VERDICT

# Equifax fine: ICO issues £500k penalty after data of 15m UK customers compromised

The Information Commissioner's Office (ICO) has fined credit rating agency Equifax £500,000 for failing to protect the personal data of up to 15m UK customers compromised during a cyber attack in 2017.

The breach occurred between 13 May and 30 July 2017. It affected 146 million customers globally. Compromised data included driving licences, financial details, dates of birth, addresses and passwords.

Information Commissioner Elizabeth Denham said:

> "The loss of personal information, particularly where there is the potential for financial fraud, is not only upsetting to customers, it undermines consumer trust in digital commerce.
>
> "This is compounded when the company is a global firm whose business relies on personal data."

While the breach occurred in the US, the ICO – the UK's non-departmental body in charge of policing data privacy – found that Equifax was responsible for the data of its UK customers.

Robert Wassall, Director of Legal Services at ThinkMarble, told *Verdict*:

"Although the cyber-attack happened in the US, the ICO was able to act because millions of UK citizens were affected. The comment that the UK arm of the company failed to take appropriate steps to ensure its American parent was protecting the information suggests that the ICO expects UK subsidiaries to ensure its overseas owners put in place appropriate security measures – ones that comply with the GDPR.

"The regulators clearly looked very closely at the data protection practices at Equifax and found that
personal information was being retained for longer than necessary – a very common situation at many organisations. This should act as a 'wake-up call' to those organisations that do not have robust data retention policies and practices in place.

"The ICO also found that there was a lack of legal basis for international transfers of UK citizens' data. This is a complex area and in practice organisations should avoid sending data outside the EEA if possible, to reduce risk."

## Equifax fine avoids $134m GDPR penalty

The Equifax fine is the highest possible under the 1998 Data Protection Act. Denham said this is "because of the number of victims, the type of data at risk" and because Equifax has "no excuse for failing to adhere to its own policies and controls as well as the law."

Wassall told *Verdict*:

With Equifax's global turnover in 2017 standing at $3.36bn, the credit rating agency could have faced a fine of up to $134.4m.

This year the ICO has issued a number of significant fines, reflecting a toughening stance towards data breaches. In July, for example, the ICO slapped Facebook with the maximum £500,000 fine for its handling of user data during the Cambridge Analytica scandal.

## How did the cyber attack happen?

The Government Accountability Office, the investigative arm of Congress, found that Equifax failed to install a patch to protect a weakness in a server hosting Equifax's online dispute portal.

The yet to be identified hackers exploited this vulnerability and sent 9,000 queries to dozens of databases containing customers' personal data. They were then able to extract the information and remain undetected for more than six weeks.

The ICO's investigation, running in parallel with the Financial Conduct Authority, found that personal information of UK citizens was retained for longer than necessary.

"Many of the people affected would not have been aware the company held their data; learning about the cyber attack would have been unexpected and is likely to have caused particular distress," said Denham.

## Biggest data breach in history?

The US Department of Homeland warned Equifax about the vulnerability two months before the breach occurred. The ICO concluded that the UK arm of its American parent, Equifax Inc, failed to take sufficient steps to remedy the weakness.

The estimated cost to Equifax for the data breach has reached $439m. According to Reuters, the credit rating agency's insurance company will only pay $125m, prompting some experts to comment that it could be largest data breach in history.

A new report released by congressional investigators noted that the Trump administration is yet to take action. The FBI, Consumer Financial Protection Bureau and Federal Trade Commission are also investigating in the US.

Equifax has since improved its cybersecurity and shaken up its management. In a statement, an Equifax spokesperson said:

> "Equifax has cooperated fully with the ICO throughout its investigation, and we are disappointed in the findings and the penalty.

> "As the ICO makes clear in its report, Equifax has successfully implemented a broad range of measures to prevent the recurrence of such criminal incidents and it acknowledges the strengthened procedures which are now in effect.
>
> "The criminal cyberattack against our US parent company last year was a pivotal moment for our company. We apologise again to any consumers who were put at risk.
>
> "Data security and combatting criminal digital activity is an ongoing battle for all organisations that requires continued innovation and attention. We have acted and continue to act to make things right for consumers. They will always be our priority."

Denham called for multinational companies to better understand and protect personal data in future.

> "Their boards need to ensure that internal controls and systems work effectively to meet legal requirements and customers' expectations," she said. "Equifax Ltd showed a serious disregard for their customers and the personal information entrusted to them, and that led to today's fine