Fashion titan French Connection says 'FCUK' as REvil-linked ransomware makes off with data

By Gareth Halfacree

Published: 2021-06-24 · Archived: 2026-04-05 14:31:31 UTC

Cheeky clothing firm French Connection, also known as FCUK, has become the latest victim of ransomware, with a gang understood to be linked to REvil having penetrated its back-end - making off with a selection of private internal data.

Founded in 1972 by current chief executive Stephen Marks, French Connection made a name for itself when it adopted the not-actually-rude-honest slogan "FCUK" in its advertising in the early 2000s. Originally founded as a mid-market women's fashion brand, the company has since expanded into menswear, watches, toiletries, and even glasses.

Sadly, attackers understood to be related to the REvil ransomware gang needed no such optical enhancements to spot a security vulnerability in the company's back-end systems. As a result, they've made off with a trove of internal company data.

Passport and identification card scans seen by *The Register* have been used by the gang as proof-of-breach, covering a range of staff members - including founder and chief executive Marks, chief financial officer Lee Williams, and chief operating officer Neil Williams.

In a statement to *The Register* French Connection confirmed it had "been the target of an organised cyber-attack affecting its back-end servers, which control its internal systems and operations."

- The latest REvil ransomware victim? Sol Oriens. Oh, a US nuclear weapons contractor
- Ransomware-skewered meat producer JBS confesses to paying $11m for its freedom
- The policy of truth: As ransomware claims rise, what's a cyber insurer to do?
- Clothes retailer Fatface: Someone's broken in and accessed your personal data, including partial card payment details... Don't tell anyone
- Risk and reward: Nefilim ransomware gang mainly targets fewer, richer companies and that strategy is paying off, warns Trend Micro

French Connection was keen to point out, however, that front-end servers, including those which process payments for its online and high-street outlets, are not thought to have been affected by the attack.

"As soon as it became aware of the breach, the company took immediate action, suspending all affected systems and engaging third-party experts to assist with resolving the situation," French Connection's statement continued. "The company is now actively working to restore its systems as quickly and safely as possible and where necessary is using manual overrides in order to ensure that the company can continue to operate."

French Connection said it had "no evidence" to suggest that any data relating to its customers had been accessed during the breach, and that so far the attack has "not had a material impact on trading" with the company "continuing to operate largely as normal."

Data snaffled by REvil and other ransomware gangs is typically offered up for sale, with the original owners given a demand before the sale is dangled in front of the black-market.

French Connection refused to comment on whether it had received such a demand and, if so, how much it was asked to pay to keep the data private.

It did confirm it had contacted the authorities, including reporting the breach to the Information Commissioner's Office (ICO), as is its legal obligation. ®
