Arlington/Roe®

Managing General Agents | Wholesale Insurance Brokers

WIRE FRAUD LIABILITY & CYBER INSURANCE

WHAT'S HAPPENING?

Wire Fraud is something we are seeing more and more. It's becoming a big issue, especially with all the business email compromise (BEC) scams going around. A lot of businesses don't realize that if they fall victim to one of these scams, the liability isn't always black and white. Sometimes, it gets split between multiple parties, depending on who had the best chance to prevent the fraud in the first place. Hackers are getting into business email accounts (usually because someone clicks a bad link or has a weak password), then they impersonate someone—a vendor, an executive or even a client. They'll send a fake email asking for a wire transfer, and before anyone realizes it's a scam, the money is gone.

WHO IS ON THE HOOK FOR THE LOSS?

It depends. Courts look at:

- Did the business have basic security measures in place, like multi-factor authentication (MFA)?
- Did the person sending the money double-check the request with a phone call or another method?
- Has the company been targeted before, and should they have known better?

REAL-LIFE EXAMPLE

A real estate closing agency got hit with a BEC attack. A hacker spoofed the agency's email and sent fake wiring instructions to a homebuyer. The buyer sent the money to the wrong account, and -poof- gone.

- The buyer blamed the closing agency for not securing their email system.
- The closing agency blamed the buyer for not double-checking before wiring the money.
- In the end, the court split the liability, meaning both had to eat part of the loss.

HOW CYBER INSURANCE CAN HELP

Here's the tricky part—not all cyber policies cover wire fraud, and even when they do, the coverage might be limited.

- Some cyber policies exclude wire fraud altogether.
- Fidelity or crime insurance may help, but not always.
- A good cyber policy can help cover fraud losses, forensic investigations and legal fees.

WHAT YOU (AND YOUR CLIENTS) CAN DO

1. Use MFA on email accounts—this alone prevents a ton of attacks.
2. Verify payment instructions with a second method (like calling the vendor directly).
3. Train employees to spot phishing and fraud attempts.
4. Make sure clients know what their cyber policy covers—most don't realize wire fraud isn't always included.

If you want to dive deeper into the legal side, check out the full article here.

Let one of our brokers know if you'd like to discuss this further.

Alec Immordino | ext 8784 | aimmordino@arlingtonroe.com
Essie Bennett | ext 2260 | ebennett@arlingtonroe.com
John Immordino | ext 8732 | jimmordino@arlingtonroe.com
Mark Swayze | ext 8648 | mswayze@arlingtonroe.com
Melissa Hilgendorf | ext 8774 | mhilgendorf@arlingtonroe.com
Sam Watts | ext 8580 | swatts@arlingtonroe.com
Sarah Immordino | ext 8731 | simmordino@arlingtonroe.com
Shelly Caldwell | ext 8687 | scaldwell@arlingtonroe.com
Sonyia Townsend | ext 8668 | stownsend@arlingtonroe.com