# FatFace sends controversial data breach email after ransomware attack

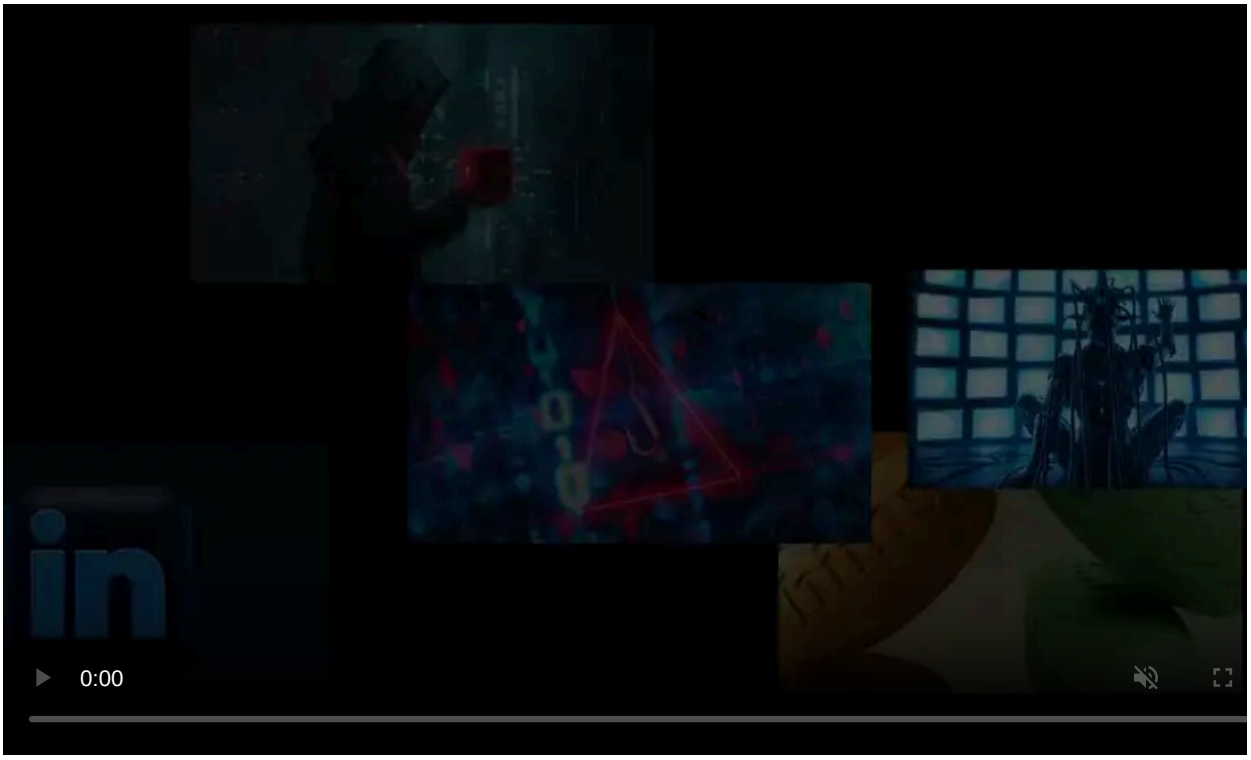
By Lawrence Abrams

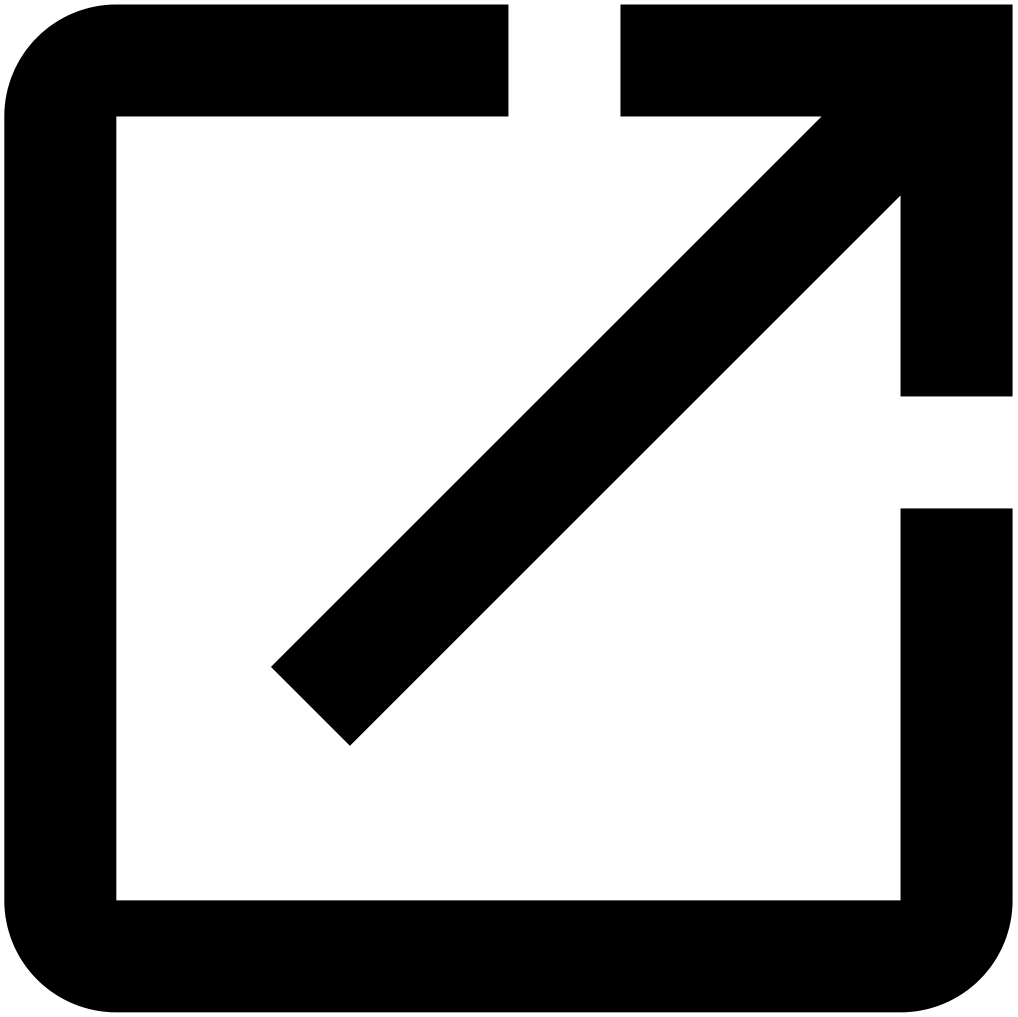
Published: 2021-03-27 · Archived: 2026-04-05 18:19:25 UTC


British clothing brand FatFace has sent a controversial 'confidential' data breach notification to customers after suffering a ransomware attack earlier this year.

This week, customers began receiving data breach notifications revealing that the popular lifestyle clothing brand, FatFace, had suffered a data breach after a cyberattack on January 17th, 2021.

According to the notification, threat actors gained access to FatFace's network and systems and accessed customer data. This data customers' names, email addresses, mailing addresses, and partial credit card information (last four digits and expiration date).


0:00



What was controversial about the data breach notification is that it told recipients to "Please do keep this email and the information included within it strictly private and confidential."

BleepingComputer has covered many data breaches. We have never seen a company asking a user to keep a data breach confidential and likely has no power to make that request.

As you can imagine, this single sentence led to quite an uproar on Twitter, with users baffled that the notification would include that type of language.

> It's a bit rich that @FatFace wait two months to inform their "valued customers" of a serious data breach and tell us to keep the email and information included in it strictly private and confidential!
>
> — Moira M (@reiver_rover) March 24, 2021

While many felt that FatFace was trying to keep the data breach under wraps, it turns out there was much more to the story.

## Data breach caused by a ransomware attack

According to Computer Weekly, the data breach was caused by a Conti ransomware attack in January 2021.

A ransom note found by Valéry Marchive of ComputerWeekly's sister-publication LeMargIT allowed the publication to review a ransom negotiation between FatFace and the ransomware gang.

As is common in today's ransomware attacks, the threat actors reviewed the victim's financial data before deploying the ransomware. This review provided insight into the company's finances, including FatFace's cyber insurance coverage, which the threat actors brought up during the negotiations.

While Conti originally asked for $8.5 million, the negotiations ultimately led to a payment of $2 million to gain access to a decryption key and a promise not to leak the 200GB of stolen data.

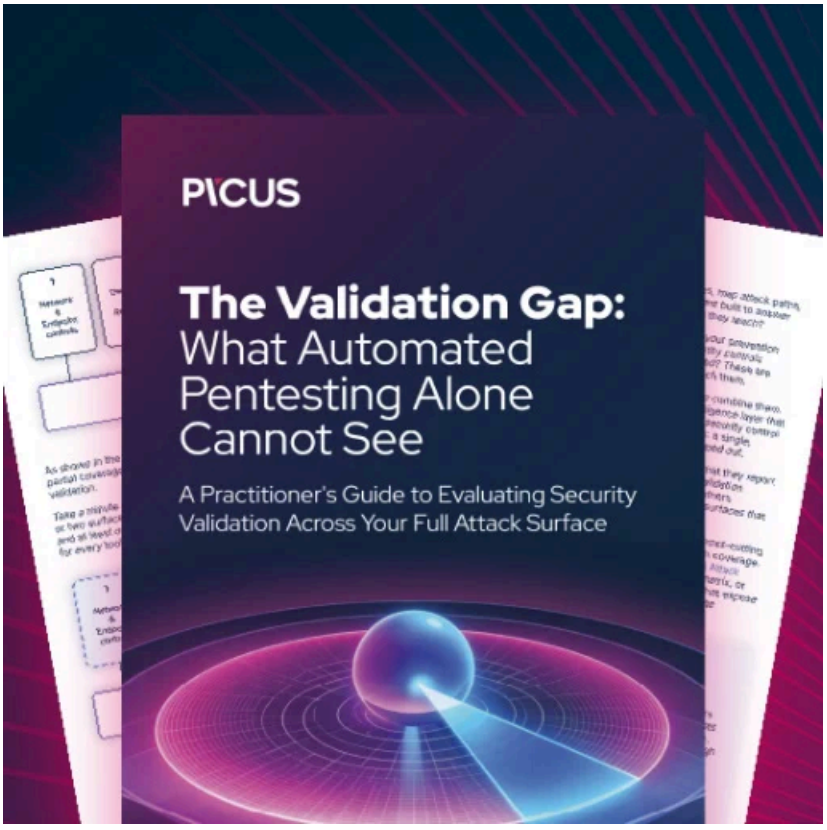
The threat actors stated that they gained access to an internal FatFace workstation via a phishing attack on January 10th, 2021, where they then spread laterally through the network.

"From there, the team was able to obtain general administrative rights and began to move laterally through the network, identifying the retailer’s cyber security installations, Veeam backup servers and Nimble storage. The ransomware attack itself was executed on 17 January and saw more than 200GB of data exfiltrated," Computerweekly reported.

The Conti gang also provided the victim with a report on how to better protect their network, including email filtering, phishing awareness tests, better Active Directory password policies, EDR technology, and an offline backup strategy.

When contacted by ComputerWeekly, FatFace confirmed the ransomware attack and said they reported it to law enforcement and the Information Commissioner’s Office (ICO).

> “FatFace was unfortunately subject to a ransomware attack which caused significant damage to our infrastructure." -FatFace.




## [Automated Pentesting Covers Only 1 of 6 Surfaces.]

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

---