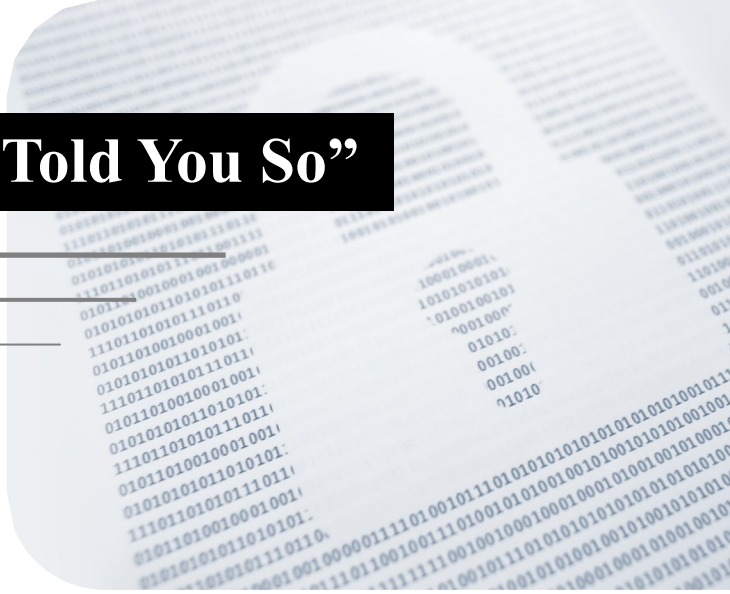
Avoiding the Cyber-Fraud "I Told You So"



What are four most hated words in the English language? Some might say it is when you hear, "***WE HAVE TO TALK***." It is usually uttered by your spouse, your child, or your boss. Nothing good ever follows that phrase. It is an early warning sign that you will not enjoy the next few minutes because bad news is about to be delivered. Others might say that the most hated four words are "***I TOLD YOU SO***." Generally, you cannot do anything about hearing the phrase "***WE HAVE TO TALK***." You can do something, however, about hearing the words "***I TOLD YOU SO***."

WE HAVE TO TALK . . . about Cyber-Fraud

In a recent television commercial campaign, we have all seen the "Settlers who settle for cable" rather than opt for the presumably technologically advanced digital satellite television entertainment. These "Settlers" are "off the grid" and hoping that they are removed from ever-increasing digital threats to our way of life. Some of these recent commercials even suggest that you cannot order a good pizza unless you are "on the grid." In today's world of "zeroes and ones," digital communication, and electronic conveniences, it would be nearly impossible to imagine representing a client in a real estate closing without communicating with them, the bank, and numerous others electronically.

Since you are holding sensitive information and communicating such information over the internet, you are a target for cyber-fraud. This is important enough to repeat. You are not an innocent bystander to cyber-fraud, **YOU ARE A TARGET**.

For the purposes of this discussion, I am going to assume that you are "on the grid" and aware of your status as a target. To that end, I am going to further assume that you have invested in the state of the art technology necessary to protect you from cyber-fraud, like email encryption, firewalls, antivirus protection, malware protection, updated software, and the many things that Information Technology (IT) professionals recommend and ALTA Best Practices require.

YOU NEED TO TALK . . . to the Following

If my assumption in the previous paragraph is incorrect, then you need to immediately make two calls:

1) To your trusted IT professional because you are attempting to exist in this digital world like one of the "Settlers" on television. Envision one of those "Settlers" starting to climb their windmill with lightning striking all around – that is you.
2) To your insurance agent because… well, once you have read this article you will understand the importance of this second call. Envision yourself driving down a crowded one-way street in the wrong direction with the other vehicles trying to hit you, and not being able to use another street. You are a target for cyber criminals and you need insurance protection. It is not a matter of "**IF**," it is a matter of "**WHEN**" you get hit by the tractor trailer that is cyber-fraud.

(Continued on page 2)

(Continued from page 1)

Even if you believe that you are on top of cyber-fraud, you still need to talk to these two individuals routinely to try to catch up. Let's face it: when was the last time you thought about cyber-fraud? If you say anything longer than ten minutes ago, then you are behind the cyber criminals because they think about it all the time.

TALK TO YOURSELF. . . Do I Even Need Cyber-Fraud Insurance?

The first key to understanding what kind of cyber-fraud insurance protection you need is to understand the exposure that you already have. For example, if you do not have a car, then you do not need automobile insurance. If you do not think that you need cyber-fraud insurance, then you should take the following test. Two simple "Yes/No" questions:

1) Do you have a computer? **2) Do you have a cell phone?**
If you answered "Yes" to either of these questions, then you need cyber-fraud insurance.

Now that **YOU** know that you need cyber-fraud insurance, the second key to understanding what kind of cyber-fraud insurance protection you need is to understand the exposure that you already have.

TALK TO ME . . . What is Cyber-Fraud and What Coverage Do You Need?

Cyber-fraud is an all-encompassing term that includes a wide variety of types of fraud. It is often confused and identified with each of its sub-classes and used interchangeably. In short, cyber-fraud is a crime or theft committed using digital access to or through a computer or computer network (including phones). **The types of liability for a cyber-fraud differ by the nature of what is being stolen**.

A. When **DATA** or **INFORMATION** is stolen, the type of liability you have and the type of insurance that you need is referred to as **CYBER LIABILITY/DATA BREACH** insurance coverage.
B. When **MONEY** is stolen, the type of liability you have and the type of insurance you need is referred to as **CRIME INSURANCE or CYBER THEFT INSURANCE** coverage.

In both instances the crime or theft is usually perpetrated through some form of digital access, and therefore lumped into the same cyber-fraud term, but the insurance coverages are substantially different.

1) LET'S TALK ABOUT STOLEN INFORMATION & CYBER LIABILITY OR DATA BREACH INSURANCE

Cyber-breach is a classic form of cyber-fraud. When a cyber-breach occurs, ***INFORMATION or DATA*** is what is stolen. We have all read about the big breaches at Sony, Target, Home Depot, JP Morgan Chase, and other high profile cyber-breaches. Traditionally, most people rationalize away the threat by saying that, "We do not have that volume of information so we are not at risk." This self-soothing rationalization provides little comfort when your number is up and you have actually suffered a cyber-breach. Remember, you are a target.

You have in your possession and need to protect your clients' non-public personal information (NPI), which first appeared on the regulatory scene in Gramm-Leach-Bliley in 1999. The concept of keeping secrets, however, is much older and the bedrock of any trusted profession. In short, we have to keep the secrets of our clients confidential and free from public or even private release. As with all endeavors, there is an ever-increasing risk that the procedures and protocols that we put into place yesterday will not survive the constant barrage of new threats today.

(Continued on page 3)

(Continued from page 2)

The cyber-breach fraud can be perpetrated many ways, including the following:

- Gaining credentials (login and password) for access to a computer network that contains NPI;
- Intercepting un-encrypted or improperly encrypted communication containing NPI;
- Improper disposal of NPI;
- Sharing NPI with a source that is believed to be trusted (but is not); and
- Many more.

The Cyber Liability or Data Breach Insurance coverage protects you in many of the following ways in the event of a data breach:

- To defend civil or regulatory actions filed against you
- To pay damages to third parties if you lose
- To provide research and information if a governmental agency looks into the data breach
- To notify clients in the event of a data breach
- To monitor clients for ID theft if they were subject to the data breach
- To determine the cause of the data breach and extent of the loss
- To restore data that was corrupted by a data breach

In inquiring about Cyber Liability Insurance for a data breach, you should inquire as to the specific coverage provided in these areas as sometimes they are not included or have a separate limitation on coverage.

The cost of data breaches is rising for companies and law firms. According to a study recently conducted by the Ponemon Institute (and paid for by IBM) the average cost of a data breach is now $154 per record lost or stolen (or believed lost or stolen). These direct costs include employing IT professionals to repair the breach, investigating the cause, setting up hotlines for clients, and offering credit monitoring for victims. This number does not include the soft and often hard to measure costs to the firm due to a damaged reputation from adverse press. A lot of people began moving their business to Lowes when Home Depot got hit.

In order to be objective, the Ponemon Institute study left out the "mega-breaches" (like Home Depot and Target) from this number because those high-profile breaches cost more than twice as much per customer than the number stated above. This study also concluded that information allowing the criminal to steal someone's identity was much more valuable to the criminal than merely an account number or credit card number. You may not have a credit card number in your file, but you have numerous clients' home loan credit applications, which is a treasure trove of NPI and a gateway to identity theft.

Do a little simple math to see whether you need insurance to protect **YOU** from a cyber-breach.

Amount Charged for a Closing
- Less (Overhead Currently Incurred)

= Net Cash Flow *(What You Thought You Made)*
- Less ($154 **Per Person Involved in the Closing**)*

= Real Net Cash Flow after a Breach
(What You Actually Made – OR LOST – Per Closing)

** If you have a closing with a husband and wife on both the buy and the sell side, that is 4 X $154 or $612 per closing of potential risk.*

(Continued on page 4)

(Continued from page 3)

It is important to note that all of the protections that we discuss concerning cyber-fraud (encrypted email, firewalls, antivirus software) protect you and your clients. This type of cyber-breach insurance protects **YOU** and **YOUR BUSINESS**.

2) LET'S TALK ABOUT STOLEN MONEY & CRIME INSURANCE OR CYBER THEFT INSURANCE

Cyber-theft is what people generally think of when they think of cyber-fraud – someone stole **MONEY** from the trust account using the internet; however, please remember that this is a separate and distinct flavor of cyber-fraud and needs to be explicitly covered by the insurance policy. In most instances, this is covered by a Crime Insurance or Cyber Theft Insurance Policy.

Cyber-theft is a crime that involves a computer and/or a computer network in order to steal or misappropriate money. This malicious crime can occur from a network breach from inside or outside your firm. Generally, it occurs when the unauthorized access to login credentials and passwords allows the cyber criminals to access bank accounts and transfer funds to themselves. Basically, they log into your online banking and transfer funds to themselves. Many banks will not reimburse a business for money lost if the transfer is made with the correct account number, login, and password. Cyber-theft Insurance covers the theft of money through the use of a computer when this information is stolen in order to steal money.

Determining coverage amounts for this type of cyber-fraud insurance is the most difficult because there are many factors to consider. These factors include:

a) What is my **Average Daily Balance** in the trust account?
b) What is the **Biggest Deal** that I handle each year?
c) **How Much Money Flows Through** the trust account in a day, month, or year?

Much like your car insurance, you will probably not find it to be cost effective to buy as much cyber-fraud insurance as you need; however, you will have to discuss these prominent issues with your insurance agent. They may want to know what type of protections you have in place (email encryption, firewalls, etc.). Much like if you have a burglar and fire alarm at your home, your insurance may be less expensive. Fortunately, this type of insurance is becoming more widely utilized and part of larger pools so the underwriting is less specific to you and more generally related to the industry.

There is one additional factor to consider and that is the State Bar. ~~If you suffer~~ When you suffer a theft of funds due to cyber-theft, you will take comfort in that the promise of insurance coverage may sway the Bar to delay in their demand that the money be restored to the trust account from your personal funds. While I cannot speak for the Bar, they have been swayed in the past to be more patient in their demand to put the clients' money back in the account.

3) LET'S TALK ABOUT GETTING TRICKED AND CRIME INSURANCE

There is another flavor of cyber-fraud that falls into the crime insurance realm. It is called Social Engineering Fraud and is possibly the most frustrating type of fraud that is prevalent in the real estate industry today. In this type of fraud, you are convinced through electronic means to send money (usually seller's proceeds) exactly where the cybercriminal wants you to send them. That is right, the criminal sends you wiring instructions on where to send them the money and you do it. Heck, you even pay the wiring fee to send it to them. Frustrating may not be strong enough, let's say infuriating. In these instances, the banks tell you that they did "exactly what you instructed them to do," and they are not liable.

(Continued on page 5)

(Continued from page 4)

Why in the world would you send money to a criminal? There is only one reason, you were tricked through FRAUD. Social Engineering Fraud is a type of fraud where they gain or use the pre-existing confidence in another person and trick you into sending funds directly to them. Here is how it works:

a) A fraudster intercepts a single or collection of unencrypted emails or mines data on the web.
b) Sufficient details of the sale are learned, including the names of the buyers and seller. Some of this information could include the copy of a settlement statement in the email.
c) The fraudster sends wiring instructions (or "revised" wiring instructions) that include a new ABA routing number and account number and requests funds for the transaction. The email would generally come from a similar (but different) sender's email address; to wit: realestatebroker@trustedfirm.com would be changed to realestatebroker.trustedfirm@gmail.com (This is just an example, but it is always a different domain.) Sometimes the true email address is embedded (e.g. RealEstateBroker<<realestatebroker.trustedfirm@gmail.com>>), which could mask the true email address, further hiding the true identity of the fraudster/sender.
d) The email could be directed either to the buyer or closing attorney:
e) If to the buyers: the buyers are directed to wire funds (for closing or additional earnest money) to the fraudster, believing they are complying with instructions from the realtor.
f) If to the closing agent: the closing agent is directed to wire the funds to the fraudster, believing that they are complying with the instructions from the Seller.

The stories of Social Engineering Fraud are plentiful, and this is fertile ground for fraud right now. We have repeatedly regaled you with stories of this type of fraud and steps to take to protect yourself and your client. People, however, are still getting tricked. Training your staff will only go so far-- you need crime insurance coverage to protect you against this threat. You should be certain to inquire about the inclusion of this type of coverage in your policy.

Let's Talk Cost

We have already covered the potential costs of not having insurance to cover these losses, so what does it cost? Every business has to do a cost benefit analysis to determine what amount of insurance fits their needs. You can adjust this cost by changing the amount of coverage and the deductible, but it is still "yet another cost of doing business" in these changing times.

First, this coverage is generally determined by the number of employees in your firm. It is not determined by the number of people with access to the trust account, but the number of people with access to a phone or computer – that includes you. On average, for the firm having a total of two to five people (not attorneys, but number of people), you can generally count on these types of coverages costing you between $1,700 and $2,400 a year or between $140 and $200 a month. You can count on it going up slightly with each additional employee; however, the cost per additional employee goes down as the number of employees goes up. No, it is not cheap – but it is cheap in comparison to a loss due to cyber-fraud. Why is it this expensive? The answer is easy. It is expensive because it is paying claims when your brethren are getting hit with cyber-fraud.

(Continued on page 6)

(Continued from page 5)

I TOLD YOU SO

If you go back through your email for just the past week, you will see that you have probably avoided some attempt at cyber-fraud. Someone emailed you about a bogus closing, a bogus wire, bogus invoice, a special gift that you have won, a racy picture, or a long lost relative that has left you a windfall. We are almost numb to some of these attempts, but they are still attempts at cyber-fraud. In most cases, cyber-fraud is committed because we let the fraudster in the house and they then take what they want. Let's face it: you know that you are a target. You have always known. Cyber-fraud Insurance is the next logical step, we have just been trying to put off the cost as long as possible.

Unfortunately, we cannot avoid the phrase "**I TOLD YOU SO**." In this instance, it will come from one of two places. First, it can come when you look in the mirror the day after the loss has occurred due to cyber-fraud, and you tell yourself these hurtful words. Second, it can come from your insurance agent when he or she hands you a check to cover your loss and they tell you "**I TOLD YOU THAT YOU WOULD NEED THIS COVERAGE**."

My hope for you is that you experience the second of these "**IT TOLD YOU SOs**" and not the first. If it is the case in which you are telling yourself these fateful words, you could be living like the "Settlers," with the most modest and inexpensive way of life - and not by your choice.

About the Author: Jonathan Biggs, Esq., VP & Director of Risk Management & Education
jbiggs@invtitle.com

Jon Biggs oversees risk management functions related to Investors Title's approved provider system. In this role, he oversees the approval process, develops educational seminars and communications-based initiatives involving approved providers and agents, and manages provider data and analysis related to the company's risk management efforts. Prior to joining Investors Title in 2012, he was partner at a firm in Durham, North Carolina, where he practiced residential and commercial real estate law for more than 20 years. Mr. Biggs holds a bachelor's degree from Duke University and a Juris Doctor from Wake Forest University School of Law.