Volume 13 Number 3

TEXAS Bankers INSURANCE AGENCY

Banking on Insurance

Winter 2012 Insurance News for the Banking Industry

Beware of the Wire

By Craig M. Collins

Know your customer. Likely everyone in banking has repeated this mantra time and time again. In today's digital age of banking, it may seem impossible to truly know the customer, but it's becoming as important as ever. Wire transfer fraud is an increasing trend in financial institutions and it looks to continue to grow in the coming years. When hundreds of thousands of dollars can be transferred with just the click of the button, knowing your customer can help banks to be on the lookout for signs that may alert the institution to a potential fraud attempt.

Today's "bank robbers" know it's far easier to rob someone with a computer or a telephone than with a gun – and it's safer, too. Electronic theft began in the early '80s as banks began implementing computer systems to track customer accounts. Criminals quickly learned that getting into a customer's electronic account is much easier to access "through the front door," using a customer's personal information. The same principle holds true today.

Wire fraud can occur through the phone, fax, email or online, and the losses average hundreds of thousands of dollars per incident. That's a lot of money moving around, often without ever hearing the person's voice. Criminals have countless methods for convincing a bank to wire large sums of money to another account, but the results tend to be similar:

- a fax to a bank with customer's information that the customer did not send
- a memo from a call with the "customer" which the customer never made
- an email from the customer's account that the customer didn't write
- a confirmation phone call to the number listed in the account, only to later find the number has been temporarily diverted by the criminal, meaning verbal confirmation comes from the thief, not the customer

The victims can be individuals, but businesses are more likely to fall prey to these schemes since they tend to carry heftier account balances than individuals. Small businesses are targeted the most frequently. They generally lack the complex security measures of larger organizations and criminals find it much easier to access sensitive information.

The majority of fraudulent foreign wire transfers wind up in Asia, Eastern Europe or Africa. These international transfers are the most dangerous because there is no government protection and no way to reverse the process. Domestic fraud isn't uncommon either. In the United States, wire transfers have some safeguards in place to manage fraud, but it should be assumed that once a transfer is made, there is no way to bring the money back. The responsibility for the stolen money could fall on the account holder and/or the bank depending on the circumstances.

Help safeguard against fraud

There are endless ways criminals will find to transfer someone else's money into their

continued on page 3

Distracted Driving

I had to do a double take this morning as I drove into downtown Austin. I glanced over to witness a fellow commuter driving while filling in her crossword puzzle. She was quite talented with her placement of the newspaper over her horn and one pinky finger guiding the steering wheel. My first reaction was to get away from that car. But this is not all I see on my morning commutes. The eyelash curler, the makeup artist or the cell phone addict are frequent companions on my drive. All items are distracting and dangerous, but the one item I see as a major safety issue is the cell phone.

With more cell phones than people in the U.S. today, distracted driving is a growing problem. How many times have you sent "just a quick text" from behind the wheel of your car or answered that important phone call you'd been waitinf for? While statistics are showing the majority of Americans disapprove of these behaviors, these same survey respondents admit to regularly committing the same unsafe actions themselves. The National Highway Traffic Safety Administration (NHTSA) reports that 18 percent of injury accidents in 2010 were reported as distraction-affected crashes, and nearly 1 in 5 distraction-related fatalities was related to cell phone use.

The statistics are sobering for anyone, but businesses have particular reason for concern. If an employee on the road is involved in an accident while using a cell phone, the employer may be held liable for injuries or damage. The liability could even potentially extend to employees i their personal vehicles if the cell phone is compnay-issued or being used for work-related calls or emails. To help address these issues, banks should consider implementing a zero-use cell phone policy for all employees.

Cell Phones & Driving Don't Mix

Distracted drivers are everywhere. On distraction.gov, the U.S. Government warns "Distraction occurs any time you take your eyes off the road, your hands off the wheel or your mind off your primary task: driving safely." Cell phones are particularly dangerous while driving because they combine all three of these distractions — physical, visual and mental — into one potentially deadly action. Using a cell phone while driving, no matter if it's handheld or hands free, creates a reaction delay equivalent to those with a blood alcohol level at the legal limit of .08 percent. The simple fact is drivers who use cell phones are four times more likely to have a serious crash. Most banks would not allow an activity that quadrupled the risk of an armed robbery, would they?

The Productivity Fallacy

Businesses are often afraid of limiting cell phone use in the car because they fear losing employee productivity. But, evidence shows limiting cell phone use increases productivity.

Thanks to what's known as inattentional blindness, it's common to miss something in plain sight when your attention is focused elsewhere. Research by Carnegie Mellon has shown that driving while using a cell phone reduces by 37 percent the amount of brain activity associated with driving. This inattention goes both ways — drivers could just as easily miss important details of a call with a client as miss details on the road. Keeping calls in the office means employees are focused on that customer.

Protection on the Road

While cell phone driving laws vary by state, your bank can take charge of your own employee cell phone use by creating a written, enforced, zero-tolerance policy for cell phone use while driving. Think about the following as you create the policy.

1. Back up your argument.
Share the statistics and research with your employees. It's important for them to understand why you don't want them multitasking behind the wheel.

2. Support from the top down.
Consider creating a statement of support explaining the importance of the cell phone policy. Let employees know they won't be expected to answer their phone while driving, even if they're using a hands free device.

3. Be explicit.
State the rules clearly. Make sure employees know they're not allowed to text, check emails or listen to conference calls while driving.

4. Offer tips on how to comply.
A little bit of guidance goes a long way. Think about the following tips to help achieve compliance:

- Encourage employees to turn phones off while driving, or leave them in the back seat to avoid temptation.
- Have employees explain in their voicemail that they don't answer calls while driving.
- Suggest that employees plan the day around when they will be unable to receive calls or return emails, which will allow them to alert others to their unavailability.
- Remind employees that nothing is som important that it can't wait for them to pull over or park.

Distracted driving is preventable. Protect your bank, its employees and everyone else on the road by considering a zero-tolerance cell phone policy and help keep one more distraction out of the drivers seat. ■

Beware of the Wire

cotinued from page 1

own bank accounts, but there are a few red flags that should help alert the teller executing the transfer hat something may be amiss. Some situations to keep an eye out for are abnormally large transfers, transfers from an account that has never wired money in the past and any transfer to Europe, Africa or Asia. Another warning sign is someone who has excuses as to why he or she can't speak with you over the phone. Banks can help protect themselves and their customers by paying attention to these and other red flags and by putting safeguards in place to help spot potential wire transfer thefts before they happen.

Consider executing account usage agreements.

Usage agreements can detail things like who is authorized to execute a transaction, which accounts are eligible for transfers, what security measures and verification steps are in place, which communications methods are used and who is liable for what if fraud were to occur. These agreements can be especially useful for businesses, but should be considered for individuals as well. Another step to consider could be to require individual, international or first-time transfers to happen in person, or implement digital security tokens that generate a new unique user password every few minutes. Phone passwords can also help distinguish the true account holder from a criminal.

Think about creating transfer procedures.

Many times fraud occurs because the protection process broke down somewhere along the way. As a result, banks should consider having a formal process for transferring funds and training employees to follow all steps in the process. For example, if the process requires a teller to call the number listed in the account after a transfer is initiated, then a teller should place the phone call. Often criminals will call immediately after faxing a transfer request to "make sure the fax went through." Speaking to the person executing the transfer should not replace calling the number listed in the account.

Know your customer.

As mentioned before, knowing the customer is as important as ever. Does this customer normally transfer money? How big are the transfers? Where does the money usually end up, somewhere local or an international account? In what ways do they typically initiate a transaction and who is the originator? Is the origination account the one that is normally used for transfers? If speaking to someone on the phone, do they sound to be the same gender as the name on the account? Knowing the answers to these questions could help alert bank employees to potential fraud in progress.

Consider training employees who are conducting transactions

Bank employees should trust their instincts when something seems amiss in a transfer request. Consider teaching these employees the warning signs that could help alert them to potential fraud — even if it might be to the temporary annoyance of the customer. While keeping customers satisfied and ensuring quick transactions are important, secure banking is the paramount concern. Ultimately, customers will appreciate your efforts toward the security of their money more than they will a quick, easy transfer. Encourage employees to trust their gut and follow the security procedures, which may include review with the bank's security officer.

Encourage customers and employees to try to protect sensitive data

It's incredibly important to protect sensitive data such as social security numbers, account numbers and passwords. In today's society, it's unnerving how easy it is to build a complete personal profile of someone using social networks and internet searches. Consider keeping digital information safe by using protected wireless networks, security software and creating strong passwords with letters, numbers and symbols. If a hacker gets into a company email system, he'll have access to email records that may have past transfer information which gives him a "template" for how to conduct the fraudulent transfer. According to a recent alert from the FBI, hackers are even initiating transactions using variations of legitimate email addresses — such as changing a letter "O" to a zero. Consider establishing protocols for safe email practices that include avoiding sending account information via email.

Wire transfer fraud is a relatively safe and easy way for a criminal to acquire a lot of money in a hurry, and it will likely continue to be the preferred method of theft in banks, at least until the next scheme comes along. It's impossible to prevent every fraud from occurring, especially as the schemes become more advanced and complex. Taking the proper precautions and educating staff is an important step that could help protect the bank and its customers. ■

Craig M. Collins is the president of Financial Services for OneBeacon Professional Insurance. He can be reached at ccollins@ onebeaconpro.com.

Holiday Party 101

Holiday parties are a great chance for employees to come together, reflect on accomplishments and bond as a team. The primary goal of any party is for everyone to enjoy themselves and get home safely, but it takes careful planning to create an environment that ensures safety as well as a good time.

Concerns such as liquor consumption, premises safety and security, discrimination and food borne illness are a few of the many issues that need to be addressed to help prevent overindulgence, injuries or even harassment. Not only could the pleasant atmosphere be ruined in a hurry, your bank could find itself liable.

Due to their infrequent nature, the liability risks of company-sponsored holiday events are often overlooked. To ensure the health and well-being of all who attend, it's important to be aware of any potential liability concerns that your company may face if the event doesn't go exactly as planned.

Particpant's Safety

As with any event, the safety of everyone attending should always be a top concern. At a company-sponsored party, it's important to also note that any accidents or injuries may be considered work-related and could be subject to workers compensation. The following tips may help avoid safety mishaps.

- If using a venue an offsite venue, inspect it to ensure it meets your standards for safety.
- Consider the effects that weather may have on safe travel to and from the party. Special considerations may have to be made to keep sidewalks and parking lots clear if the event is outside of normal business hours.
- Keep an eye on party-goers to ensure that no one wanders off or goes to his or her car alone after dark.
- Review situations for employees with disabilities who may require special attention.

Harassment and discrimination

No matter where your party is held, it may be considered an extension of the workplace. Policies that guide behavior in the workplace should apply to the party as well, including violence, harassment, discrimination and the general code of conduct. Prior to the event, let employees know the standards to which they will be held.

- Ensure everyone knows the event is optional and is not required for continued employment, advancement or any other benefit. All invitations and should emphasize this point.
- Make sure that the party is not tied to any specific religious tradition and is referred to as a "holiday party."
- Management should help monitor employees' behavior to ensure that it conforms to company policies. Prompt action should be taken when activities stray beyond acceptable bounds.
- Limiting alcohol consumption will help avoid impaired decision-making and lowered inhibitions, which can lead to poor behaviors.
- Avoid activities or items that could lead to physical contact, unwanted social pressure or inappropriate conversation.
- Any complaints made as a result of a holiday party should be taken seriously. Document, investigate and treat the complaint like a workplace incident.

Alcohol service

One of the most important issues that should be addressed at a holiday party is whether alcohol is going to be served, and if so, which controls will be instituted. Some companies have recognized the liability exposure that alcohol represents and have chosen to hold holiday events free of beer, wine or liquor. If it will be served, there are important considerations that can help to limit potential problems.

- Hold the event at an off-site location and hire professional bartenders who have their own insurance and are certified for alcohol-service. Speak with the vendor to determine what protocols for keeping minors from being served and preventing people from being served while intoxicated.
- Make sure there are plenty of non-alcoholic beverage options available.
- Instead of an open bar, consider passing out drink tickets to control the amount of consumption.
- Stop serving alcohol well before the end of the event to help prevent drinking and driving.
- Ensure that plenty of food is available. Starchy snacks will help slow the absorption of alcohol into the bloodstream, while salty foods should be avoided as they encourage more drinking.
- Someone should have the training and authority to "cut off" anyone who is intoxicated.
- Provide alternative transportation that may include free cab rides.
- Develop guidelines ahead of time for the management group and meet with them so they understand their responsibility to be role models.

Insurance

It's also important to use vendors that carry their own insurance coverage. All catering firms, bartending firms, facilities or entertainers should be required to produce Certificates of Insurance (COI) with sufficient coverage and limits of liability.

When reviewing rental contracts, note any hold harmless or indemnity agreements that could release the vendor from liability and instead hold your company responsible for losses from situations outside of your control.

Holiday parties are a time for celebration and appreciation, and everyone wants them to be memorable – but for the right reasons. Making smart decisions to ensure a safe party environment can help ensure a healthy happy holiday season. ■