

Who's ripping off your bank? (April 22, 2009)

Conditions favor employee theft, but banks can fight it

A host of possible steps begins with setting a sterling example for employees to follow

By Mary Sherwood, senior risk engineering consultant, Zurich Services Corp.

April 22, 2009

It is a staggering estimate that almost 95% of all businesses experience employee theft, fraud, or embezzlement. U.S. businesses lose over \$650 billion in revenues annually to occupational fraud and abuse, according to a 2008 annual report issued by the Association of Certified Fraud Examiners. That accounts for 6% of total of gross income.

Financial institutions are especially vulnerable to employee theft because of the large amounts of cash on hand, high-speed internet transactions that are difficult to track, and high employee turnover.

No matter the size of the bank, preventing employee theft is a priority for all. But before you can establish a viable prevention program, it helps to understand the underlying causes of this behavior.

Why employees steal

Research shows that an employee caught stealing is often experiencing some desperate personal crisis. Among these issues: gambling debts that got out of hand; an escalating addiction; or family financial turmoil. The current economic slowdown may result in an increase of such activity.

Surprisingly, however, many cases of employee theft are simply crimes of opportunity. Employees cite lax controls and perceived management indifference as major reasons behind the decision to cheat an employer.

Furthermore, they watch the bosses for cues. They notice when managers take extra time for lunch; pad expense accounts; and abuse perks like car services. They rationalize their thefts with an "everybody does it" attitude and they often assume the company will write off any losses or charge them to its insurance company.

Other common reasons for employee theft are anger and bitterness toward a boss or the employer in general: "They don't pay me enough" or "I didn't get a raise." Employees who do not feel as though they have a stake in their company are more likely to steal than those who feel fairly treated.

Current business and economic trends exacerbate the problem. Companies that outsource departments may find that loyalty diminishes, leading to more casual attitudes about stealing. Corporate downsizing often results in layoffs, causing feelings of anger and frustration—both by those let go and those left behind. When such bitterness festers, it can lead to employees taking what they feel is owed to them.

Management misconceptions

If so many employees steal, why aren't managers more aware of the problem and why can't they stop it?

One reason is denial. Managers simply cannot believe that someone they may have worked side by side with, or hired and trusted, is capable of dishonesty. So they overlook obvious signs and don't bother with simple precautions that might deter most employees from criminal activity.

Managers might also hold inaccurate assumptions. They may think that everyone knows where management stands on employee dishonesty, so they never bother to put the company policy in writing. They may assume that well-compensated employees will not steal. They may assume that honest employees will report others they suspect of stealing. They may focus prevention efforts on newer employees while imagining senior employees to be trustworthy.

And so they spend their efforts counteracting theft by outsiders, rather than insiders. Or they may consider employee theft a "big company" problem, while, in fact, smaller businesses often suffer more than larger companies.

Prevention: Building the foundation

Strict oversight procedures are the key to addressing the employee theft problem. Any bank that is serious about cutting down on employee-related losses should first take a few general steps:

- Start at the top. Determine the role of the bank's board of directors in the anti-fraud program. It is highly recommended that the board "own" this process.

- Conduct a survey of your business. Catalogue existing dishonest actions and identify areas of weakness where future dishonest activities could occur. Then develop an immediate plan to reduce your exposure to those risks. Follow up with regular reviews.

- Create a written policy on employee theft. Make sure that all employees—existing and new hires—receive it. Discuss it at a staff meeting or in a memo. Enforce the policy consistently among all levels of staff.

- Set goals and standards. Ethical standards should be set high. A published code of conduct should be made available to all employees. They should be expected to conform to those standards. Inform supervisors and employees about the impact of employee theft and stress that they are key to solving the problem.

- Run background checks on new hires. Checking up on a resume and calling references is not a sign of distrust—it is an act of prudence. The time and cost are worth the reassurance that you know who you are getting.

- Establish an internal audit committee to perform ongoing audits and investigate suspected fraud.

- Insure the confidentiality of all investigations into suspected employee dishonesty and assure proper retention of company records, including computer data and email.

- Have a plan in place for public disclosure of the investigations to the media, legal counsel, and oversight bodies.

Prevention: Establishing controls

Once the overall policies are in place, financial institutions should adhere to strict internal controls, including the following:

- Segregate incompatible duties. Assign duties such as entries, transaction processing, and balance reconciliation to different people. Storage of negotiable instruments should not be maintained by the same employee who keeps the records.

- Impose physical restrictions. Limit direct physical access to cash, bearer bonds, collateral stocks or bonds, cosigned traveler's checks, U.S. savings bonds, and official bank checks. Restrict access to un-issued checks and check-signing machines. Remember to lock file cabinets and vaults.

- Require dual controls. Mandate countersignatures for disbursements in excess of a given amount and exercise dual control procedures over vault cash, vault supplies of traveler's checks, night depository mail, and ATM items, among others.

- Record transactions swiftly and accurately. Reconcile account balances to physical balances daily. Ensure that tellers are responsible for their own cash supplies and clear checks daily to ensure timely deposit.

- Safeguard hardware and software. Bank documents or customer records kept on disks could be just as valuable as cash to an employee bent on illegal activity. Store disks and CDs in locked cabinets and make sure that computer users have personal passwords and that firewall systems are in place. Lock up laptop computers—never leave them lying around in offices.

Look beyond the obvious

The list of precautions does not end there. Thieves always invent new ways to steal. The key is for banks to be one step ahead. It's unfortunate that employee theft is so pervasive, but it's clear that by taking reasonable precautions and by creating an atmosphere where honesty is expected and dishonest acts are not tolerated at any level, managers can significantly reduce the extent of the problem. BJ

Zurich corporate disclaimer: "This information was compiled from sources believed to be reliable for informational purposes only, and should be regarded as a guideline which you can use to create your own policies and procedures.

You are in the best position to understand your business and your organization and to take steps to minimize risk, and we wish to assist you by providing the information and tools to assess your changing risk environment. We trust that you will customize these points to reflect your own operations. Any and all information contained herein is not intended to constitute legal advice and accordingly, you should consult with your own attorneys when developing programs and policies. We do not guarantee the accuracy of this information or any results and further assume no liability in connection with it. Zurich Services Corporation is a member company of Zurich in North America.”

[This article was posted on April 22, 2009 on the website of ABA Banking Journal, www.ababj.com, and is copyright 2009 by the American Bankers Association.]