

# Report: Travelex paid hackers \$2.3 million worth of Bitcoin after ransomware attack

GC [grahamcluley.com/travelex-paid-ransom/](https://grahamcluley.com/travelex-paid-ransom/)

April 9, 2020



Remember how back in January I raised one of the central mysteries behind Travelex's ransomware attack – namely, had the foreign currency exchange service paid its attackers a ransom or not?

Travelex was notably refusing to answer any questions about whether it had given in to the extortionists' demands.

But now, the *Wall Street Journal* reports, it sounds like Travelex paid US \$2.3 million worth of Bitcoin to the REvil ransomware gang, who had threatened to publish personal data of customers stolen from Travelex's network.

Owned by London-listed payments conglomerate Finabl PLC, Travelex found its operations crippled by a New Year's Eve ransomware attack that left some of its systems offline for weeks. The finance company paid out the ransom in the form of 285 bitcoin, according to the person with knowledge of the transaction.

Asked about the payment, a Travelex spokesman said the firm has taken advice from a number of experts and has kept regulators and partners informed about its efforts to manage the recovery. A U.K. law-enforcement investigation into the breach is continuing, he said. He declined to comment further on the incident.

Whether ransoms should be paid or not is a divisive topic, and I find it hard to give a simple answer. I can well understand the position of those who say that it encourages more ransomware attacks against other organisations if a ransom is paid. It certainly does.

But at the same time, when a company is on the ropes, it has no other options, and its survival is in question, it's hard not to sympathise with a difficult decision being made to pay those who were behind the attack if it helps ensure the firm stays afloat, and jobs are saved.

 **Sign up to our newsletter**

Security news, advice, and tips.

Travelex's management team had been strongly criticised for its shambolic response to the attack, which saw the firm delay confirming it had been hit by ransomware for over a week.

Eventually Travelex began to hobble back online at the end of January.

The financial problems faced by Travelex and its parent company, Finabl, have only increased in the months since due to the enormous impact the Coronavirus pandemic has had on its business.

*Found this article interesting? Follow Graham Cluley on Twitter to read more of the exclusive content we post.*

- 
- Malware
  - Ransomware
  
  - #Malware
  - #ransomware
  - #Revil
  - #Travelex



**Graham Cluley** • @gcluley

Graham Cluley is a veteran of the anti-virus industry having worked for a number of security companies since the early 1990s when he wrote the first ever version of Dr Solomon's Anti-Virus Toolkit for Windows. Now an independent security analyst, he regularly makes media appearances and is an international public speaker on the topic of computer security, hackers, and online privacy. Follow him on Twitter at @gcluley, or drop him an email.