Volume 14 Number 1

TEXAS Bankers INSURANCE AGENCY

Banking on Insurance

Summer 2013 Insurance News for the Banking Industry

Corporate account takeovers

By Craig M. Collins

In our digital society, banking is more accessible than it's ever been. Bank customers can automate monthly bill pay, deposit checks with cell phone cameras, transfer funds through text messages and tweet about the entire process directly from a bank app. Banks can serve millions of customers without a single branch office. Banking has become so easy, customers don't even have to think about it. Unfortunately, criminals are thinking about it. With more money increasingly changing hands through the internet, theft through these digital channels is on the rise.

One of the more frequent scams today is known as Corporate Account Takeover. According to the Texas Bankers Electronic Crimes Task Force[1], Corporate Account Takeover happens when thieves manage to gain access to a business' banking information through "legitimate" channels by stealing user credentials and passwords. The thieves then initiate transfers to other accounts, often held by money mules, who then withdraw the funds or transfer them on to other criminals.

Small to medium size businesses are particularly at risk because they carry much larger account balances than individuals and generally have lower-level security in place than large corporations. Compromising the users' banking credentials is far easier than trying to hack directly into a bank's secure system. Some of the more popular methods the FBI has seen employed by thieves include:

- Sending infected emails containing a Trojan horse virus called Zeus that records keystrokes for passwords and account information
- Planting pop-up advertisements on legitimate websites that install viruses once the user clicks
- Redirecting a user away from a banking website and asking them to verify key account information which criminals can then use to take over the account

Corporate Account Takeover can happen in all types of business accounts, including churches, hospitals and government entities. Banking customers often assume their bank will reimburse them for any funds missing from their account, but, for instance, if the account was accessed using the customer's verified legitimate credentials, is the bank responsible for these missing funds? Depending on the circumstances, liability for these types of thefts can be heavily litigated.

The Internet Crime Complaint Center (IC3) published a Fraud Advisory on Corporate Account Takeover[2]. The IC3's

Advisory suggests banks take a three-part approach to trying to prevent this type of fraud: Protect, Detect and Respond.

1. Protect

IC3 encourages banks to "implement processes and controls to protect the financial institution and corporate customers." These controls can include elements such as verifying bank protocols for transfers, educating bank employees on the threat of fraudulent transfers and encouraging them to follow bank procedures to the letter. For example, if a customer call-back is a part of the confirmation process for a transfer, it may be advisable to call the customer as opposed to answering a call from the supposed customer. Many criminals will immediately call the bank to verify the transfer in order to prevent the bank from making the call to the true account owner. Additionally, bank employees should not conduct bank business from their personal computer at home, or send bank information through personal email accounts.

Banks may also want to consider providing tips to the cus-

continued on page 3

Are you ready for healthcare reform?

By John Burkholder

For the past three years, employers have been barraged with predictions of what health insurance will look like after the Patient Protection and Affordable Care Act, now popularly called the Affordable Care Act or ACA, is implemented in its entirety.

With the Jan. 1, 2014 implementation date a mere 20 weeks away, those rules and regulations continue to be released weekly, and delays and postponements are becoming more and more commonplace.

Even with a number of key issues still unresolved, the sky is not falling. In spite of all of the alarmists' scare tactics, the vast number of financial institutions already have in place, or are within a tweak or two of having, the coverages in place that satisfy the "minimum essential coverage" requirement as defined later in this article.

Understanding the ACA

All carriers are currently revising their offerings that do not satisfy that requirement and will be ready to amend your plan, if necessary, to comply with the new law. Any such changes do not need to be made until your first plan anniversary date on or after Jan. 1, 2014.

Most of the changes required by the law that are actually new to you are such things as employee notices that should be furnished to you by your broker or insurance carrier, payroll-based changes such as the Additional Medicare Tax that should be withheld from high wage earners or reporting the value of your health plan for employers that file 250 or more federal W-2 forms.

To understand the ACA, you must first realize that the law's primary focus is to require all Americans to secure minimum essential health insurance. It is an individual responsibility law. Individuals who do not have access to affordable care through their employer's group insurance plan or under a government-sponsored plan must arrange to purchase individual health insurance on their own.

Employer-based group health insurance is a key source for millions of individuals to secure health insurance and thereby satisfy their legislatively mandated requirement to do so. Therefore, even though the ACA is primarily about "individual" coverage, there are some spillover requirements for employers.

Play or pay provision

One of the key "spillover" features of the law is a requirement that all "large" employers (50 full-time or FTE employees for more than 120 days during the previous calendar year) must provide to their full-time employees the minimum essential health benefits that are affordable.

This is the so-called "play or pay" provision that will assess taxes to large employers that do not provide affordable minimum essential coverage to their employees. However, the Obama administration recently announced that it will delay implementation of this mandate under the Affordable Care Act until Jan. 1, 2015.

Going forward

Many requirements have already been implemented over the past 24 months, such as providing a uniform summary of benefits and coverage to all applicants and enrollees, limiting the amount of contributions to a flexible spending account for medical expenses to $2,500 per year, including the value of group health plan benefits on W-2 forms provided to employees of employers issuing 250 or more W-2 forms, and adding or keeping children covered until they turn 26 years old.

Going forward, while the large employer mandate is suspended, a variety of key provisions remain in play. Subject to any future adjustments, large employer plans are still obligated to comply with a number of specific changes. Waiting periods for new employees cannot exceed 90 calendar days. Plans with waiting periods for new employees, such as the "first of the month following" 90 days, will have to amend their plans to be in compliance.

Lifetime and annual limits will no longer apply to Essential Health Benefits. While pre-existing conditions for children have already been eliminated, on the first plan anniversary date after Jan. 1, 2014, there will be no pre-existing condition exclusions for enrollees of any age.

Health Insurance Exchange

By Oct. 1, all employers are supposed to notify their employees about the availability of a new Health Insurance Exchange (an online marketplace where individual employees without coverage can purchase health insurance) and how employees can access information on premium subsidies that might be available when purchasing individual coverage through the Exchange.

The notice to employees was originally supposed to take place March 1, 2013, but the Fed had to delay the notice until Oct. 1, as there was no Exchange information to give to the employees on March 1. In Texas, the Exchange will be a Federal government-run exchange. It is supposed to be available effective Jan. 1, 2014, with enrollment available beginning Oct. 1, 2013. However, the federal government is still struggling to meet that deadline.

Taxes and fees

Also new for 2014 are taxes and fees to be paid by insurance companies, medical device manufacturers and pharmaceutical manufacturers. A Health Insurer Tax Fee, a Reinsurance Fee, a Comparative Effectiveness Research Fee (PCORI) and Exchange User Fee will be levied on insurance companies that will, in turn, have to pass on those fees and taxes to employers in the form of rate increases.

For small employers (fewer than 50 employees) who maintain health insurance plans for their employees, the "Essential Health Benefits" must be included on the first day of the plan year on or after Jan. 1, 2014. In addition, annual cost-sharing exposure limits for employees under small employer health plans will be limited to an indexed cap adjusted annually by the Fed.

Currently, those limits are $6,250 per year for individuals and $12,500 per year for families. All insurance companies are filing new plan designs with the state to make sure the coverages they provided comply with the new ACA requirements. ■

For more infomation on healthcare reform, please login to www.ytexasbankers.com/magazine to read the full article in the August 2013 issue of Texas Banking magazine.

When I grow old ...

The population in America is changing. As Americans age and medical advancements give rise to longer lives, the need for long-term-care is increasing. It is estimated there are 44.4 million American caregivers age 18 and older who provide unpaid care.

In fact, the annual cost to companies for workers' lost productivity due to elder care issues is estimated at $2,100 yearly per employee, to the tune of $33.6 billion each year.

Although Medicare provides valuable benefits, it does not cover these costs. Long-term care insurance helps bridge the gap by covering the costs of nursing homes, assisted living centers and in-home care.

Chances are you or some of your employees are facing a long-term care issue with a spouse or parent right now. A 2004 study revealed that more than 44 million Americans provide care for an adult family member or friend age 18 or older. Sixty percent of employed caregivers report that they had to make work-related adjustments as a result of their care giving responsibilities.

While most banks offer the traditional choice of health and life insurance along with retirement planning, more and more banks are adding a new benefit: long-term care insurance. It is a timely benefit that meets the growing concerns of employees who are responsible for their aging parents and worried about the consequences of their own longevity.

Why should we as individuals and employers think about buying long-term care? Without long-term care an unplanned accident, illness or disability could wipe out a lifetime of savings. Private nursing care runs about $85,000 a year. Without long-term care, you or a loved one will be footing the bill. Medicare is not picking up these costs, and you and I will be required to spend our savings when monies are depleted or be left with a Medicaid nursing facility.

Here are a few examples of average everyday folks in need of long-term care. The stories are true:

- A 45-year-old man with a bright future has an auto accident and due to a brain injury needs 24-hour care.
- A 39-year-old mother of three has an outpatient medical procedure; something goes wrong during the procedure and she now requires 24/7 care.
- A 94-year-old widow develops Alzheimer's and needs 24/7 care.

Are you interested in long-term care for yourself or as a benefit for your bank employees? Contact us for more information about this important coverage. 800-318-4142 or insurance@texasbankers.com. ■

Corporate account takeovers

cotinued from page 1

tomers themselves, or establish requirements for certain customers. For instance, it's not unusual for a bank to require corporate customers to carry their own crime insurance to have protection in place in the event of certain types of losses. Banks might also consider requiring a certificate of insurance from business customers that demonstrates the proper insurance is in place, much like what is already required for closing on a loan.

Email accounts for small businesses are notoriously easy to break into, giving criminals access to all the details and procedures normally used with email transfers. As a result, banks may consider recommending to customers that they designate an individual computer that is used only for account transfers. The use of a dedicated machine may help prevent unauthorized users from engaging in transfers, and also potentially help the business provide a secure environment for these transfers by avoiding the malware that can be acquired through email and web browsing. It may seem like an unnecessary expense to designate a computer for this one purpose, but the cost of one machine is far more affordable than the potential cost of a breach or theft.

Cash Management Systems are also susceptible, and with an administrator's credentials, thieves can gain access to individual accounts and Personally Identifiable Information (PII) across the entire system. For example, one method being employed by cyber criminals is to use the system to add unauthorized ACH payroll accounts. Unauthorized payroll payments can sometimes go unnoticed, so banks might consider recommending to business customers potential caps to the amounts distributed through the payroll. Banks might also consider encouraging business customers to evaluate their overall security procedures and protection options.

2. Detect

There are tools available to banks today to potentially detect thefts in progress. Many of these systems use scoring techniques to attempt to grade the likelihood of a transaction as legitimate or as a potential fraudulent transfer.

Banks shouldn't underestimate the ability of employees to potentially identify in-progress theft as well. For example, if an employee notices that a small company that deals locally is suddenly sending a large transfer to an overseas location, and then seeks to verify the legitimacy of the transaction, he or she might be preventing a possible theft.

3. Respond

Fraudulent transfers should be responded to in a matter of minutes, not hours, warns IC3. The sooner banks respond, the greater the chance of recovering a customer's money. The IC3 website offers suggestions for reacting to a fraudulent transfer, which include verifying that the transaction is in fact fraudulent, attempting to reverse the transaction and reporting the theft to the proper authorities.

While some attempted fraudulent transfers can be stopped or reversed, losses due to Corporate Account Takeover are in the hundreds of millions of dollars each year. Banks can't prevent all fraud attempts, but diligence is invaluable. As with many forms of fraud, the criminals will evolve with the prevention techniques. Work to keep your employees educated and alert.

References

1. Texas Bankers Electronic Crimes Taskforce, "What is Corporate Account Takeover?" http://www.ectf.dob.texas.gov/aboutcato.htm
2. Internet Crime Complaint Center, "Fraud Advisory for Businesses: Corporate Account Takeover" http://www.ic3.gov/media/2010/corporateaccounttakeover.pdf ■

Craig M. Collins is the president of Financial Services for OneBeacon Professional Insurance. ccollins@onebeaconpro.com.

TEXAS Bankers INSURANCE AGENCY
203 W. 10th Street
Austin, Texas 78701

We work for you!

Texas Bankers Insurance Agency is proud to say we have served the banking community for over 25 years. We have been blessed to work with great bankers and currently insure over 200 banks nationwide. We provide a wide variety of insurance products but we also educate our clients and keep them abreast of the latest insurance issues and claims trends. But our agency does much more than sell insurance.

On occasion, we hear from bankers that their insurance agent is a bank customer, a board member or a close friend. So buying insurance coverage from Texas Bankers Insurance Agency may not be an option. We do understand the value of these situations. However, we can be a resource for your bank and help preserve your local business relationships through our consulting services.

Here are a few of the fee based consulting services we can offer:

- Review all insurance policies and advise you of any restrictive policy language or missing coverage.
- Review insurance losses and offer risk control help to reduce premium hikes.
- Inspect locations for property, liability or workers compensation claim issues.
- Educate staff on the proper way to complete insurance applications, when to report changes and claims to the insurance company.
- Provide insurance checklists with helpful insurance tips that protect your bank.
- Provide RFP (request for production services). We can take on your insurance application process, assign insurance agents, review proposals and provide input. We can help implement your new insurance program into the bank.
- Speak at your board of directors meetings and answer insurance questions, discuss the hot topics in banking industry and talk about insurance claims we see in Texas and country wide.
- Hold insurance educational seminars by phone, webinar or on site.

We hope the next time your insurance coverage is up for renewal, you will consider calling our agency experts. We will help you get the proper insurance coverage at a fair price. For more information call me at 800-318-4142 or email at insurance@texasbankers.com. ■

TEXAS Bankers INSURANCE AGENCY