



Cookson Walker Consulting

Fraud Alert

Safeguard Against Internal Theft

By Eric Walker and Paul Greenhow

Do you have controls in place to protect your organization from theft and fraud? Many privately-owned businesses, insurance brokers being no exception, are tending to concentrate the performance of operating and custodial accounting responsibilities among fewer staff, increasing their exposure to the potential misappropriation of assets, primarily cash.

For insurance brokers, misappropriation typically occurs in the form of employee theft of receipts, often hidden through the manipulation of premium receivable balances, known as "lapping," and third-party theft of disbursements through cheque fraud.

Lapping receivables is more common in the industry than brokers may think or care to admit. Fortunately, a portion of receipts stolen by dishonest employees may be recovered from fidelity bond insurance, which is mandatory in Ontario. According to the Registered Insurance Brokers Act, Revised Statutes of Ontario, 1990: "RIBO requires every member, or sole proprietor, partnership, or corporation to maintain fidelity insurance against losses arising from dishonesty of employees, a proprietor or partners, directors and shareholders in the amount of at least \$100,000 in respect of any one occurrence."

The minimum fidelity insurance level of \$100,000 is common. Theft in excess of \$100,000 results in a broker seeking redress from the employee or absorbing the loss.

Cheque fraud has been described by Frank Abagnale (a fraud consultant and former fraudster who cashed approximately \$2.5 million in fraudulent cheques and whose life was depicted in the film *Catch Me If You Can*), as one of the fastest-growing crimes in the United States. Cheque fraud losses in the U.S. have been estimated at \$20 billion a year and growing at an annual rate of 25 per cent. More than one million fraudulent cheques are written every day, more than 13 per second.

Similar Canadian statistics contained in a 1997 Neilson Fraud Survey Report indicate that the cost of cheque fraud in Canada is in the range of \$1 billion to \$2 billion each year.

So what can brokers do to prevent these types of theft and fraud? Most importantly, they must be cognizant of and understand the internal financial controls that should be in place to protect their business. Outside accountants can assist in understanding and improving these measures.

Lapping

Lapping, which is a common type of theft, occurs when accounting entries for the collection of receivables are postponed to conceal an existing cash shortage. An

employee who handles cash often perpetrates this type of theft and/or cheque receipts and then enters them into a computer system. He or she defers recording the cash/cheque receipts stolen from one customer and covers the resulting shortages with the receipt of cash or a cheque from another. These in turn are covered from the receipts of a third customer a few days later. The employee must continue to cover the shortage through repeated lapping or find another way to conceal the shortage.

Lapping can be easily prevented by separating the handling and recording duties related to cash and cheque receipts. It can be detected by comparing the name, amount, and dates shown on remittance advices with cash receipts journal entries and related duplicate deposit slips.

Consider some preventative accounting measures:

- The receptionist should open all mail and stamp all cheques received "for deposit only." The details of the receipts should be listed on a daily log and a copy of that log ought to be provided to the accounting manager.
- The cheques stamped "for deposit only" should be referred to an accounting clerk, who would make the daily deposit to the trust and general accounts.
- The accounting manager should record receipts from his/her copy of the log with reference to the bank deposit book
- The accounting manager should be responsible for follow-up collection activities, which would include sending monthly statements to all clients. Any exceptions must be approved by the controller/CFO/owner.
- Other additional procedures may be appropriate if the brokerage has cash sales (e.g., issue receipts to clients).

Cheque fraud

Cheques may be stolen from the premises of a broker or from mail and courier services. Stolen blank cheques can be filled out and deposited and subsequently withdrawn or cashed. Stolen issued cheques may be altered by cut and paste methods or by chemicals that lift and dissolve ink. New payee names and/or dollar amounts are then inserted by the perpetrator, who deposits the altered cheque into an account for ultimate withdrawal. Counterfeiters may use scanners to reproduce high-quality images of a stolen cheque from which they can manipulate the entire document, again changing payee and dollar amounts.

The existence of low-cost, high-quality scanners, colour copiers, laser printers and desktop publishing have all combined to assist criminals, arming them with sophisticated technology to forge or reproduce authentic-looking cheques.

Targets for these activities are typically organizations transacting in large sums of money, such as insurance brokers, whose handling of agency bill premiums often amounts to several million dollars annually, even for smaller entities. A broker employing five to 10 staff may transact in volumes of \$3 million to \$6 million a year. This level of activity could involve net premium payments of significant amounts to the key carriers of a brokerage. Brokers report that this type of theft often occurs through mail and courier services.

A number of "best practices" in preventing cheque fraud are provided by local police departments, Canadian banks, and Chartered Accountants, including:

- "Positive pay" automated services offered by banks that compare cheques issued on the payor's account to cheques presented for payment, usually at another bank. Unmatched items are brought to the payor's attention by the payor's bank, usually within the return item time frame. This protects the payor from unauthorized withdrawals.
- Lock up unissued cheques, cancelled cheques, cheque reorder forms and signature stamps to restrict employee and cleaning crew access. Audit unused cheques on hand on a regular basis.
- Unused cheques for closed or dormant accounts should be destroyed.
- Use quality cheque paper stock, with security features such as chemical protection, foil stamping, fluorescent fibres, padlock icons, microprinting and holographics.
- Use ink that permanently bonds to paper.
- Use a type font size of 12 points or larger as forgers erase smaller type and replace it with larger.
- Reconcile bank statements monthly and review returned cheques. Report suspicious or unusual items to your bank immediately. Reconciliation can now be performed daily by downloading transaction data from the bank to your computer.
- Segregate the preparation, reconciliation and signing of cheques.
- Centralize the issuing of cheques in the hands of authorized staff.
- Distribute mail at the post office, not at a drop box.
- Use electronic payment services for vendor payments and payroll direct deposits to reduce exposure to cheque fraud. These banking services offer access restrictive security services including primary and secondary levels of authorization.

When cheque fraud occurs, who is responsible? The answer is not clear and it depends on the circumstances. For example, if a cheque is approved by the disbursing bank and the bank has not reviewed the transaction with the payor as part of an agreed-upon service, the disbursing bank may be on the hook. However, if the payor approved the transaction and did not have, for example, positive pay service, the payor may have to absorb the loss. If the depositing bank does not institute a hold, or checks with the disbursing bank, it is possible the depositing bank is responsible for the loss.

Internal control primer

Internal control comprises the plan an organization and all the coordinated systems established by the management of an enterprise to assist in achieving management's objective of ensuring, as far as practical, the orderly and efficient conduct of its business, including the safeguarding of assets, the reliability of accounting records, the timely preparation of reliable financial information (CICA Handbook, 5200.03).

From a financial reporting perspective, financial controls can be divided into two categories, assertion and environmental. Assertion controls directly affect the reliability of financial information by preventing or detecting error or fraud in the recording of related transactions and balances.

Assertion controls include: Segregation of incompatible functions (e.g. custody, deposit and recording of cash, ideally involving three staff); completeness controls (e.g. prepared and reviewed bank reconciliations ensure no unrecorded cheques); authorization controls (e.g. approval of payroll or purchases); third-party controls (e.g. supplier statements, bank statements, insurer statements); accounting system controls (e.g. evidence of a complete system with general ledgers and sub-ledgers promotes accuracy); computer processing controls (e.g. processing error logs); systems implementation and conversion controls; restricted access to assets (e.g. signature authorizations); periodic count and comparison (e.g. supplies count), and computer operations controls (e.g. access codes).

Environmental controls indirectly increase the reliability of all financial information by creating an environment where errors or fraud are less likely to occur or more likely to be detected. They include: Organizational controls (e.g. honest and competent personnel who are carefully hired, fired, supervised and trained); systems development controls (e.g. computer system conversion, implementation and change plans and approvals); reporting controls (e.g. budgets/comparison to prior year results); management supervisory controls (e.g. review of financial reports); insurance and protection of records (e.g. off-site storage of backup programs and protection in the event of loss); documentation controls (e.g. computer operating instructions / procedures manuals)

Of particular relevance to preventing lapping and cheque fraud are segregation of incompatible functions, management supervisory, and authorization controls.

Good internal organizational controls are sometimes overlooked in the rush of providing good service or the push to get an administrative task accomplished. Investing time in protecting and safeguarding your hard-earned cash should also be part of the everyday conduct in a broker's business.

For more information, Eric Walker and Paul Greenhow of Cookson Walker can be reached at (416) 368-7990, or ewalker@cooksonwalker.on.ca and pgreenhow@cooksonwalker.on.ca.