

## Minnesota Court Rules That Email Hacking Scheme Losses Are Covered Under Cyber Business Interruption Provision (Insurance Law Alert)

11.30.22



(Article from *Insurance Law Alert*, November 2022)

For more information, please visit the [Insurance Law Alert Resource Center](#).

A Minnesota district court granted a policyholder's summary judgment motion, ruling that losses stemming from a hacking scheme that allowed a bad actor to intercept and impersonate emails relating to invoice payments were covered under a Technology Professional Liability Policy. *Fishbowl Solutions, Inc. v. Hanover Ins. Co.*, 2022 WL 16699749 (D. Minn. Nov. 3, 2022).

Fishbowl was the victim of a scheme in which a bad actor gained access to the email account of a senior accountant and impersonated her in communications with clients in order to provide new payment instructions for invoices. After discovering the fraud, Fishbowl sought coverage under a provision that stated:

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."

Hanover denied the claim on several bases, each of which was rejected by the court.

**Actual Loss of Business Income:** Hanover argued that there was no loss of "business income," defined as "Net Income . . . that would have been earned or incurred if there had been no impairment or denial of 'business operations.'" Hanover claimed that business operations refer only to income-generating activities and that invoicing clients does not generate income, and that Fishbowl sought recovery of money already earned, rather than money "that would have been earned." Rejecting these contentions, the court concluded that the policy did not expressly limit business operations to income-generating activities and that the diversion of invoice payments was income that "would have been earned" (rather than income that was already earned) notwithstanding that the work for those invoices had already been performed.

**Directly Resulting From Data Breach:** While Hanover conceded that Fishbowl experienced a data breach, it argued that the loss did not result directly from that breach. Rather, Hanover claimed that the loss resulted from intervening causes, including the negligence of the customer that remitted payment to the bad actor without noticing warning signs about potential fraud. Noting the lack of evidence of such negligence, the court declined to find such "intervening agency" and ruled that Fishbowl's losses "would not have occurred without the bad actor accessing

Ms. Williams’s email and sending fraudulent communications.”

*Impairment of Business Operations:* Hanover argued that there was no impairment or interruption of Fishbowl’s business operations because it continued to conduct its normal income-generating activities even during the period of email hacking. Rejecting this assertion, the court held that the term “impairment” is sufficiently broad so as to encompass the hacker’s interference with the accountant’s email and does not require a business to cease functioning entirely. The court noted that while the provision includes the word “Interruption” in its title, use of the word “impairment” within the text of the provision indicates that the policy “specifically grants coverage when a business suffers something less than a total suspension of operations.”

Authors and  
Contacts

Bryce Friedman  
Partner  
[bfriedman@stblaw.com](mailto:bfriedman@stblaw.com)  
[+1-212-455-2235](tel:+12124552235)

Chet Kronenberg  
Partner  
[ckronenberg@stblaw.com](mailto:ckronenberg@stblaw.com)  
[+1-310-407-7557](tel:+13104077557)

