What to know about wire transfer risk

Guest editorial
Becky Harding, CPCU
Director of
Work Truck Total Protect
877-924-5777
becky@worktrucktotalprotect.com

It's Monday morning and you come to your office, turn on your computer, get a cup of coffee and see your employees standing in a huddle discussing something. Curious, you inquire about their conversation. You are alarmed by their looks of sadness and fear … and then the bookkeeper tells you the alarming news. Over the weekend, someone hacked into your company's computer system and gained access to bank records, passwords and relevant security information. With this data, the hacker then proceeded to wire money from your bank account to their account. Your accounts have been drained dry.

What do you do? Who is going to pay for this? How are you going to 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, 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 letter will stipulate who can complete the wire transfer within your organization and will also have several security questions the authorized employee must answer 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 individual they're speaking with is authorized per the record on file and confirm the wire transfer authorization information is accurate. If they do not follow the security protocol, they can be held liable for a fraudulent wire transfer.

However, if they do follow protocol but the hacker was good enough to obtain the security questions and answers from your system, convince the bank they were 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. Their phone calls are usually recorded. Even if you suspect they did not follow the security guidelines, proving it can be nearly impossible. It is incredibly rare that a bank does not follow through with their security obligations.

The odds are that you will not be reimbursed by the bank and would need to look for 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 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. A 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 data 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, typically limited to 50% of the Cyber Liability limit. So, if you have a Cyber Liability policy with a limit of $1,000,000, you can usually add the Funds Transfer Fraud coverage for a limit of up to $500,000.

Determining which of these options 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 exposure other than Funds Transfer that would make a Cyber Liability policy attractive?

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

> **"At the time of the wire transfer, the bank should ask the previously agreed-upon security questions, make sure the individual they're speaking with is authorized per the record on file and confirm the wire transfer authorization information is accurate."**