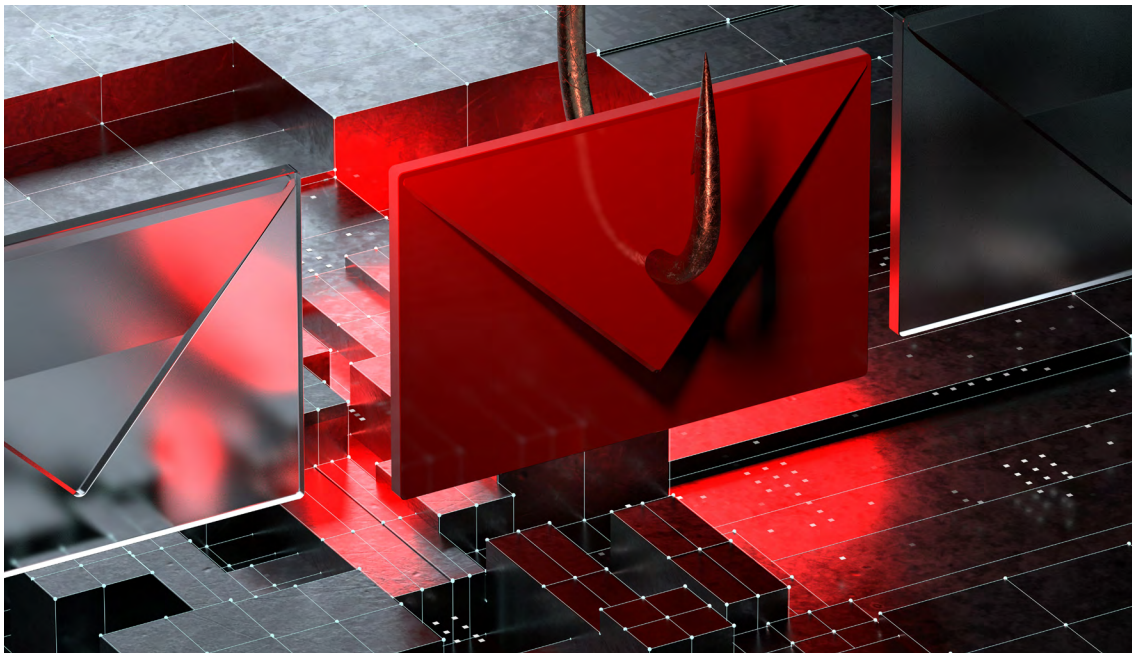
LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com
THURSDAY, DECEMBER 15, 2022

PERSPECTIVE

Email scam losses may find recourse via cyber or business interruption coverage

By Peter S. Selvin



Shutterstock

Losses arising from email scams are usually covered, if at all, under a company's crime policy. But a recent decision from The District Court in Minnesota suggests that recourse may also be found under an insured's cyber or business interruption coverage. Importantly, the decision suggests that a "data breach" triggering cyber coverage may occur where a bad actor infiltrates and manipulates an insured's email system.

In *Fishbowl Sols., Inc. v. Hanover Ins. Co.*, 2022 U.S. Dist. LEXIS 200210 (D. Minn. Nov. 3, 2022), a bad actor gained unauthorized access to the email account of Fishbowl's senior staff accountant, Wendy Williams. The bad actor then created multiple "rules" within Williams' account that interfered with proper receipt of incoming emails.

Those rules also redirected emails with the words "invoice," "wire transfer" or "payment" to an email account controlled by the bad actor. Another rule diverted emails from Williams' inbox to a subfolder and marked them as read. The rules impacted Williams' ability to communicate with certain Fishbowl clients. In addition, the bad actor sent emails to and from Williams' account, at times impersonating her and at times impersonating Fishbowl clients.

While those rules were in place, Fishbowl issued two invoices to its customer Federated. Following the issuance of those invoices, the bad actor, impersonating Williams, emailed Federated and stated that Fishbowl had recently changed banks. The email directed Federal to make its payments to a bank account controlled by the bad actor.

Believing that the email was from Williams, Federated made payment to the account controlled by the bad actor. When Williams reached out to Federated to confirm payment of the invoices, the bad actor, now impersonating Federated, responded by saying that payment had been initiated and would appear in Fishbowl's account. In fact, Federated had sent the payments to the bad actor's account, resulting in a loss to Fishbowl of around $180,000.

Fishbowl's insurer Hanover issued a policy which contained a "Cyber Business Interruption and Extra Expense" clause which provided as follows:

"We will pay actual loss of 'business income' and additional 'extra expense' incurred by you during the 'period of restoration' directly resulting from a 'data breach,' which is first discovered during the 'policy period' and which results in an actual impairment or denial of service of 'business operations' during the 'policy period'."

This language contains elements of both cyber coverage ("data breach") and business interruption coverage (loss of "business income … during the period of restoration").

Peter Selvin *is a partner at Ervin Cohen & Jessup LLP and chair of the firm's Insurance Coverage and Recovery Department.*

As such, some of the court's determinations are relevant to both forms of coverage.

After Hanover denied Fishbowl's claim, Fishbowl sued. Both Fishbowl and Hanover filed cross motions for summary judgment. Finding coverage for Fishbowl's loss under the foregoing policy language, the Court granted Fishbowl's motion and denied Hanover's motion.

At the threshold, Hanover did not dispute that the infiltration and manipulation of a Fishbowl's email system was a "data breach." This itself is notable because data breaches are normally understood as an instance in which cyber attackers gain access to personal information that is stored on a database. *See, e.g., In Re Anthem, Inc. Data Breach Litig.*, 2018 U.S. Dist LEXIS 140137 (N.D. Cal. 2018). Nevertheless, and while the decision does not disclose how the policy defined "data breach," the fact that this "spoofing" incident triggered coverage suggests that practitioners ought to look to their clients' cyber coverages in seeking reimbursement for losses arising from email scams.

As revealed in the summary judgment briefing, the core disputes between Fishbowl and Hanover had to do with policy terms that frequently arise in business interruption coverage – whether the disruption of customer payments representing already completed work constituted "business income;" and whether the bad actor's interference in the payment of Fishbowl's invoices constituted the impairment of Fishbowl's "business operations."

As to the first issue, Hanover argued that as used in the context of business interruption policies, the term "business income" typically means forward looking income-generating activity that would have occurred but for the "interruption" event. *See, e.g., Nat'l Union Fire Ins. Co. of Pittsburgh v. Transcanada Energy USA, Inc.*, 52 Misc. 3d 455 (N.Y. Sup. Ct. 2016). Hanover further argued that because payment on the Fishbowl invoices represented money already earned, rather than money that would have been earned, Fishbowl did not suffer a loss of "business income." The Court rejected Hanover's position on this point.

Similarly, the Court rejected Hanover's position that the bad actor's interference in Fishbowl's collection of payments on its invoices constituted an "impairment" of its "business operations." The Court noted that the policy's use of the word "impairment" distinguished the case from those instances where the complete suspension of an insured's business was required to trigger coverage. *See, e.g., Buxbaum v. Aetna Life and Casualty Company*, 103 Cal. App. 4th 434 (2002) (complete suspension of all business operations was required for business interruption coverage to be triggered). The Court concluded that the use of the word "impairment" rather than "interruption" demonstrated that the pertinent clause in the policy "grants coverage when a business suffers something less than a total suspension of operations." *Id.* at *27.

Finally, Hanover argued that because Fishbowl was allegedly negligent in failing to notice warning signs in the fraudulent emails and the charged payment instructions, the loss was not "directly resulting" from the data breach. *Id.* at *19. Importantly, this argument echoes similarly unsuccessful arguments about direct causation frequently made by insurers where a loss from an email scam is asserted under a crime policy. *See, e.g., Am. Tooling Center, Inc. v. Travelers Cas. & Sun Co. of Am.*, 895 F.3d 455 (6th Cir. 20180 ("direct loss" requirement satisfied); *Ernst & Haas Mgmt. Co. v. Hiscox, Inc.*, 23 F. 4th 1195 (9th Cir. 2022) (finding that the loss "result[ed] directly" from the email scam). While the Court in Fishbowl did not cite to the foregoing cases in rejecting Hanover's causation argument, it found that because Fishbowl's loss would not have occurred without the bad actor accessing Ms. Williams's email and sending fraudulent communications, Fishbowl's loss "directly result[ed] from" the data breach. *Id.* At *23.