duplicate the check so that it may be converted to cash again and again.

How does a check artist get access to a company's legitimate checks? The check artist may:

- Be (or arrange to be) a rightful recipient of such a check or know someone who is a rightful recipient,
- Steal the check, often from the incoming mail in home mail delivery boxes,
- Purchase the check, at discount, from organized check thieves, or
- Be an employee of the company, its bank, its check-printing service, the postal service, or any company that rightfully receives a company check or handles the check in any way.

Additionally, a check artist is likely to take note of the bank account and bank routing information that appears on the company check. Using this information, check perpetrators can use computers, desktop publishing

software, and color laser printers to produce numerous counterfeit checks purportedly issued by the company.

Counterfeit checks may not necessarily resemble the company's, but they can look legitimate enough to be cashed and initially processed through the banking system. These checks have the company bank account and bank routing information imprinted on them so, at least initially, the checks will be debited to the company's account. By the time the checks are discovered to be counterfeit, the perpetrators are typically long gone.

Here are steps to consider for mitigating exposure to check artist fraud:

- Consult with a commercial banker regarding security features and use them in your company's checks.
- Be aware of red flags. For example, counterfeit checks typically do not have micro-encoded features.
- Closely monitor and reconcile your company's bank balance. Report all discrepancies and issues to the bank, both to alert the bank and to protect the company's legal rights and remedies.
- Examine cancelled checks for indications of alterations, duplicates, or counterfeits.
- Consider the use of "positive pay" or "reverse positive pay" procedures.

Accounts Receivable/Incoming Payment Processing

Frauds naturally take place "where the money is." In many companies, that's the accounts receivable or remittance processing unit—the place where payments flow into an organization.

Remittances

Jonathan, a long-term employee in ABC Company's accounting department, was responsible for opening the incoming company mail and processing all remittances received on customer accounts. Jonathan was also responsible for responding to customer account balance inquiries, adjusting customer accounts for billing errors and other mistakes, and collecting and writing off problem accounts.

What opportunities did Jonathan have for defrauding his employer?

- Diversion of payments—Jonathan diverted some of the checks paid to the company by depositing them into a personally controlled bank account he had established in a name that was similar to the company name.
- Write-offs—Jonathan covered up some of his fraudulent activity by falsely portraying customer accounts as uncollectible and by writing off outstanding balances in those accounts. He did this so that all checks subsequently received on the written-off accounts could be diverted without arousing suspicion.
- Lapping—Jonathan also engaged in "lapping" payments—e.g., a payment made on one customer's account (Account A) is applied to another customer's account (Account B), where payments had previously been diverted. In other words, payment on Account A is used to make up for an existing shortage in Account B. As a result, Account B is now in balance, but Account A is not. Future payments on other accounts will need to be applied to Account A to hide this diversion. Jonathan used this practice repeatedly to keep accounts in an ostensibly "current" status.
- Unexpected payments—When payments were occasionally received on accounts that had been written off as uncollectible, Jonathan diverted those payments as well. These payments were not expected and thus never missed by the company.

The above scenario illustrates a lack of segregation of duties. The employee had control of both receiving and recording incoming customer remittances, as well as the authority to apply payments to customer accounts and to make account write-offs.

Misappropriation of Waste, Scrap, and Salvage Property

Companies that work with waste, scrap, and salvage property are common targets of fraud since they may have no clear expectation of the value or amounts due from the sale of these assets.

Scrap Management

James, a production process supervisor in the ABC Company manufacturing plant, is responsible for oversight of a process where cutting and shaping of copper components is performed. This process produces copper scrap and waste that is collected for reuse or resale by the company. James routinely returned to the company plant during evening hours, filled his pickup truck with scrap and waste, and then sold this material to a recycler.

In this scenario, access control measures could have either prevented James from returning to the plant during evening hours or at least alerted management that he was doing so. Effective physical security measures include monitoring who is in a company's facilities, knowing when they are there and, in the case of nonstandard business hours, confirming that employees, vendors, and visitors have a valid reason to be there.

Key considerations for a company include:

- Physical security of work sites should include measures to appropriately restrict work site access, and
- Subjecting vehicles entering and exiting company premises to inspection.

Conflicts of Interest, Kickbacks, Bribes, and Employee Corruption

Employee Corruption

Mike, a real estate manager for ABC Company, is in charge of office space for company operations in several states. His responsibilities also include contracting with vendors for maintenance and build-out.

- Mike has electrical upgrade work done to his cabin by the same contractor who provides services to ABC Company, and that job is billed to ABC Company as though the work was performed at a company location. Mike approves the bill for payment.
- Mike has improvements done to his home by the same construction contractor he routinely hires to make office space alterations for the company. Mike pays nothing for the improvements to his home.

Companies can mitigate exposure to employee corruption by:

- Hiring ethical people.
- Developing, documenting, and regularly communicating high ethical standards for all business dealings and activities.
- Ensuring that ethics program training and manuals include practical guidance for the real situations faced by employees.
- Insisting that company leadership set a high ethical example and "play by the rules."
- Developing a culture that supports, and expects, the reporting of ethical lapses.
- Taking appropriate, consistent action when ethical issues arise and violations occur.

Expense Account Reimbursement Fraud

Employee abuse of expense accounts represents a significant risk for many companies.

Time and Expense Issues

George, an employee of ABC Company, travels extensively on company business. George's manager routinely approves his expense account after only a cursory examination. This cursory review has helped George find several ways to "beat the system" and obtain reimbursement payments for which he is not entitled.

How does George take advantage of his employer?

- Mischaracterization of meal and entertainment expenses—George and his friends frequently go out to dinner at expensive restaurants in the city. George charges these meals on the company credit card and submits an expense report that falsely indicates he was entertaining clients and conducting other company business.
- Overstated expenses—George collects blank receipts from taxi cab drivers and other sources, completes these receipts to indicate a higher expense than was actually incurred, and submits the receipts for company reimbursement.
- Fictitious receipts—George's business travels sometimes include meals that are paid for by business associates or included as part of an event he is attending. In these cases, George uses his personal computer to produce a counterfeit "receipt" for separate meals that never took place and submits the fictitious receipt.
- Altered receipts—George alters receipts by increasing the dollar amount shown on the receipts and altering the dates and other information on old personal receipts to make them appear current and business-related.

An effective program for combating employee expense reimbursement fraud should include, among others, the following policies:

- Accept only *original* supporting documents.
- Require written explanation and replacements for lost original receipts. Closely examine excessive incidents of "lost receipts" and refuse to reimburse the expenses.
- Require timely submission of fully supported employee expense reports.
- Have the employee's business unit supervisor or manager conduct a prepayment review of the employee's expense reports and required documentation.
- Require an additional review of "corrected" employee expense reports.
- Conduct an annual internal audit of employee expense reports and related company credit card use.

Payroll Fraud

It is often impossible for company management to know every employee and their pay status. Furthermore, payroll processes can often make it possible for false payments to be made. Common payroll fraud schemes include, among others, payments to:

- Nonexistent employees ("ghost" employees) added to the company payroll by someone with the authority to add new employees.
- Employees for hours not worked (falsified time reports).
- Employees for unauthorized salary/pay rates, overtime, or bonuses.

Payroll fraud may involve collusion between employees (e.g., between the employee who receives the fraudulent pay and an "insider" with the ability to facilitate the payment).

Ghost Employees—Deferred Separation Status

Chris worked as an information technology representative in the human resources (HR) department with responsibility for maintaining HR information systems databases. Chris was responsible for updating employee data in the system (e.g., change of address, change in employee status). The HR database maintained by Chris fed into other company information systems, including the payroll system.

When a salaried employee resigned from the company, Chris would defer changing that employee's status to "inactive" for a week or more after the employee's last day of work. The company payroll system would automatically compute wages due the former salaried employee for every day that the employee remained "active" in the system.

Prior to each subsequent payday, Chris would temporarily change the address shown for the former employee to an address that Chris controlled, e.g., a mail drop. After the system issued a paycheck, Chris would change the former employee's address back to the original. Chris would make sure that the former employee status was reflected as inactive when he felt it necessary to "end" the scheme.

In the rare circumstance when anyone questioned these payments, Chris was prepared with phony documentation indicating a payment had been made to the former employee in error and that collection action was being initiated to recover the overpayment.

Payroll fraud risk mitigation efforts that companies should consider include:

- First-line manager review of payroll reports. First-line managers generally have the best knowledge of employee status and how much and when they should be paid. However, companies need to

understand there is risk that can arise related to overdependence on "routine" report reviews because "busy" managers may routinely not spend time performing an adequate review.

- Unscheduled, random, in-depth reviews by managers of payroll reports conducted several times a year with a required report on all findings (including "nothing found" or "no exceptions" reporting).

- Manager certification that a payroll report review was conducted and that all discrepancies found were appropriately resolved/reported.

- Active review of payroll data by internal auditors for fraud warning signs.

The existence of adequate segregation of duties also needs to be assessed. Employees with the ability to add new employees or to change employee profile information should not have the ability to approve payroll payments or adjustments, enter pay hours, change pay rates, or authorize bonus or other special payments.

Payroll fraud warning signs include:

- Frequent changes in an employee's payroll mailing address, direct deposit account, or check-deposit instructions, particularly changes occurring more than once in a short span of time that subsequently change back to the original information.

- Sharp increases in an employee's pay without apparent reason or explanation.

- Broad disparity in a particular employee's pay compared to similarly situated employees without apparent reason or explanation.

- "Employee" names found in payroll records that do not appear in company rosters, email address directories, and telephone lists.

- Employee correspondence sent to an address on file that is returned as undeliverable.

- More than one paycheck issued to the same name, Social Security number, address, and/or direct deposit bank account.

- Frequently "backed out" or changed entries to payroll systems by a particular system user.

- Terminated employee payroll changes that are processed late by the same system administrator/user.

Use of Company Funds to Pay Personal Expenses

Alternative Company "Checkbooks"

An employee can gain access to the company "checkbook" in several ways.

Purchase Card

As the administrative assistant for a regional vice president, Betsy has access to a "p-card" (purchase card) that allows her to order and obtain office supplies. However, Betsy routinely pays for merchandise with this card for her husband's home-based business. Betsy's boss is expected to review a monthly report of p-card transactions for his group; however, as he is "much too busy to be concerned with the purchase of pens and paper clips," he has delegated these reviews to Betsy.

Travel and Entertainment—Helping the Boss

Betsy is responsible for making travel and entertainment arrangements on behalf of her boss, including attendance at major sporting events by company executives and key customers. Betsy's boss is required to authorize payment for these costs with his officer's signature stamp. However, Betsy has possession and control of his signature stamp and routinely uses it to approve payments on behalf of her boss.

Trusted employees are often allowed to bypass internal controls to "assist" others. However, these trusted employees can take advantage of controls they are routinely allowed to circumvent. Circumvention of existing internal controls, even by exception, is a common theme in employee fraud. Assessment of fraud risk needs to address not only the question of whether internal controls have been properly developed and designed but also that such controls have been effectively implemented and are consistently applied. If exceptions to existing controls are allowed, alternate controls need to exist.

Computer-Related Fraud

Computer-related crimes may be committed by persons with or without authorized access, including user and/or physical access. Of particular concern is the potential risk associated with disgruntled employees, contractors, or other insiders who may have high-level computer system access, authority, knowledge, and/or familiarity.

Computers can serve as the target of criminal activity, but more often they serve as a "tool," or the means, to accomplish a crime. Two basic examples:

- ***Cash diversion***—Computerized systems may be used to skim funds from customer accounts or to embezzle company funds and to hide that activity.

- ***False documentation***—Computers may be used to produce fraudulent documentation.

Effective protection for computer systems includes formulating and implementing a computer fraud risk management plan. Some components to consider:

- Identify internal and external risks to system security, data confidentiality, and data integrity.

- Design and implement safeguards in response to identified risks, including those arising due to changes in the business.

- Periodically monitor and test safeguards.

Physical Security of Technology Assets

The physical security of computers and computer systems is naturally an extension of a general physical security program. Existing physical security policies and procedures need to be adapted to meet the specific threats associated with information systems and related assets. Controls to consider:

- Restrict access to the areas where computers and computer data are housed.

- Perform comprehensive background investigations on personnel who will have access to computer areas and information.

- Utilize asset-protection programs, such as asset-tracking devices or software installed on laptop computers.

Defenses against unauthorized, malicious, and/or fraudulent logical access to computer systems include good physical security and use of security technologies. Successful computer system intrusions may involve unauthorized appropriation and use of user passwords. Compromised passwords need to be reported promptly, with swift action taken to revoke all related systems rights.

RESPONDING TO THE THREAT OF FRAUD

Responding to the threat of fraud can be challenging. There is no "cookie-cutter" fraud response strategy that is appropriate for every business. The diversity of fraud risks associated with different business environments and situations requires that fraud risk responses be appropriate for the specific business operations, business environment, and fraud experience.

Consider that the "ideal fraud opportunity" might include any of the following factors:

- A weakness in the internal control system or the ability to easily override the control system (i.e., an opportunity).
- Pressures or incentives to commit fraud sufficient to overcome the pressures or incentives *not* to commit fraud.
- Perceived reward for fraud is relatively high.
- Perceived risk of detection is relatively low.
- Potential penalty, if caught, is perceived as being small or relatively inconsequential.

Therefore, an effective fraud response plan should:

- Limit fraud *opportunities* by establishing strong internal controls and limiting overrides of those controls.
- Manage *pressures* and *incentives* inherent in the business process (to the extent this is possible).
- Focus fraud prevention and detection efforts on risks where potential financial loss is the greatest or where cumulative losses from smaller frauds may be significant.

- Foster a strong "perception of detection" through proactive fraud identification, detection, and investigation efforts.

- Respond to identified fraud by consistently applying a "zero-tolerance" policy.

Fundamental Elements of Corporate Governance

Although businesses may differ in their fraud risks, most fraud response programs need to incorporate, or at least consider, certain fundamental elements. This is true of businesses of all types, sizes, and organizational structures.

Ethical Values of the Company

A highly ethical business culture is an essential element in any effective fraud prevention and deterrence program.

The culture of an entity starts with, and takes its tone from, the very highest level of the business. The "tone at the top" permeates the entire organization and is, therefore, a huge component of company culture.

A corporate value system built on honesty, integrity, and ethical values presumes a lack of tolerance for behaviors that lack integrity. Insistence on honesty and integrity in all business dealings is the cornerstone for how a company will deal with its customers, employees, and business associates and how customers, employees, and business associates are expected to deal with the company.

At the most fundamental level, this means that a company must begin its fight against fraud by adopting, and by supporting, a highly ethical business culture.

Code of Ethics or Code of Conduct

Many companies incorporate their key ethical values into a formal policy document, typically referred to as a "code of ethics" or "code of conduct." Establishing and communicating such a code is an excellent way to ensure that employees and business associates understand the corporate values and the expected behaviors in support of those values. Communicating this code often includes training programs that further articulate the conduct and behaviors expected of all company employees and, in many cases, of those who do business with the company.

A written code outlines what the company means by "honesty and integrity" on a practical level. Guidelines within the code (or they might be supplements to the codes) provide employees with expectations of how they are expected to conduct themselves within the company and as representatives of the company. Businesses often post their codes on their Web sites to more broadly educate the market on their expectations of employees and business associates.

A code of ethics or code of conduct commonly includes specific segments that address:

- Behaving with honesty and integrity.
- Complying with laws and regulations.
- Disclosing/reporting conflicts of interest.
- Maintaining confidentiality of information.
- Receiving or giving gifts.
- Reporting instances of company code violations.
- Using company assets and resources.

Many companies require that employees acknowledge, often in writing and on an annual basis, their receipt and understanding of the company code. As part of the acknowledgement process, it is not unusual for employees to be asked to list any applicable exceptions or to certify that they are in full compliance with the code.

Guidelines for business associates (vendors, partners, etc.) should also set expectations of those parties in dealing with the company.

Business Structure

Business structure includes, but goes beyond, organization charts. Every person within an organization is entitled to (and must understand) his/her roles, responsibilities, accountabilities, and reporting relationships. Effective business structures clearly and succinctly establish, in writing:

- Roles and responsibilities,
- Accountabilities, and
- Performance measurement and reporting.

In its simplest form, employee roles and responsibilities within the organization are set forth in written job descriptions. Accountabilities define the responsibilities and authority of a position, as well as the internal reporting structure—whether for the chief executive or the mailroom clerk. Accountabilities provide clear organization guidelines and a mechanism for checks and balances to guide and assess employee management and performance.

Checks and balances are also critical to an effective fraud prevention and detection program, and identified deviations need to be addressed on a current basis, particularly when they conflict with a company's code of ethics, code of conduct, or established authority(ies).

Whistleblower and Hot-Line Programs

When fraud occurs, it is often the case that someone associated with the organization observes questionable behavior, notices discrepancies in records or practices, or learns other information that arouses suspicion that something wrong is taking place.

Consider the following:

- Frauds may become known to someone associated with the victim organization, such as an employee, a vendor, or a customer of the organization.

- It is estimated that more than 40% of frauds are detected via a "tip."

Many companies have instituted "whistleblower" programs. In fact, under Sarbanes-Oxley, publicly traded companies subject to regulation by the U.S. Securities and Exchange Commission are now required to establish confidential and anonymous procedures for employee reporting of concerns related to questionable accounting or auditing matters.

Whistleblower programs often include so-called "hot lines," i.e., toll-free telephone lines dedicated to receiving whistleblower information. Effective whistleblower programs often incorporate the following practices:

- Hot lines are answered by staffers who have been specially trained to receive whistleblower information and elicit meaningful information.

- Hot lines are staffed during business and nonbusiness hours.

- Whistleblowers have the opportunity to remain anonymous, and anonymity requests are strictly honored.

- Callers are asked to call back at a future date so that additional information may be obtained after the company has made an initial inquiry or conducted an investigation.

- Hot-line calls, and related follow-up activities and actions, are well-documented, and summary reports of hot-line activity are provided to the highest level of management.

- Retaliation, through any means, for providing information is strictly prohibited, and the company takes action to enforce this retaliation ban.

- The hot line is well publicized, with use by employees, vendors, customers, and other business associates actively encouraged.

Many companies also provide mechanisms other than, or in addition to, hot lines for the confidential reporting of suspected fraud. These mechanisms include direct reporting to the board of directors, higher-level managers, legal counsel, and internal audit or security personnel via a dedicated email address or other means.

FINAL THOUGHTS ON FRAUD RISK AND RESPONSE

This booklet is intended to provide the basis for thoughtful consideration of the types of fraud risk. It would be impossible to include every type of fraud risk; however, it is hoped that this booklet can serve as a valuable reference.

You are encouraged to review this booklet and to consult, as necessary, with professional advisors such as your insurer, forensic professionals, and legal counsel.

ABOUT THIS BOOKLET

This booklet was developed by KPMG Forensic℠ for distribution to business owners, risk managers, and others who need to address the risk of fraud in a business environment. The information it presents is intended to provide practical suggestions for recognizing and responding to that risk.

All information provided is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we have tried to provide accurate and timely information, there is no guarantee that the information will continue to be accurate following publication. No one should act upon such information without appropriate professional advice, after a thorough examination of the particular situation.

Names presented are for illustrative purposes only and do not represent actual individuals or companies.

KPMG Forensic is comprised of multidisciplinary professionals from KPMG International member firms. Professionals in KPMG Forensic draw on extensive experience in forensic accounting, law enforcement, investigations, technology, fraud and misconduct risk assessment, anti-fraud risk controls, program design and implementation, asset tracing, computer forensics, and forensics data analysis.

KPMG Forensic assists organizations in their efforts to achieve the highest levels of business integrity through the detection, prevention, and investigation of fraud and misconduct. Our services not only help organizations discover the facts underlying concerns about fraud and misconduct, but also assist them in assessing their vulnerabilities to such activities, and developing controls and programs to address these risks.

Special recognition is given to Patricia Tilton and Gail Bonitati of KPMG LLP's Forensic Group for their contributions. The views and opinions are those of the authors and do not necessarily represent the views and opinions of KPMG LLP.

Patricia Tilton, Partner
KPMG LLP
90 S. 7th Street
Minneapolis, MN 55402
Telephone: 612-305-5384
E-mail address: pmtilton@kpmg.com

Chubb Group of Insurance Companies
Warren, NJ 07059
www.chubb.com

Form 14-01-0044 (Rev. 8/06)