Does Your Company do Wire Transfers? If so, be Careful

GUEST EDITORIAL
By Becky Harding, CPCU
Director of Association Programs
JD Fulwiler & Company Insurance
1-877-924-5777

It's Monday morning and you come to your office, turn on your computer and prepare to start your day. Before you can do so, your bookkeeper comes in and tells you one of your worst nightmares. Over the weekend, someone hacked into your company's computer system and gained access to the bank records, passwords and relevant security information. With this information, the hacker then proceeded to wire money from your bank account to his or her account somewhere in India. Your accounts have been drained dry.

What do you do? Who is going to pay for this? How will you get your money back?

Wire transfer risk is real, and it happens more often than you may think.

Will the Bank Accept Liability?

When you arrange for wire transfers with your company's bank from your corporate account, the following two things will typically happen.

1. You will be asked to sign an authorization letter which becomes a permanent record on file with the bank. This authorization letter will stipulate who can complete the wire transfer within your organization and will also have several security questions that must be asked to the authorized employee each time a wire transfer is requested.
2. You will be asked to submit a separate form for each individual wire transfer request. This is the form that stipulates the amount of the transfer, where the money should go, etc.

At the time of the wire transfer, the bank should ask the previously agreed-upon security questions, make sure the person is authorized per the record on file and confirm that the wire transfer authorization information is accurate.

If the bank does NOT follow the security protocol, it can be held liable for a fraudulent wire transfer.

However, if it DOES follow protocol but the hacker was good enough to obtain the security questions and answers from your system, convince the bank he or she was the authorized employee and the transfer ultimately goes through, the bank is NOT legally liable for your loss. You are on your own.

Banks are extremely regimented. They follow protocol and their phone calls are usually recorded. Even if you suspect your bank did NOT follow the security guidelines, obtaining proof can be nearly impossible. It is incredibly rare that a bank does not follow through with its security obligations.

The odds are that you will not be reimbursed by the bank and should look to an alternative remedy for this exposure.

How can I Protect Myself?

There are two ways to procure coverage for this unique, but all-too-real risk:

1. ***A Crime Policy*** — Most companies now cover Crime exposures on their commercial insurance policies. There are many Crime coverages available, but most business owners are electing to only cover Employee Dishonesty. The Employee Dishonesty limits chosen usually range from $25,000–250,000. You can add coverage called "Funds Transfer Fraud" to your existing Crime policy to cover yourself in the event the bank does not accept liability in the scenario being discussed in this article. The only downside to this option is that you typically cannot add Funds Transfer Fraud at a limit higher than your Employee Dishonesty limit. So, if you have Employee Dishonesty at $50,000, you are limited to $50,000 for Funds Transfer Fraud as well.
2. ***A Cyber Liability Policy*** — Cyber Liability policies cover your company for a variety of things, but most of the policies are purchased for coverage against hacker activity. This can be the loss of your customers' personal information, such as credit card numbers, addresses, etc. It also protects your employees' personal information which may be stored on your company's database. You are liable for the staunch protection of this information as well as the notification to these individuals if their personal information is compromised. The liability limits on the Cyber Liability policy are usually $1,000,000. "Funds Transfer Fraud" can also be added to the Cyber Liability Policy, limited to 50% of the Cyber Liability limit. So, if you have a Cyber policy with a limit of $1,000,000, you can add the Funds Transfer Fraud coverage for a limit of up to $500,000.

Determining which option is most appropriate for your organization depends on your operation. Do you have a Crime policy currently on your commercial insurance package? Do you have a Cyber risk *other* than Funds Transfer that would make a Cyber Liability policy attractive?

These are all things to discuss with your broker. As computer fraud and the hacker world become more sophisticated, these issues become more important to bring to the forefront. A thorough review of your exposures and your coverage are paramount between you and your insurance professional.

As the preferred insurance agency of the NTEA, JD Fulwiler developed the ***Protection Plus*** *program to provide the industry with underwriting, risk assessment and loss prevention services. JD Fulwiler will shop among many top insurance carriers with which it does business to find a coverage solution that best meets your needs. For more information on the Business Insurance Program, visit NTEA.com or call 1-800-441-6832.* ❖