PAYROLL FRAUD

Hidden Dangers in Every Transaction

Lowers Risk Group – Risk Mitigation White Paper Series

LowersRiskGroup™
Protecting People, Brands, and Profits

(540) 338-7151 | www.lowersriskgroup.com

PAYROLL

BACKGROUND

Payroll, like fraudulent billing schemes, relies upon false documentation being used to cause the victim company to make a fraudulent disbursement. False documents might include such items as a false employment application, false W-4, false I-9 forms, fake driver's license and social security card, or fraudulent time reports. Payroll schemes make up about 9.3% percent of the cases of fraudulent disbursement of cash with a median loss of $48,000 which ranks fourth among the cash disbursement scheme types. Given that the total lost revenues due to fraud and abuse are estimated to be over $3.5 trillion annually worldwide, 9.3% of that figure is very significant.[1]

In general, payroll schemes are one of two types: "Ghost employees" or "False Submissions" of hours or salary. The term "ghost employee" refers to a phantom or non-existent employee. The person is on the payroll, but doesn't actually work for the victim company. In some cases the ghost person is real, but is also a friend or relative of the employee who is perpetrating the fraud.

In order for a ghost-employee scheme to work, several things must happen:

1. The ghost must be added to the payroll or be in the system as an active employee.
2. Some method must be devised for creating pay due to the ghost. In some cases, it could be false time and wages for an hourly employee. Another way might be to get the system to generate a payment for a non-taxable payment, such as a relocation payment.
3. A paycheck or pay advice must be issued to the ghost and such issuance concealed from anyone else.
4. The check or funds must be delivered to the perpetrator or an accomplice.

TYPICAL/EXPECTED HIRING AND PAYROLL PROCESSES

A. **Hiring**

1. The applicant completes a standard employment application accompanied by an authorization that contains a release that allows the employer to conduct pre-employment screening. This release should be constructed to allow the employer to conduct similar

[1] Report to the Nations on Occupational Fraud and Abuse, 2012.

checks at any time to update the information. Screening should be performed in line with the competing business factors of risk tolerance and budget. Best practice programs evaluate the business drivers that compel an organization to conduct screening and implement a methodology that delivers to them. Regardless the specific methodology, all best practice screening programs must include the following components.

- Identity Verification

  The value of all screening activity is dependent upon the logical connection between the subject being screened and the data in the records being researched. Given this, it follows that the identity of the subject must be vetted prior to executing searches. This is particularly true for criminal records searches. Because criminal records are stored and disseminated to the public in name indexes, a dishonest subject need only change their name or vary a critical identifier to avoid their criminal past being uncovered.

- Scope Determination

  If a jurisdiction is not searched where a subject committed crime, that information will not likely be found. This may sound patronizing, but the fact is that our court system is divided into roughly 3300 jurisdictions comprising of more than 10,000 individual courts. These jurisdictions do not communicate well with each other; determining where to look is vital.

  Once the identity of the applicant has been established, the information gained should then be cross-referenced with the subject's address history. The jurisdictions where a subject has resided, worked, been educated, paid bills, and had mail delivered for the last 7-10 years should be part of the best practice scope determination. All names developed from the application, release, and/or identity verification activity should be added to the search criteria within these jurisdictions.

- Search Fulfillment

  Dependent upon the search conducted, a best practice program will utilize that authoritative source to make certain information used in a hiring decision is the most accurate and up-to-date available.

  The use of database information without authoritative source confirmation is at best irresponsible and potentially illegal. The advantage of a database tool is its potentially broad scope; the challenge is its depth. As a best practice, database information should only be used as a pointer to determine where more detailed information might reside.

A comprehensive list of screening components and the order in which a best practice program would employ them is as follows:

Identity Verification

- Social Security Locator
- Database Criminal Research
- Internet Research

Scope Determination

- Legal Names
- Jurisdictions

Search Fulfillment-Criminal

- Federal Criminal Records Search
- Local Criminal Records Search

Search Fulfillment-Position Related

- Credit Report
- MVR
- Drug Testing

Search Fulfillment-Credentials

- Employment History Verification
- Education History Verification
- Professional License Verification

- Evaluation

Once screening is completed, a Consumer Report is generated and routed to the appropriate process-determined recipient. The evaluation of the information contained in the report is no less critical than the preceding steps of the process. The evaluation must demonstrate that the End User has applied their standards consistently and with cause.

While not strictly a matter of law, the EEOC has issued guidance to employers regarding their use of information contained in background checks, drawing out the

potential disparate effect these checks can have on protected classes particularly in dense urban demography. End Users of Consumer Reports should heed this guidance outside the employment context when evaluating reports for independent contractors and their employees. An absolute bar for existence of a criminal record without business necessity is highly discouraged.

The best practice evaluation method balances the need to treat all applicants in a non-discriminatory manner and protect the workplace. This is accomplished by creating rejection criterion contrasting business necessity and position risk against criminal or other irresponsible behavior. These criteria must factor the age and nature of the offense or act and its relevance to the job or position being sought. Criteria should also be sensitive to a pattern of irresponsible behavior rather than a single act.

Criterion must then be applied consistently and properly documented to be defensible. Best practice programs should route all reports containing potentially exclusionary elements to an appropriately trained and skilled manager for adjudication against the policy of the company

2. Once an application is completed, several different scenarios can exist for hiring:

- The hiring and payroll process are centralized. The application is reviewed at the central location and all pre-employment screening is conducted by the central office or is done by a vendor that is managed by the central office.

- The application is reviewed at the local office and pre-employment screening is conducted locally in accordance with company directives. In other instances, the application and release are forwarded by the local manager to a company-approved pre-employment screening agency. The results are returned to the local manager. Prior to an employment offer being extended, the local manager must forward the application and the results of the pre-employment screening to the corporate HR office for review and approval.

- The local manager has complete authority to screen and hire. Corporate policies may or may not exist to govern the process.

The first option is considered the most controlled and desirable, but is often the slowest. To overcome this obstacle, many companies incorporate "provisional employment" in the hiring process. This allows an individual to be hired contingent upon the results of the pre-employment screening. In this situation the applicant typically signs a letter acknowledging his provisional employment status.

- The hiring authority approves the application and the results of the pre-employment screening. An offer of employment is extended that identifies the position and rate of pay.
- The applicant accepts, in writing, the offer of employment. A W-4 and other payroll documentation is completed and returned to the hiring authority.

B. **Payroll**

1. The hiring authority provides the payroll department (part of Finance) with a copy of the signed Offer Letter and Acceptance Letter along with the W-4 and any other required documentation.

2. The payroll clerk enters the new employee into the payroll system. The change is verified by a second employee and validated with the original documentation from HR. This serves as a dual control over the process.

    - The system should automatically generate a report when the change is made.

    - As an alternative, the system would generate an automatic monthly report.

    - In either case, the report is sent to the departmental manager of the new employee and the payroll clerk has no capability to prevent the report from being sent.

3. For hourly employees, hours worked are entered on time cards or into a computerized time-collection application.

4. The employee's time is tallied and verified by the supervisor regardless of whether the time is submitted manually or through a computer program.

5. The verified timecards are signed by the supervisor and forwarded to the payroll department. If the system is automated, the supervisor must log onto the program, review the time, and submit it to payroll.

6. Unless automated, the payroll clerk enters the time into the payroll system.

7. Trial payroll runs are made and reviewed under dual control, i.e., Payroll Supervisor and an accounting manager separately review the run and sign off on it.

8. Based on the trial run, funds are transferred by wire transfer from an operational account to a payroll account for the exact amount of the payroll.

9. Funds are directly deposited from the payroll account to the employee's accounts where direct deposit has been authorized. "Pay Advices" are sent to or delivered to employees.

10. If manual checks must be issued, checks are printed and the check run is reconciled under dual with the payroll documentation prior to the checks being mailed or immediately thereafter.

COMMON VULNERABILITIES

A. Hiring

1. Hiring policies are inadequate to ensure proper pre-employment screening.
    - Corporate HR is unaware of what resources are available to conduct pre-employment screening.
    - The HR budget does not permit conducting pre-employment screening at an adequate level.
    - HR is misinformed as to what is legally permissible regarding pre-employment screening.
2. Corporate HR staff conducts little or no review of the actions of local hiring managers. In some cases, this is due to inadequate staffing at the corporate level. In other cases, there is a conscious decision made to decentralize the hiring process because of autonomous business units established through acquisitions and mergers.

B. Payroll

1. In small to mid-size companies, payroll is often part of the HR department. As a result, dual control or separation of duties is frequently lost.
2. In small to mid-size companies, the payroll accounting function is not independent of the general ledger function.
3. There is often poor accountability of vacation and sick leave. As a result, these items are sometimes subject to abuse.
4. Supervisors often fail to do an adequate job of tallying and verifying the hours worked of their employees. Some computerized systems allow the supervisor to access and change the employees' time records.
5. Many systems do not have, or don't use, the capability to produce reports when employees are added to their payroll. Many places do not ask supervisors and managers to periodically review and validate the names of the employees on their payroll.

6. Reconciliation is often not done of the payroll bank account statement and cancelled checks with the payroll.

7. Payroll registers are often not reconciled with the general ledger control accounts.

ESSENTIAL CONTROLS

1. Payroll policies and procedures have been incorporated into a written document; the document is current and contains all essential controls contained herein.

2. Additions of employees to payrolls must be approved by the Director of Human Resources; approvals should only be granted after formal offers of employment have been extended through HR and accepted by the applicant.[2]

3. Addition of names to the payroll database is restricted by terminal access, application access, user name, password, and user rights.[3]

4. Additions or deletions to departmental payrolls appear in automatically generated exception reports or scheduled monthly reports to the departmental supervisor.[4]

5. Documentation is maintained to support all additions, changes, or deletions to the payroll system. Departmental supervisors are required to verify payroll listings at least quarterly.

6. Hourly employees' time is recorded by time clock entry or computer.

7. Any manual entry to a timecard must be approved by the employee's supervisor or manager.

8. Manual timecards of employees are tallied by the supervisor before submitting to the payroll department. For on-line systems, the supervisor reviews the employee's submitted time and approves it.[5]

9. Monthly reconciliation occurs between the payroll ledger and the HR employee list by someone outside the payroll department.

[2] In small to mid-size companies, this function is not formalized and is left up to the hiring manager.
[3] In those companies where there is not appropriate separation of duties, a single user might be able to create a new employee, add the employee to the payroll, set the employee's wages, and enter time for the employee into the system.
[4] The person entering the data should not have the capability to prevent the reports from being generated.
[5] In an automated system, the supervisor would not have access to the employee's time until the employee submitted it. If changes had to be made once it was submitted, the employee would have to log back on, make the changes, and then re-submit it for the supervisor's approval. Any such action should generate an exception report for later review by management or auditing.

10. Payroll checks are drawn on an account used exclusively for the payroll purpose. The amount of funds transferred to a payroll account from operating funds each pay period should be determined by the payroll program. Wire transfer instructions should reflect the exact amount of the payroll.[6]

11. To the extent possible, payroll is distributed in the form of "direct deposit" to each employee's bank account.

12. Documentation (i.e., voided checks) used by payroll to set up direct deposit of payroll checks is destroyed immediately; destruction is done in a secure manner.

13. If manual checks must be issued, checks are printed and the check run is reconciled under dual with the payroll documentation. The person authorizing the check run should not have the authorization or capability to retrieve the printed checks or the documentation regarding the check run.[7]

14. If payroll checks are used for any employees, the payroll department distributes the checks. They are not given to departmental supervisors or managers to distribute, nor are they normally mailed.

15. Payroll checks are given to individuals based upon personal recognition or after presentation of proper employee identification.

16. In order to detect possible kickbacks to supervisors, exception reports are generated for those departments having overtime or incentive pay that is outside established parameters.

17. Periodic audits of employees' paychecks or earning statements are conducted to validate the deductions from pay and benefits. Errors are investigated.

18. Terminated employees are removed from the payroll database prior to the next pay period.

19. At least annually, an audit is conducted to compare the master payroll records of HR (written) with the computer generated payroll record. Variances are investigated.

---

[6] Prior to the transfer of funds, the "trial run" payroll should be reviewed under dual control and approved. The review should include, at a minimum, the following:
(1) Valid names of employees
(2) Hours worked
(3) Wage rates
(4) Deductions
(5) Unusual items

[7] Any attempts to modify the print file (i.e., change a payee) should cause an automatic exception report to be generated. Prior to the checks being mailed, the check run should be reconciled with the payroll documentation by a second person. Any discrepancies should be investigated.

20. The payroll accounting function is independent of the general ledger function.[8]

21. The IT department has no access to the HR or Payroll application programs.[9]

COMPENSATORY MEASURES

1. **Hiring:** There is no substitute for adequate pre-employment screening and every effort should be made to move a company to adopt "best-hiring" practices As an interim measure, companies should at least do the following:

    - Ensure the company's employment application process includes having the applicant sign an adequate release.

    - At a minimum, require more in-depth screening for applicants who will fill positions that will permit access to financial records, or who can enter data regarding any type of financial transaction, or whose approval is required before disbursing corporate funds. Require that corporate HR and management review the employment application and screening file prior to an offer of employment being made.

    - If an offer of employment MUST be made prior to completion of all pre-employment screening, ensure such employees are hired provisionally, pending the outcome of the results.

2. **Payroll**

    - Internal audit or corporate security should utilize fraud detection software to analyze employee database files for duplicate names, duplicate addresses, duplicate bank accounts, duplicate or invalid social security numbers, P.O. boxes, mail drop addresses, terminated employees, or other potentially fraudulent data.

    - Where local managers have hiring authority, the audit department should match payroll records with HR files. They should also conduct reviews of the employee hiring files and, for a certain percentage, verify the data contained in the files.

[8] If these two functions are not independent, then it becomes much easier for the payroll accountant to hide illegitimate payroll transactions by coding them to obscure or un-reconciled portions of the general ledger, such as those that would not produce a W-2.

[9] Because of their unique privilege as "super users" of the corporate computer systems, IT personnel are positioned to create users and privileges to which they are not entitled or to manipulate data or operations within applications. Consequently, Payroll and HR systems should be beyond the reach of IT personnel if possible.

- Analyses should be conducted of the deductions of payroll checks. Ghost employees will often have no withholding taxes, insurance, or other normal deductions.

- Payroll MUST be reconciled by personnel not responsible for its distribution and reconciliation.

CASE STUDY #1: "SuperUser"

The Manager started employment with ABC Company as a staff accountant in September of 1991 and rose through the ranks to become the Director of Financial Services for ABC Technical Services in August of 2004. According to the FBI's review of the banking records of the Manager's primary account, the Manager began issuing up to three checks to himself each payday in 2000, usually ranging from $1,500 to $3,000. This process continued to an undetermined date (but believed to be in December of 2002) when ABC Company changed to the PDS system of direct deposit. The total amount of the fraudulently issued checks has not yet been determined.

On January 1, 2004, ABC Company began a new program for direct payroll deposit using the PeopleSoft application. Using his "SUPERUSER" status for the PeopleSoft program, the Manager fraudulently converted four previously terminated employees to active status and set up their payroll accounts to have their disbursements deposited into his bank account. From June 18, 2004 to July 27, 2006, the Manager processed direct deposits for these re-activated former employees totaling $498,149.40. All of these funds were deposited into his personal account at Secure Bank.

Laying The Foundation For Fraud: The first step was to create a location where employee payments could be hidden and also not have a W-2 generated. On an unknown date, a "table" was created within PeopleSoft for earnings described as "Non-Tax Relocation" or NTR. The effective date was set as 01/01/1930. According to an explanation provided to the investigator, using such a date would ensure that no data would ever be entered subsequently that would be rejected because it was outside the effective date. It should be noted that the program does not document who took these steps, but they were steps that were required for the fraud to be successful.

A second safeguard was implemented, presumably by the Manager also. The mapping for these Non-Tax Relocation (NTR) earnings to the General Ledger was set to the Insurance Benefits account. According to the Chief Financial Officer (CFO) at ABC Company headquarters, this account is extremely difficult to reconcile because of the large volume of transactions that flow in an out of that account on a daily basis. Consequently, in the words of the CFO, "It was unlikely that anyone would have noticed the additional money."

The next step taken was to use the PeopleSoft program features to reactivate four previously terminated ABC Company employees. Screen shots from the PeopleSoft program are available that verify the termination dates for all employees. The following four individuals were used and their termination dates are identified below:

- Charles Jones: June 26, 2003
- Clark Vinson: September 10, 2003

- Robert Jensen: January11, 2004
- Gary Trudenski: July 9, 2004

Screen-captures from the program reveal that Charles Jones was restored to active status on June 15, 2004 (effective May 15, 2004) and Clark Vinson on August 24, 2004 (effective October 1, 2004). Documentation on the other two employees, Robert Jensen and Gary Trudenski, has not yet been provided by ABC Company. It should be noted that the program does not retain an audit trail of who made the changes.

At the same time that Clark and Vinson were restored to active status, their direct deposit information was set to match the bank transit number and account number of the Manager. Documentation has not yet been received from ABC Company as to when Jensen's and Trudenski's bank transit number and account number were changed to match that of the Manager.

Payments Begin (Through PeopleSoft): The next pay period after setting up the banking routing and transit numbers, the first direct deposits were generated for Clark and Vinson into the Manager's account. Records from the PeopleSoft program show the first direct deposits from each of the four individuals were as follows:

Name	Pay Ending	Issue Date	Pay Advice #	Amount
Charles Jones	6/10/2004	6/18/2004	51876	$2,027.38
Clark Vinson	8/19/2004	8/27/2004	74902	$2,760.50
Robert Jensen	8/19/2004	8/27/2004	74888	$2,691.56
Gary Trudenski	8/19/2004	8/27/2004	74908	$3,063.12

As a result of running a specific query in the PeopleSoft program, the staff at ABC Company Headquarters was able to determine that these payments were the result of pay sheets being manually created by a user as opposed to coming from the Time and Labor portion of the program. Again, the system lacked specific audit trails to determine which user manually created the pay sheets to generate the direct deposits. However, it would have been accomplished during that portion of the payroll processing that the Manager always performed.

Total Fraudulent Payments (Through PeopleSoft): Following is a summary of the fraudulent direct deposits received by Manager from the payroll accounts of Jones, Vinson, Jensen, and Trudenski:

Name	Issue Period	Number of Deposits	Total of all Deposits
Charles Jones	6/18/2004 - 7/27/2006	53	$252,632.14
Clark Vinson	8/27/2004 - 7/27/2006	48	$239,762.49

Robert Jensen	8/27/2004		1	$2,691.56
Gary Trudenski	8/27/2004		1	$3,063.21
		TOTAL	103	$498,149.40

Attempted Digital Cover-up: The PeopleSoft program normally keeps monthly, quarterly, and year-to-date balances of all payroll accounts. This data is used in the preparation of W-2's. It would be important for the perpetrator of this fraud to eliminate those balances. The investigator reviewed documentation that revealed that the payroll accounts of Jones and Vinson had been adjusted at the end of 2004 and 2005 so that their earnings balances were zero. According to the documentation reviewed by the investigator, the system does not record who made these changes.

Fraud Discovery: The fraud could have possibly gone undetected for a much longer period of time if not for an effort by a payroll staff member to improve efficiency. A special system query was established in order to segregate the Pay Advices of terminated employees from other employees for mailing purposes. It is normal for terminated employees to have a final paycheck or deposit to be processed to clear up unused vacation or sick pay or similar benefits. So the appearance of recently terminated employees through such a query was to be expected. What was unexpected, however, was the appearance on the query results of two employees (Clark Vinson and Charles Jones) who were terminated in 2003. What was even more unusual was the fact that no Pay Advice for these two employees could be located, even though the appearance of their names on the report was indicative of the fact that a Pay Advice had been issued. The Payroll Supervisor verified the fact that earnings for the two terminated employees had been generated in the system and that the direct deposit for both employees were going to the same bank and same account number. Research by the Payroll Manager revealed that this account belonged to the Manager and that the fraud, using the PeopleSoft program, had been transpiring since the pay period for June 10, 2004. The matter was then brought to the attention of senior management at ABC Company International.

CASE STUDY #2:

"How a Contractor Lost $1.9 Million to Embezzlement"

By Katie Rotella

Laura Peggy Hartley was a trusted employee of Marlin Mechanical Corporation. The Phoenix-based company hired her in 1991 as payroll and employee benefits administrator, and she was a diligent yet friendly worker for more than eight years.

Co-workers found the 51-year-old Hartley to be sociable and loyal. They knew she would go toe-to-toe with the insurance agencies when they needed help. She was a past president of the Women's Auxiliary of the local Plumbing-Heating-Cooling Contractors, and very involved in the organization. She had a dominating presence that demanded attention.

Hartley's devotion to her job continued through the years and even became stronger, according to Marlin's owners Mark Larson and Mark Giebeihaus. She took few, if any, vacations, opting instead for long weekends, picking and choosing her days off carefully. She was not away from her desk for more than a day or two at the most.

So it was difficult for the company to let her go in April 1999 when she violated a company confidentiality clause by disclosing pay rate information and health records to other employees. She was given a month's salary and asked to leave.

However, it was far more difficult to believe only a month and a half later that this same loyal employee, runner up in 1998 as the NAPHCC's Auxiliary Woman of the Year, had embezzled nearly $1.9 million dollars over the course of eight years.

"She worked for us for so long and did a good job," said Giebelhaus, still shaking his head in disbelief and disgust. "There was no reason to suspect anything."

Employee Dishonesty: Theft in general is always a hard-to-swallow reality when running a business. But being a victim of internal theft guarantees a lump in your throat. Take a bite out of these facts from the U.S. Small Business Administration:

- Almost two-thirds of theft comes from employees.
- Nearly one-third of all bankruptcies are caused by internal theft.
- Employees steal more than $1 billion a week from their employers nationwide.

One of the main reasons internal theft thrives is that management continues to believe in myths and misconceptions about the nature of dishonest employees. They surround themselves with a false sense of comfort saying, "It could never happen to me, my guys are loyal." But all too often warning signs are ignored, and it's too late to curtail the crime.

The folks at Marlin found out the hard way that there is no stereotypical thief. Like a book, embezzlers can't be judged by their cover. They can be old or young, male or female, new hires or seasoned workers, field technicians or executives; they could even be friends or family members.

Hartley had been in a position to dominate the woman she trained for the sales clerk position, and ultimately subverted the authority of the company. Almost every week for eight years she signed and cashed bogus insurance checks into her own bank account. In the last few months of her employment, she was pilfering more than $40,000 a week. She stole to the degree that the system allowed, and didn't stop until she was caught.

What makes embezzlement different from robbery or larceny is one word - "trust." By definition, the "fraudulent appropriation of property or funds" by a person you trust can leave you feeling vulnerable from all sides. The best way to avoid being a victim of embezzlement is to have a system of internal controls in place to safeguard your business and profits.

Understanding Why: Employees steal more as a result of opportunity rather than need. They usually believe they're smarter than their employers and can beat the system, so it's important to be familiar with some of their common schemes:

- Simple Embezzlement - An employee receives cash and he pockets it without recording the transaction. This type of theft is hard to detect if there is no subsequent transaction entry required in accounts payable. By pre-numbering your sales invoices or receipts, you can reduce the temptation to steal. Having regular monitoring procedures also ensures your sales are being recorded.
- Lapping - A temporary withholding of receipts for personal use. For example, an employee receives a check as payment on an open account. He holds out a $100 cash payment made by Customer A on April 1. To avoid getting caught, another $100 is taken from a $200 payment by Customer B on April 5. This is sent on with proper documentation to the accounts of A. The employee pockets the remaining $100, increasing the overall shortage to $200.

Fraud of this nature can go on for years without detection. It requires detailed record keeping on the part of the embezzler, who has to remain one step ahead at all times. Like Hartley, the thief is likely a person given more authority than the position calls for and s/he will steal until s/he is caught. Something unusual has to happen to bring the crime to light, such as a customer complaint or unexpected time away from the job for the embezzler.

When Hartley was fired in April, her scheme was uncovered because she could no longer manipulate accounts and records for her own use on a daily basis. The company's sales clerk and controller began to wonder why insurance checks were arriving only once a month instead of every week as before. It didn't take long to follow the paper trail back to Hartley.

One reason many businesses require a regular vacation is to keep indispensable employees from dispensing company funds. An employee who is hesitant to delegate his work to others, or keeps track of business transactions outside his regular accounting books could be stealing your profits.

- Payroll Fraud - A payroll administrator adds bogus names to the company payroll and collects several salary checks each week. This is easy to spot in smaller mom-n-pop shops, but as a business grows, or experiences high turnover, the temptation to pad his own wallet might be too great for an enterprising embezzler. To curb this type of theft, make sure no one is placed on the payroll without your permission. It's also a good idea to have the preparation of the payroll handled by a separate person from the one who actually pays the employees - especially when cash is involved.
- Computer Crime - Dishonest employees can divert funds and goods for their personal gain. Small businesses understand the importance and ease of computerized data, but it also makes it easier for embezzlers to attack your profits. Personnel records, inventories, receivables, payables, bank accounts, and all other records are sometimes contained on a single computer or computer network to which several "trusted" employees have full access to all programs and applications. Managers, supervisors, and employees should never have access to data and applications beyond their need.

What's Next? "We've stopped the bleeding," said Giebelhaus of the company's loss and new outlook on employee dishonesty.

With the help of the Phoenix and neighboring police departments, Hartley was apprehended, convicted, and sentenced after a plea bargain was settled. Her lawyers had hoped to cap her jail time at five years (the minimum for the felony charge she pleaded guilty to), but the judge sentenced her to eight years in a state prison.

Though this was a first-time offense, the judge called Hartley a "serious repeat offender," who betrayed the trust of her employer and co-workers. She could face more jail time and hefty fines from the IRS for failure to pay taxes on the money she stole.

When Hartley was arrested, about $38,000 was recovered from her. Another $30,000 was recovered from her daughter, whom she had given several gifts, loans etc. over the years. Marlin's insurance company handed over a $130,000 check for the company's dishonest employee coverage. But, according to the owners, Hartley spent most of the money she stole buying gifts for friends and gambling away a large portion.

The grand total of her theft may never be known, and will never be fully recovered. Though no drastic changes were made to the internal checks and balances of Marlin Mechanical, the company hired a human resources director in September to clean up all employee issues and help

perform background and reference checks on new hires. Also, all bank statements and canceled checks are now forwarded to Giebelhaus' home instead of the office.

"Even with the amount she took we've had a good year," Giebelhaus admits. "But the largest impact of the loss was to the other employees. She really stole from them." Her actions reduced the share price the employees had invested in the company, and has cost them their yearly bonuses for the past few years. "You hate to see someone you've known and trusted for eight years go to prison, but she's paying for what she's done. She devalued the company and its 130 employees," Giebelhaus said in a statement he made in front of the judge, Hartley, and 30 Marlin employees in an Arizona courtroom. They all were satisfied as the "clink" of the bailiff's handcuffs echoed in the courtroom when he led her away.

Reprinted with the permission of Business News Publishing ©2002

CASE STUDY #3:

Downsizing Exposures

By David Elzinga, CA , CFE

The trend toward downsizing has eliminated some layers of control within companies and opened the door to fraud. This was the case with one large firm that had eliminated several senior positions, including the manager of the payroll department. As a result, only a supervisor and two clerks ran payroll.

On a Friday afternoon about three years after the downsizing, the company's security manager received a disturbing call from one of the payroll clerks, who told the following story. Her supervisor, in a mad dash to get away on vacation, had asked for an advance on his next paycheck. When she attempted to process it electronically (the company's payroll was by automatic bank deposit), the bank rejected the deposit because the account had been closed. (It later emerged that the bank had closed the supervisor's personal account due to suspicions of fraud by the supervisor.) She called the supervisor, who was on his way to the airport, and he told her that he'd changed banks and gave her the new account number. When his new bank confirmed receipt of the advance, the amount they confirmed was three times more than the amount she'd authorized. "Something isn't right," she told the security manager, who agreed.

The security manager decided to conduct a two-pronged investigation. He began a discreet check into the supervisor's background for signs of a recent change in lifestyle, one of the potential indicators of fraud. He also received management's approval to retain forensic accountants to examine the payroll system.

His background investigation revealed that the payroll supervisor was recently divorced and now living with a girlfriend. According to office gossip, he was spending lavishly on his new relationship. Other rumors suggested that he was buying and using drugs.

Meanwhile, the forensic accountants, following interviews with the payroll clerks to understand the payroll system, identified several red flags. The first was the supervisor's refusal to allow the clerk responsible for processing the payroll to have a computer in her office. Instead, she had to use the supervisor's computer to download the payroll files, which were then sent to the bank.

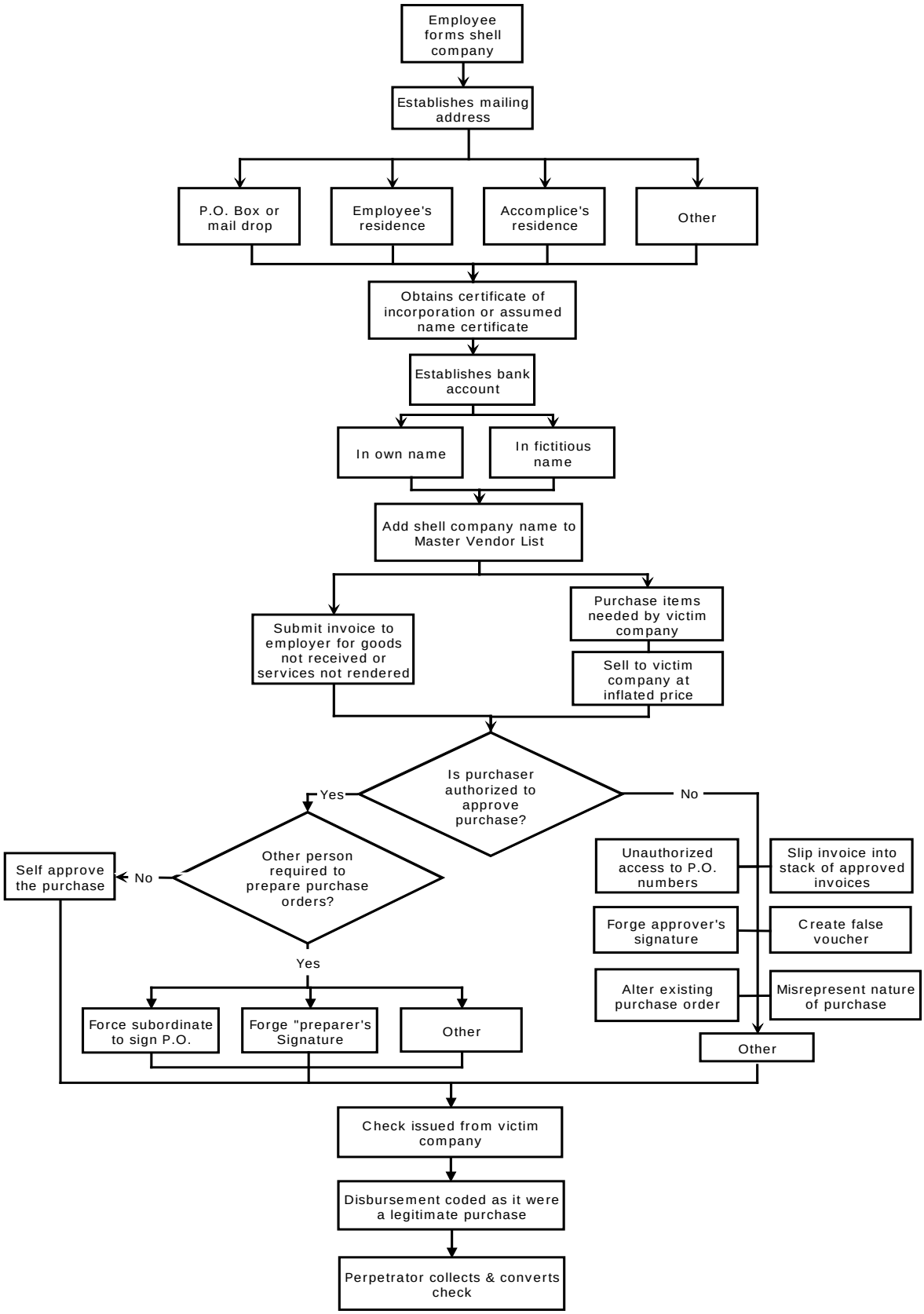
They also noted that the payroll supervisor developed and programmed the payroll system and did all the troubleshooting himself. Combined with the security manager's findings, these unusual and highly controlling behaviors led to the conclusion that the payroll supervisor was manipulating the system to his financial advantage. At this point, however, they had no proof; the company's records (which he was also manipulating) showed no evidence of any fraud. The proof was likely in the payroll supervisor's banking records, but they had no access to them.

Puzzling over how the supervisor might be defrauding the company, the forensic accountants wondered whether the fraud was occurring after the payroll clerk had downloaded the files from the company's database onto the supervisor's computer. Since he controlled the system at that point, he could be altering the amounts for himself before they were transferred to the bank. If that were the case, the fraud would show up on the bank's records. The bank was the next stop.

Although physically located at the bank, the records were in fact the company's property. After meeting with the bank, the security manager obtained the records and gave them to the forensic accountants for analysis. Their theory proved correct, and they exposed a large-scale fraud.

It worked like this: The supervisor searched the company's files for recently retired or terminated employees whose payroll records had been deactivated. He then reactivated those employees, putting them back on the payroll. Because this was a huge firm with thousands of employees, including numerous contract workers who came on and off the payroll, no one detected what the supervisor was doing. After the payroll clerk electronically sent the payroll records to the bank, her supervisor would "unsend" the files before the bank retrieved them; the bank never knew the files had been sent. He then changed the banking information for the reactivated personnel so that their pay was deposited into his account. Each pay period he chose a few names and kept them activated for a short time, replacing them with others to avoid suspicion. Even if someone noticed unwarranted payments to a recently retired employee, for example, they would be attributed to a slip in the system. Since the payroll supervisor was in charge of investigating these types of problems, he essentially policed himself.

The supervisor kept the scheme going for three years by stealing little by little, continually switching among the employees he used to cloak the fraud, paying some of the taxes on funds diverted to his account as he went along, and adjusting the company's books. (His cover was finally blown when he failed to anticipate that his new bank would call the payroll clerk to confirm receipt of the deposit.) The scam netted him almost $150,000 over three years. During this time, the company received "clean audit opinions" from its external auditors because the supervisor was able to manipulate the records. Moreover, the internal audit department had conducted a compliance audit of the payroll with no major exceptions being noted. When he returned from vacation, the supervisor was confronted with the documentary evidence against him. He confessed his scheme and was terminated with cause. The forensic accountants' report was submitted to the company's insurance provider as part of a proof of loss on a fidelity bond claim. The company recovered its loss and the forensic accountants' fees. The report was turned over to the police, which used the evidence to prosecute and eventually convict the supervisor. He was also ordered to pay restitution.


Employee forms shell company
Establishes mailing address
P.O. Box or mail drop
Employee's residence
Accomplice's residence
Other
Obtains certificate of incorporation or assumed name certificate
Establishes bank account
In own name
In fictitious name
Add shell company name to Master Vendor List
Submit invoice to employer for goods not received or services not rendered
Purchase items needed by victim company
Sell to victim company at inflated price
Is purchaser authorized to approve purchase?
Yes
No
Other person required to prepare purchase orders?
No
Self approve the purchase
Yes
Force subordinate to sign P.O.
Forge "preparer's Signature
Other
Unauthorized access to P.O. numbers
Slip invoice into stack of approved invoices
Forge approver's signature
Create false voucher
Alter existing purchase order
Misrepresent nature of purchase
Other
Check issued from victim company
Disbursement coded as it were a legitimate purchase
Perpetrator collects & converts check

LOWERS RISK GROUP – Fidelity & Crime White Papers

There are three conditions that are present when fraud occurs: Opportunity, Incentive, and Rationalization. The information contained in these papers demonstrates examples of vulnerabilities and how applying essential controls can significantly reduce the risk of fraud.

ABOUT LOWERS RISK GROUP

Lowers Risk Group combines the services of three industry-leading companies – Lowers & Associates, Proforma Screening Solutions, and Wholesale Screening Solutions – to create a complete risk management service offering for organizations of all shapes and sizes. Employed in concert or on a standalone basis, we excel in providing comprehensive enterprise risk management and human capital risk solutions to organizations operating in high-risk, highly-regulated environments. Our specialized background screening and crime and fidelity risk mitigation services protect people, brands, and profits from avoidable loss and harm. With Lowers Risk Group you can expect an experienced and professional approach to your risk assessment, compliance, human capital, and risk mitigation needs to help move your organization forward with confidence.

Contact Information:

Lowers Risk Group
125 East Hirst Road
Suite 3C
Purcellville, VA 2 0132

Telephone: 540-338-7151
Fax: 540-338-3131
Email: info@lowersrisk.com
Web: www. lowersrisk.com