

Data breach

An online retailer of medical products discovered that its primary website was attacked. Spotting a vulnerability, hackers had inserted malware onto the site and managed to gain access to a database containing the credit card details of over 90,000 customers.

Due to local breach notification laws in place, the retailer had to notify all 90,000 individuals affected by the incident and provide them with identity theft restoration services. This wasn't the end of the incident, however. Immediately after the notification, the business noticed a significant drop-off in sales.

Following an investigation by forensic accountants, it was established that the insured had lost a total of 5,196 orders as a direct result of notification over a 12-month period, resulting in a business interruption loss of \$475,646. The cost of this reputational damage came on top of the \$230,000 incurred to remove the malware from the business's website, provide legal advice, and carry out the notification process. The entire loss, including the business interruption caused by reputational damage, was covered under the retailer's cyber insurance policy.