

IN THIS ISSUE:

- ≡ Employee Dishonesty Claims: A New Twist
- ≡ Prevent Security Breaches by Former Employees with Thorough Exit Procedures
- ≡ Meet new Senior Underwriter, Tim Bennett

Employee Dishonesty Claims: A New Twist

Employee dishonesty losses involving the creation of fictitious loans and subsequent embezzlement of funds are fairly common. In a typical claim, a dishonest loan officer creates a bogus loan and either funds it themselves or dupes an unsuspecting fellow employee into disbursing funds. The loan officer then steals the money for personal use. **In a recent claim, however, a different twist emerged.**

A dishonest loan officer took unauthorized draws on legitimate lines of credit and gave the funds to other bank customers in what can best be described as a “Robin Hood” scenario. The recipients of the funds would not have qualified for real loans for a variety of reasons, but the loan officer believed they were good people who deserved the money.

The customers who received the funds were unaware of the fraud. In fact, the loan officer created phony loan documents and commitment letters to help hide the scam. The bank was completely unaware of the situation as well; none of these “loans” were underwritten or approved.

In order to facilitate the scheme, the loan officer instructed a teller to initiate a draw on a line of credit and create a cashier’s check payable to the bank. Then, the loan officer approached a different teller with instructions to deposit the check into a particular account. **Typically, the affected lines of credit had long periods of inactivity prior to the unauthorized draw.**

As is often the case, the loan officer was well-respected and had an extremely loyal customer base. Accordingly, when customers identified errors on their line of credit statements, they contacted the dishonest loan officer directly, who blamed the errors on systems problems. To rectify the situation, unauthorized draws were taken from other customers’ lines of credit and applied to the accounts of the customers who complained.

Because of the cover-up activity, the scheme involved many accounts and hundreds of transactions.

The bank became suspicious when the loan officer stopped repeatedly into the bank during vacation to handle transactions. The scheme unraveled when customers with incorrect statements began contacting bank management.

Article continued on next page ⇨

Prevent Security Breaches by Former Employees with Thorough Exit Procedures

When an employee is terminated or leaves, the employer needs to ensure that all access points for that employee are cut off.

Recently, an executive level employee was terminated. The bank was diligent in blocking access to the usual and apparent bank systems such as its email system and customer database. **However, the bank overlooked another access point.**

Article continued on next page ⇨

SIDE NOTES

Fraud prevention is one of the most important and complex issues that banks face.

Because of this, the ABA, through its subsidiary Corporation for American Banking (CAB), endorses the best-in-class Anti-Fraud solution, **Guardian Officer®** from GlobalVision Systems to effectively combat the various types of fraud that have evolved through technological advancements.

Guardian Officer® offers an advanced and comprehensive suite of fraud prevention modules, automating the process of monitoring, detecting and reporting fraudulent activities among all transactions of all product lines for financial institutions of all sizes. It is designed to prevent and reduce the incidence of Check Fraud, Check Kiting, Deposit Fraud, ATM Fraud, ACH Fraud, Wire-Fraud, Debit and Credit Card Fraud, among other fraud activities.

For a due diligence report from the ABA, contact Kimberly Smith, CAB Director, at 202-663-7516 or ksmith@aba.com.

For more information or to request a demo, contact GlobalVision at sales@gv-systems.com.

The program’s reinsurer, American Bankers Mutual Insurance, Ltd. is distributing their 2010 Annual Report to shareholders this month. Contact Monica Condon at 800-BANKERS or mcondon@aba.com with questions.

■ Employee Dishonesty Claims: a New Twist, *continued*

When confronted, the loan officer claimed only to have altruistic motives—unauthorized advances were provided to people who deserved a break. These transactions ranged from several thousand dollars to over \$200,000.

After the scam came to light, some of the bogus loans were converted to legitimate commitments. Unfortunately, full recovery was not possible in many cases because customers had no way to repay money that had already been spent. **The total amount of unrecoverable funds was over \$500,000.**

Steps to Mitigate Employee Dishonesty Losses

- ≡ Require that all loan proceeds are prepared and disbursed by someone other than the approving officer.
- ≡ Loan officers should not be given cashier's checks as proceeds from one of their loans.
- ≡ All dormant accounts, including inactive lines of credit, should be flagged, segregated and maintained under dual control.
- ≡ In addition to requiring annual vacations of at least one consecutive week, always prohibit access to work stations and suspend computer privileges for the duration of the individual's vacation.
- ≡ Issue account and loan statements on a quarterly basis.
- ≡ Encourage employees to report any unusual activity or "gut feelings" to their manager, even if the concern involves a higher level employee.

■ Prevent Security Breaches by Former Employees with Thorough Exit Procedures, *continued*

The former employee had dial-in access codes for teleconferences and board meetings and was calling in, silently listening to the bank conduct business. Using her access codes, she was able to learn confidential information about the bank and its customers.

To minimize your bank's vulnerability from potential information security issues by former employees or contractors, your bank should have appropriate exit processes to ensure that all access points are terminated:

- ≡ **All physical items should be collected**, such as entry badges, keys, and company issued cell phones and laptops.
- ≡ **Access should immediately be blocked** to all systems including email accounts, phone/voicemail, telephone and Web-based conferencing, and databases containing customer information.
- ≡ **Banks should create a "termination checklist" to follow each and every time an employee or contractor leaves** to provide an easy reminder of all needed steps to be taken and to ensure nothing is overlooked.

For more loss control tips or resources, visit <http://abais.com/loss-control-resources-overview.aspx>

Meet our new Senior Underwriter, Tim Bennett, CIC



We are pleased to announce that Tim Bennett has joined ABA Insurance Services as a Senior Underwriter. Tim comes to us from Banclinsure, where he was a Territory Sales Manager for 9 years. Previously, he was a Senior Underwriter in the Middle Market D&O and Crime Division of Chartis Insurance (formerly AIG Companies) for 5 years.

A native Ohioan, Tim graduated from Case Western Reserve University with a BS in Business Management.

Tim's account management skills, broad product knowledge and experience underwriting a variety of commercial product lines including D&O, bond, professional liability and P&C, are highly valued as he is assisting in the development of our bank P&C program. Once underway, he will be responsible for underwriting our P&C line of products.

To reach Tim, call 800-274-5222 or email him at tbennett@abais.com.

For more loss control information or to view this SafeTalk newsletter online, visit abais.com. To subscribe to SafeTalk®, request reprints, or should you have additional questions about this newsletter or its articles, please contact us at marketing@abais.com or 1-800-274-5222.

ABA Insurance Services Inc. dba Cabins Insurance Services in CA, ABA Insurance Services of Kentucky Inc. in KY, and ABA Insurance Agency Inc. in MI.