SANDBERG PHOENIX

PROFESSIONAL LIABILITY BLOG

Beware of the Hacker: Cyber Protection During Pandemics and Beyond

AUTHOR: NICHOLAS P. VAN DEVEN

CONTRIBUTOR: KATRINA SMELTZER

We live in interesting times. Most online nomads have grown tired of hearing about how the current health pandemic has – and will continue to – impact their daily lives both at home and the office. Businesses are inundated daily with posts about new laws, court closures, insurance coverage strategies and projected economic recovery timelines. As more employees around the country continue to log in from home instead of within the four corners of an office, one issue merits a closer look for all professionals – hackers.

The issue is most prevalent for businesses who handle, transfer and wire funds for the benefit of third parties. When wire transactions are compromised, courts have embraced a comparative fault analysis. Simply, the "party who was in the best position to prevent the forgery by exercising reasonable care suffers the loss." See *J.F. Nut Co. v. San Saba Pecan, L.P., 2018 WL 7286493 (W.D. Texas 2018); Arrow Truck Sales, Inc. v. Top Quality Truck & Equipment, 2015 WL 4936272 (M.D. Fla. 2015)*; see also *UCC Section 3-404(d); State Sec. Check Cashing, Inc. v. Am. Gen. Fin. Services, 972 A.2d 882 (Md. Ct. App. 2009)*. When analyzing comparative fault in these scenarios, the courts have used the UCC's "imposter rule" for guidance. In other words, whomever was the cause in fact of the misdirected payment should shoulder the responsibility for its misdirection.

Each of these cases turns on the nuanced facts presented. There is no preference for protecting or targeting a certain category of professional. Brokers, agents, lenders, service providers and customers all must heed the warning of the courts. If you want the court to protect your money and electronically stored and shared information, you need to take affirmative steps to protect it.

Sure. This seems simple in principle. But, in practice, things get lost. It's the way of the world today. Fast, direct, done. And now, more than ever before, more employees are working from their "home office" (i.e. kitchen table).

So, regardless of the brand of business you partake in, here is a non-exhaustive checklist of considerations to review internally with your loss mitigation or risk management team:

- Preference for wire instruction confirmation made by phone or other real time, verifiable writing;
- Require strong passwords and other multi-factor authentication and access through virtual private networks (VPN's);

- If you are uncertain about whether your employee's email and other systems are currently protected as they work from home, contact your providers about free or other budget friendly options, including complimentary training sessions;
- Keep an eye out for changing state and federal regulations on the issue of business cyber-security to ensure your business is legally compliant on the topic since that will, at a minimum, likely be the standard of care by which you are judged in a suit for negligence;
- Investors and venture capitalists will likely favor investing in companies with these protections in place which can impact profitability going forward in an already gloomy fiscal 2020;
- Review and strengthen terms of existing cyber policies with carriers or as policies come due for renewal;
- Be prepared for employees to become more comfortable working from home and after the cessation of the virus requesting that their remote participation continue and have a plan in place;
- Advise remote employees to keep laptops within their physical control and screens hidden from others;
- Contemplate narrowing the field of personnel with authorization to confirm and initiate financial transfers;
- Log off; and
- Again, log off.

This is not the end all, be all. If anything, this list should get the conversation going. It should continue with your insurance carriers, local bank officer and remote employees. Start a dialogue about it during your next WebEx team meeting or planning session. Above all else, be well and stay safe.