RepRisk
Due diligence on ESG and business conduct

REPRISK CASE STUDY

# Equifax

## Equifax Data Breach Scandal

### What happened?

On September 7, 2017, the US-based consumer credit reporting agency Equifax announced that a cyber-attack on its computer systems between May and July 2017 had enabled hackers to access the personal data of about 143 million people in the US. By September 21, Equifax shares had plummeted by 33 percent following reports that the cyber criminals had been able to access full names, social security numbers, birth dates, and addresses, allegedly leaving consumers vulnerable to identity theft.

Although the attack reportedly began in mid-May, the CEO of Equifax claimed that the company had only discovered the breach on July 29, 2017.

A week after Equifax announced the data breach in the US, the security of the internal portal of Veraz, the company's Argentinian operation, was found to be vulnerable, as the records of thousands of customers could allegedly be accessed by using the word "admin" as both the login and password. It was claimed that the weakness could lead to a breach of the personal data of more than 100 employees and 14,000 customers from Argentina.

Equifax's troubles worsened when it came to light that its Chief Financial Officer and two other senior executives had sold shares in the company worth USD 1.8 million on August 1, 2017, just days after Equifax discovered the cyber-attack, and more than a month before the breach was made public. The discovery prompted the US Department of Justice (DOJ) to launch an investigation into the

## Case Study Timeline

**2017**

**May-July**
Equifax's computer systems are hacked.

**July 29**
Equifax's security team discovers the cyber-attack.

**August 1 and 2**
Three Equifax senior executives sell shares worth almost USD 1.8 million.

**September 7**
Equifax announces the breach, alleging that around 143 million US clients have been affected. The company's stock value plummets by 33 percent.

**September 15**
Equifax's Chief Information Officer and Chief Security Officer announce their immediate resignation.

**September 18**
DOJ launches an investigation into possible insider trading by three Equifax executives.

**September 26**
Equifax's CEO also announces his resignation.

**October 2**
Equifax admits that a total of 145.5 million Americans have been affected by the breach.

**October 10**
Equifax admits that the hackers also targeted customers in the UK and Canada.

**November 22**
The company is served with a 50-state class action lawsuit and faces around 240 individual class-action lawsuits as well as more than 60 investigations by US, British, and Canadian government agencies.

possible violation of insider trading regulations. On September 15, the company's Chief Information Officer and Chief Security Officer announced that they would be resigning with immediate effect. One week later, on September 26, 2017, Equifax's CEO also announced his resignation.

On October 2, 2017, Equifax admitted that 145.5 million Americans had been affected by the US data breach, 2.5 million more than previously thought. Two weeks later, Equifax announced that the breach had affected approximately 694,000 customers in the UK, as well as clients in Canada.

New York's Attorney General, the US Federal Trade Commission, the UK Financial Conduct Authority, and other government agencies launched investigations into the data breach. On November 22, 2017, the company was served with a 50-state class action lawsuit, accusing it of negligence in failing to prevent the data leak and mismanagement following the breach.

In January 2018, Equifax launched a free lifetime "credit lock" service for victims of its data breach in order to prevent would-be identity thieves from obtaining credits or loans.

On March 1, 2018, Equifax admitted that the names and drivers' license numbers of a further 2.4 million US citizens had been accessed during the 2017 data breach.

On March 15, the US Securities and Exchange Commission charged a former Equifax Chief Information Officer with insider trading over claims that he had exercised all of his 6,815 stock options and sold the resulting shares ten days before the breach had been made public.

One day later, the Australian Competition & Consumer Commission filed a lawsuit against Equifax's Australian subsidiary for violating consumer laws by making false or misleading claims about its credit reporting services.

## Was it foreseeable?

In June 2014, RepRisk reported that US state attorneys were conducting investigations into Equifax and other credit bureaus for inadequate consumer protection controls.

### Case Study Timeline

**2018**

**January 31**
Equifax launches a free lifetime "credit lock" service for victims of its data breach.

**March 15**
The US Securities and Exchange Commission charges a former Equifax CIO with insider trading.

**March 16**
The Australian Competition & Consumer Commission files a lawsuit against Equifax's Australian subsidiary for violating consumer laws.

In May 2016, RepRisk also identified reports of investigations into Veda Advantage, an Australian credit reporting agency purchased by Equifax in February 2016, by the Office of the Australian Information Commissioner over complaints that it had sold sensitive financial information to its marketing subsidiary, Inivio.

## Consequences for Equifax

At the time of writing, Equifax is facing approximately 240 individual class-action lawsuits and more than 60 investigations involving government agencies of the US, the UK, and Canada. The company has lost three senior executives and is struggling to rebuild trust with consumers.

## Company Description

**Equifax Inc** provides information solutions and human resources business process outsourcing services for businesses, governments, and consumers.

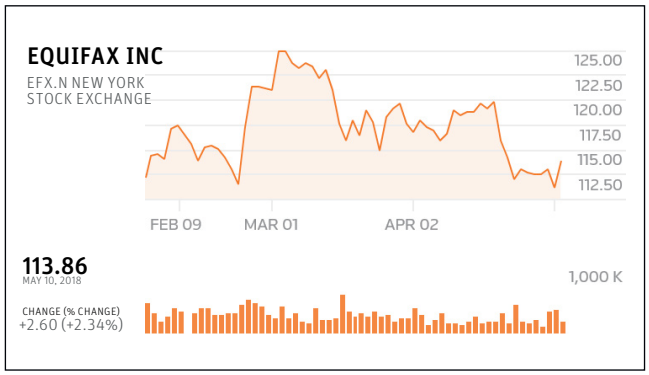


Figure 1: Equifax's share price on the New York Stock Exchange as of April 2018 (graph adapted). They have lost about a quarter of their value since Equifax disclosed the incident in early September 2017. Source: Reuters.