

# Protecting your company from internal fraud.

Volume

Business Whitepaper Series

3



JOHNSON  
BANK®



# From computer viruses to employee theft,

fraud is blind to the size or prominence of a company. The cost to your business to offset a loss, indemnify individual victims or financial institutions, or even cover court fees could be staggering. The best defense is a combination of tactics: internal controls, check and Automated Clearing House (ACH) security, periodic audits, and a strong partnership with your financial institution and insurance provider.

## On the Inside: Recognizing and Preventing Occupational Fraud

Since the earliest days of employer-employee relationships, there have been those who have had a reason, an opportunity and a rationalization for stealing from the company they work for. Even with modern awareness and tighter security measures, internal fraud remains one of the areas of greatest potential risk to any organization.

The most common types of internal fraud are asset misappropriation (e.g. money skimming, check tampering, payroll fraud, supply theft), corruption and falsifying records. They can happen in any department and at any level of seniority, although studies have shown that in the majority of cases:

- The fraud was committed by long-term, trusted employees, often with a position of authority
- Took an average of 18 months to detect
- Was the result of poor internal controls

## Recognizing Red Flags

Fraud is most often committed by employees who have financial problems and/or feel that they are somehow “owed” by their employer. Contributing factors can include drug, alcohol or gambling addictions. Common warning signs include a decline in work ethic, personality or life style changes, tips or complaints from others, and analytical anomalies in areas where the employee has access. Examples of these anomalies include:

- Unexplained changes in account balances
- Irregularities in source documents
- Missing or altered documents
- Photocopied rather than original documentation
- Incorrect endorsements on canceled checks
- Excessive debit or credit memos
- Cash shortages or overages

- Excessive late charges
- Unreasonable or changing expenses or reimbursements

To protect your company and help prevent internal fraud:

- Segregate duties so no one person is responsible for writing and signing checks, handling cash receipts, posting accounts receivable and reconciling bank statements.
- Control access to the vendor and employee master files within your accounts payable system.
- Limit the number of people who are authorized to sign checks.
- Secure important documents and information, including check stock, bank records, passwords, account numbers and endorsement stamps.
- Don't leave incoming or outgoing mail unattended.
- Conduct surprise internal and external audits.
- Insist on “mandatory separation” from work, i.e. at least five consecutive business days of vacation annually for employees.
- Perform pre-employment background checks and provide ethics training to all employees.
- Give employees access to only the computer files and applications necessary for their specific jobs.
- Offer a confidential way for employees to report concerns.
- Offer an Employee Assistance Program for employees struggling with dependency or other issues.

## Take Your Protection to the Next Level

Making fraud harder to commit can in many cases be deterrent enough, but no plan is full proof. In an era where some of the most reputable and respected entities like the FDIC, Small Business Administration and IRS have been falsely used as covers in phishing scams, every organization needs to be extra vigilant. Most financial experts agree that beyond the other common techniques outlined above, the four biggest methods of protecting your business are:

- 1 Reconcile accounts daily. Looking at your account activity online each day will help you catch unauthorized transactions within 24 hours—critical in preventing the money from being withdrawn. (Once it is, your chances of recovering the funds are unlikely.)
- 2 Use dual control. Having one person create transactions and a second authorized person approve the release of the funds prevents any one person from being in a position where he or she can embezzle money or siphon it off to other accounts.
- 3 Use security tokens. Ask your bank to provide strong authentication controls in addition to your user ID and password to confirm your identity when transferring funds. A common method is to provide you a device called a security token or key fob that generates one-time-use passwords.
- 4 Talk with your financial institution and insurance carrier. Ask about other cash management protection products and services like Check Positive Pay, ACH debit filters and ACH blocks, and consider adding fraud protection to your insurance coverage. Talk with your insurance provider to see which products are available and how a policy could be created to meet your business' current and future needs. Also work with your bank to make sure that—in addition to providing the best protection for your funds—they offer ongoing on-site training so your current and future employees are well trained and understand how their actions can affect your business. Finally, remember that no bank or vendor should ever call or email you to ask for a password or other sensitive data. Protect this information as if your livelihood depends on it—because it does.

## A number of products are available to help protect your business. These include:

- + Computer Crime Coverage (fraud and data restoration expense)
- + Funds Transfer Fraud Coverage (forgery, expense reimbursement)
- + Claim Expense Coverage
- + Fidelity Coverage (employee theft, ERISA fidelity, employee theft of client property),
- + Forgery or Alteration Coverage
- + On Premises and In-Transit Theft
- + Disappearance or Destruction Coverage
- + Money Orders and Counterfeit Money Coverage

## Additional Tips

- + Never click links or install programs suggested in emails that relate to your bank accounts, even if the email appears to be from an official or familiar source. Banks that value their clients' protection would never request sensitive data like passwords or financial information via email.
- + Always access online banking by typing the bank's address into the web browser rather than through a link that was emailed to you. (You would most likely be rerouted to a fraudulent site where your information could be collected.)
- + Be sure the site you are on is secure. Look for a closed lock in the lower right hand corner of the web page and make sure the website address begins with https://.
- + If you ever are in doubt about a request you receive, contact the bank separately via a publicly advertised phone number (e.g. the phone book, newspaper or television ad) to verify that what you receive is legitimate.
- + If you suspect fraud has occurred, act quickly. Involve your bank immediately, keep detailed records of what happened, and be sure the issues are thoroughly resolved and preventative measures are taken before reinstating your business procedures.

*This information is intended to be a general guide to understanding some of the fraud issues that are prevalent in business today. It is not intended to provide legal guidance.*

For more information, please call Johnson Bank at 877.236.2739. Johnson Financial Group is a premier financial services company offering comprehensive financial solutions in the areas of banking, trust, insurance and investment management through Johnson Bank and Johnson Insurance.

[johnsonbank.com/business](http://johnsonbank.com/business)

17909