SPECIAL REPORT

WOULD YOUR BANK PROTECT YOU IN THE EVENT OF A FORGERY?

THE SIGNIFICANT PROTECTIONS AFFORDED BANKS UNDER THE UCC AND CUSTOMER CONTRACTS REQUIRE CRITICAL ANALYSIS OF YOUR COMPANY'S CRIME INSURANCE COVERAGES

(07-17-2014)

This Special Report was written by Daniel P. Hale, J.D., CPCU, ARM, CRM, LIC, AIC, AIS, API of Marsh & McLennan Agency LLC. Mr. Dan Hale can be contacted at 734-525-2429 or dhale@mma-mi.com. More Special Reports are available at www.mma-mi.com.

Many organizations are under the impression that their financial institution would back them up in the event of a forged check is cashed on the company's account. This is not necessarily the case given the wide ranging protections under the Uniform Commercial Code (UCC) and the contract between the bank and the customer.

In most situations, banks will rely upon the obligation of its customer to review their own bank statements and to exercise care in avoiding incidents of forgery, including checking the back-grounds of employees.
This Special Report contains a real-life example of a denial by a bank of a six figure loss involving employee theft through forgery.

The protections afforded to banks should cause companies to carefully review their commercial insurance programs for adequacy. Such coverages involve more than employee dishonesty coverage and include insurance for forgery of checks by non-employees (called "depositor's forgery coverage"), theft by non-employees over computer net-works or systems (called "computer fraud coverage"), and other areas.

Crime insurance forms can vary widely, and you must examine the specific provisions of your employee dishonesty coverage in conjunction with your insurance counselor or risk manager.

Coverage for Incidents of Forgery May Be More Important Than You Think

Computer technology has enabled some thieves to take properly issued checks and to change the amounts for which the check was issued. Further, aside from this, there is the age-old problem of employee embezzlement of company funds through check forgery schemes.

Many employees think that any forgery of checks is the responsibility of the drawee bank. This is not always the case. In fact, the Uniform Commercial Code (UCC) and bank documents substantially limit a depository institution's liability in the event of a forgery. One bank-customer contract reads as follows:

> "You are responsible for monitoring and reviewing the activity of your Account and, if applicable, the work of your employees, agents, and accountants. Toward that end, Business Account Owners should have at least two (2) individuals inspect statements on a regular basis to look for improper and unauthorized signatures, alterations, forged endorsements, overpayments and any other irregularities and to insure that the accounts are being handled in a proper manner."
>
> "The customer has thirty (30) days from the time of the [bank's] mailing of the statement to you, to notify [bank] of any discrepancies."

The Uniform Commercial Code also provides significant protections to banks including the following:

> "A person whose failure to exercise ordinary care substantially contributes to an alteration of an instrument or to the making of a false signature on an instrument is precluded from asserting the alterations or the forgery against a person who, in good faith, pays the instrument or takes it for value or for collection." UCC 3-406.
>
> "If the bank sends or makes available a statement of account or items pursuant to subsection (a), the customer must exercise reasonable promptness in examining the statement for the items to determine whether any payment was not authorized because of alteration of an item or because a purported signature by or on behalf of the customer was not authorized. If, based on the statement or items provided, the customer

should have reasonably discovered the unauthorized payment, the customer must promptly notify the bank of the relevant facts." UCC 4-406(c).

"If a bank proves its customer failed, with respect to an item, to comply with the duties imposed on the customer by Subsection (c), the customer is precluded from asserting against the bank:

* * *

(2) The customer's unauthorized signature or alteration by the same wrongdoer on any other item paid in good faith by the bank that the payment was made before the bank received notice from the customer of the unauthorized signature or alteration and after the customer had been **afforded a reason-able period of time not exceeding 30 days** in which to examine the item or statement of account and notifying the bank." UCC 4-406(d) (emphasis added)

Banks are not hesitant to rely upon the provisions of their contracts and the Uniform Commercial Code to deny liability to their customers arising out of forgery. The following is an excerpt from a letter that a bank sent to its customer after the customer asked the bank to reimburse it for not catching an employee's embezzlement of funds through forgery:

"Based on the above-referenced facts as [we] understand them, and on the above-referenced sections of the UCC and the Contract governing the Account, [company's] failure to notify [us] within thirty (30) days of receiving its May 2002 statement (the statement which revealed the beginning series of alleged multiple forgeries by [employee]) precludes [com-pany] from asserting the claim against for any of the subsequent forgeries by [employee]."

"Moreover, regardless of the 30-day test of UCC 4-406, [company's] failure to sufficiently investigate [employee's] background which would have dis-closed a prior conviction of embezzlement in Michigan for the same nature of activities as alleged in the instant case, together with its failure to review its monthly statements in accordance with the Contract and in accordance with the UCC, constitutes sufficient negligence by [company] to preclude any recovery for a claim against [bank] for such alleged forgeries under UCC 3-406 and Section 2.24.02 of the Contract."

"As stated above, although [bank] can genuinely sympathize with [your] loss, based on the foregoing, [bank] must respectfully decline any claim for reimbursement by [you] arising from the facts as set forth above. **Please also be advised that, taking into consideration each forgery claim against [us] must be analyzed based on its own facts and circumstances, claims similar to this one by [customer] are normally declined by [bank] on the same basis as described herein**." (emphasis added)

The above presents a discerning application of the law to facts which face most businesses – the exposure of forged checks. This can relate to employee forgeries, as in the above cited case, or can relate to forgeries by non-employees, such as your customers or others.

These exposures can be addressed through the design of an appropriate crime insurance program, including employee dishonesty, depositor's forgery and computer fraud coverages.

As a result of the Uniform Commercial Code and the contracts that virtually every company has with its financial institution(s), the analysis of the adequacy of your commercial crime coverages is critical.

Occupational Fraud and Abuse Risk Management

Aside from negotiating appropriate crime insurance coverages, there are other things organizations should consider in their overall risk management plan to avoid crime losses.

In the Report to the Nation, the Association of Certified Fraud Examiners makes a number of suggestions:

1. Consult a certified fraud examiner. These certified fraud examiners have special knowledge concerning fraud detection and deterrents. Regular audits are not designed specifically for fraud and abuse. A fraud examiner can assess your organization's unique fraud risks and design programs to cost effectively reduce exposures and to help resolve suspected fraud and abuse matters.

2. Set the tone at the top. Employees who view their leaders as honest people are more inclined to emulate that behavior. The opposite is also true. Do not give employees an excuse to be dishonest.

3. Have a written code of ethics. A written code of ethics sets forth what the organization expects from its employees.

4. Check employee references. Some occupational offenders chronically abuse their position and are simply discharged. These persons usually go on to other organizations where they continue their patterns of fraud and abuse. They often purposefully select organizations where they know prescreening is nonexistent.

5. Examine the bank statements. The organization's unopened bank statement should be reviewed at the highest possible level. Since most occupational fraud involved skimming cash and false disbursements, a responsible person unconnected to the bank reconciliations should look for unusual patterns, dual endorsements, unfamiliar vendors and unfamiliar financial trends.

6. Utilize a hotline. In this study a majority of occupational fraud and abuse cases were discovered through tips and complaints by fellow employees. Employees are often in a position to observe improper conduct but frequently have no way to report it without fear of retribution. Some companies use a subscriber service while others maintain an internal hotline.

7. Create a positive work environment. Employees frequently commit occupational fraud and abuse as a way of "getting back" at the organization for perceived workplace injustices. By creating a positive and open work environment, the employing organization can often reduce the motivation for its employees to commit fraud and abuse.

For a complete copy of the Report to the Nation by the Association of Certified Fraud Examiners, you can call 800-245-3321 or 512-478-9070 or you can download this from the Internet at www.cfe.net.com.