IADC COMMITTEE NEWSLETTER

CYBER SECURITY, DATA PRIVACY AND TECHNOLOGY

March 2018

IN THIS ISSUE

This article provides an overview of this important UK court decision that could have worldwide implications. In a class action lawsuit, the UK's highest court held that UK's largest supermarket chain was vicariously liable for its disgruntled employee's misuse of the company's payroll data despite finding that the supermarket chain was the intended victim. This opinion could start a trend of class actions for data breaches and have far reaching consequence for companies and insurers.

First Class Action Data Breach in the UK – Employer Found Vicariously Liable for Rogue Employee's Actions

ABOUT THE AUTHORS

Elena Jelmini Cellerini is a senior claims expert for EMEA where she deals with complex and multijurisdictional matters. She's also global Practice Group Leader for Cyber claims. She can be reached at elena_jelmini@swissre.com.

Vikram Khurana is a senior associate in the Commercial IP/IT team at Bristows where he specialising in technology, telecommunications and outsourcing projects. Vikram has in-depth experience of leading complex, strategic technology projects. He can be reached at vikram.khurana@bristows.com.

ABOUT THE COMMITTEE

Corporations and law firms around the world are constantly dealing with cybersecurity, data privacy and other important technology issues, both in business and, where available, in litigation discovery. Burgeoning technologies are placing new and increasing demands on in house and outside lawyers and their clients. All are being challenged to meet new and strict data privacy and security guidelines and the consequences for failing to meet these requirements can be devastating. The Cyber Security, Data Privacy and Technology Committee will address the differing substantive laws globally in these areas, and be of interest to many other committees whose members and activities are impacted by technology. Learn more about the Committee at www.iadclaw.org. To contribute a newsletter article, contact:

Elizabeth S. Fitch
Vice Chair of Publications
Righi Fitch Law Group
beth@righilaw.com

Facts: In 2014, Andrew Skelton, a disgruntled employee of Morrisons, one of the UK's largest supermarket chains, deliberately leaked payroll data relating to almost 100,000 Morrisons employees online. The data included bank sort codes, bank account numbers and salary details. Skelton was sentenced to eight years in prison for criminal misuse of the payroll data. While Morrisons took immediate action to protect the employees from financial loss, around 5,500 of the affected employees brought collective redress action (an EU form of class action) and sought emotional distress damages. This is the first case of its kind since the Court of Appeal in *Vidal-Hall v Google* in 2015 established that victims of data breaches can claim damages on the basis of emotional distress alone, without having suffered financial loss. The class action was brought on the basis that Morrisons was directly liable for Skelton's act (under the Data Protection Act 1998 (DPA), at common law (misuse of private information) or in equity (breach of confidence)), or alternatively on the basis that it was vicariously liable for its employee.

Decision: On 1 December 2017, the High Court handed down a lengthy judgment in which it found that, while Morrisons itself was not primary liable for the breach (the court holding it had taken reasonable steps to protect the data), it was nevertheless **vicariously liable for its employee's misuse.** The Court reached this conclusion despite it finding that Morrisons was effectively the intended target and victim of Skelton's actions (he had the specific intent of causing Morrisons harm), and the steps it took to protect data were sufficient or otherwise would not have prevented the breach. Notably, the Judge gave Morrisons permission to appeal his decision on vicarious liability, and Morrisons has stated that it will appeal the decision to the Supreme Court.

(Note: the 1 December 2017 judgment did not deal with quantum. This will be decided at a separate hearing if the parties do not reach agreement **– the claimants' lawyers are talking about a settlement of £300 per claimant – which would result in a total liability of about £1.6m.**)

Consequences: The application of employers' **vicarious liability** in this case to claims under the DPA in this case is notable, extending the concept of acting 'in the course of employment' to a data protection law (in a previous unrelated case, Morrison was found responsible for the acts of an employee who got into a fight with a customer). The judge himself suggested he may have had reservations about his own decision in granting permission to appeal: *"The point which most troubled me in reaching these conclusions was the submission that the wrongful acts of Skelton were deliberately aimed at the party whom the claimants seek to hold responsible, such that to reach the conclusion I have may seem to render the court an accessory in furthering his criminal aims."*

In addition, the judgment is likely to start a trend of **class actions for data breaches**.

Once the General Data Protection Regulation (GDPR) comes into force on 25 May 2018, employers involved in such breaches will face the risk of regulatory action (which could include fines of up to 4% of global annual turnover or €20m), class actions under EU rules, and vicarious liability for rogue employees (even where the employer is the target). While most organisations are already taking proactive steps to become GDPR-compliant, this judgment reinforces the need to protect data and ensure they are properly prepared to respond to incidents of data breaches. Some steps Morrisons could have done to further mitigate the actions of its employee include controlling employee access to data, using software to scan emails and data transfers, and enhanced employee monitoring and training.

Assuming Morrisons' appeal goes ahead, the Court of Appeal's consideration of the issues explored in the High Court will be hotly anticipated, and we look forward to its analysis as to whether data protection law permits vicarious liability and, indeed, whether such liability arises where as in this case the employer itself has not breached data protection law.

In terms of coverage, it will be interesting to see how the cyber market will react to the Morrisons case and if we start seeing coverage for criminal acts committed by employees. Such losses are currently typically excluded in standard cyber policies, under the criminal acts exclusion:

'We shall not be liable for Damages or Expenses on account of any Claim:

3.1 directly or indirectly caused by, arising out of or in any way connected with your conduct, or of any person for whose conduct you are legally responsible, which involves:
1. Committing or permitting any knowing or willful breach of duty, or violation, of any laws; or
2. Committing or permitting any criminal, deliberately fraudulent or deliberately dishonest act or omission; or
3. any actual or attempted gain of personal profit, secret profit or advantage by you to which you were not entitled.'

Past Committee Newsletters

Visit the Committee's newsletter archive online at www.iadclaw.org to read other articles published by the Committee. Prior articles include:

NOVEMBER 2017
Blockchain Unchained: One Lawyer's Quest to Figure out what the Hell Everyone is Talking About
Kendall Harrison

AUGUST 2017
Def Con Hacker Conference: An Accidental Tourists Observations
Elizabeth S. Fitch

MAY 2017
Doe v. Backpage.com and its Aftermath: Continued Uncertainty and New Litigation in the Wake of the Supreme Court's Denial of Certiorari
David Patrón

APRIL 2017
Incorporating Technology into the Management of the Work Processes at the Firm
Donna L. Burden, Elizabeth S. Fitch and Park L. Priest

FEBRUARY 2017
"The First Thing We Do, Let's Kill All The Lawyers"
Elizabeth S. Fitch and Elizabeth Haecker Ryan

DECEMBER 2016
A Primer for Understanding Blockchain
Doug Vaughn and Anna Outzen

AUGUST 2016
The Attorney-Client Relationship in the Electronic Age
Elizabeth S. Fitch and Theodore M. Schaer

MAY 2016
Understanding the Defend Trade Secrets Act of 2016: "We're Not in State Court Anymore"
Peter J. Pizzi and Christopher J. Borchert

DECEMBER 2015
Cyber Armageddon: Survival or Annihilation?
Theodore M. Schaer and Elizabeth S. Fitch