Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Lessons From UK's Data Backlash

By **Kim Roberts**
(October 2, 2018, 12:56 PM EDT)


Kim Roberts

The banking arm of U.K. retailer giant, Tesco Personal Finance PLC, and national air carrier British Airways are the latest British icons to find themselves in legal difficulties regarding data breaches.

The U.K. regulator, the Financial Conduct Authority, fined Tesco Bank 16.4 million pounds on Oct. 1 for "failing to exercise due skill, care and diligence in protecting its personal current account holders against a cyber-attack" in November 2016.

In the case of BA, it revealed a breach of its IT system on Sept. 7, which had exposed the personal information, including credit card details, of 380,000 customers. It swiftly acknowledged the problem — notifying customers that personal and financial details had been affected — and appears to have been proactive in its efforts to rectify the breach and thereby seek to prevent damage to its reputation. Indicators include that it has made contact with affected customers quickly, and offered free credit protection to those affected for a year following the cyber security incident.

So far regulatory recourse against BA has not been made public. However, potential legal action against BA has been initiated by claimant lawyers, with one firm inviting affected individuals to join to a group litigation action and bring a legal challenge against the carrier. One firm claims that it may recover a payment of up to 1,500 pounds from BA for each and every customer affected. If awards at that level were made for every affected customer the total amount of damages that BA would be liable to pay would reach 570 million pounds, recognizing, of course, that this would be an extreme scenario.

Beyond the ICO

Both cases are examples of the breadth of risks arising from data breaches beyond the established route of the Information Commissioner's Office (ICO), the regulator responsible for data privacy and General Data Protection Regulation enforcement in the U.K., handing out fines.

For example, the FCA pursued Tesco Bank under "Principle 2," which requires a firm to conduct its business with due skill, care and diligence. The FCA found that Tesco Bank breached Principle 2 because it failed to exercise due skill, care and diligence to:

- Design and distribute its debit card;

- Configure specific authentication and fraud detection rules;
- Take appropriate action to prevent the foreseeable risk of fraud;
- Respond to the November 2016 cyberattack with sufficient rigor, skill and urgency.

The action from the FCA should be a warning to any organization that falls under the FCA's regulatory framework. Not only will data breaches gain the attention of the ICO, they may well result in a "double-whammy" as the FCA also has the power to enforce against firms by imposing hefty fines.

From Regulation to Litigation

Data breaches, such as the BA and Tesco Bank breaches, have become increasingly common, with many companies becoming aware of incidents where information has been lost, compromised or acquired. In some cases data is acquired by bad actors engaged in criminal acts, and in others data is lost or compromised as a result of human error or system failures. The court of public opinion voices most loudly the growing concerns of consumers about what personal data companies collect and why they do so, how data is stored and why it is retained. Of course, these questions are all relevant when a cybersecurity incident takes place, when the focus turns to why the company had the data which is accessed or acquired in the first place, or why they had kept the data for so long.

The majority of enforcement action for data breaches has been undertaken by the regulators under the old legal regime, before the GDPR became effective in May this year. The highest maximum fine the ICO could issue under the old legislation was 500,000 pounds. In that context the ICO's largest fines have been between 350,000 and 500,000 pounds, although these were meted out quite rarely and fines at this level have only happened in around 10 or so cases.

The extended enforcement powers under the GDPR allow the ICO (and the other EU data privacy regulators) to issue fines of up to 20 million euros (or equivalent in sterling) or 4 percent of the total annual worldwide turnover in the preceding financial year, whichever is higher.

In terms of litigation, there have been only a few proposals or mooted cases against companies from lobbyists. The path is clear for such action, however, following the ruling of an English court last year against the U.K. supermarket giant, Morrisons. In that case, 5,518 former and current staff from Morrisons brought a liability claim against the company following a security incident in which employee information was stolen by an ex-employee. Where there was no obvious route for the claimants to seek financial damages, they claimed for damages as a result of the anxiety and stress they had suffered in connection with the breach.

What makes a difference for BA is that the claimant group which is being assembled following this recent data breach seeks damages under the new GDPR regime. Under Article 82 of the GDPR: "Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered." This leaves the door wide open for claimant firms to seek damages for individuals affected in a multitude of ways by the data loss. How "material and non-material damage" will be defined remains to be seen. However, in the U.S., such damages are already frequently sought in class actions and include compensation for stress or anxiety as a result of losing personal data and time spent rebuilding credit ratings and organizing new accounts, among other heads of loss.

Global Scope

The GDPR bites not only on entities which have operations inside the EU, but also those entities which are based outside of the EU, such as in the U.S., which collect and use the personal data of EU nationals. As such, in a similar scenario to what has happened at BA, a U.S. carrier facing a similar breach could well face claims in the European courts from affected individuals. Remember too, that the GDPR affects businesses in every sector, regardless of the size of the organization. Contrasts can also be drawn between the U.S. and the EU in terms of the legal definitions of concepts such as "personal data" and "data breach," as these have subtle but fundamental differences and challenge the ability of organizations when responding in a crisis situation to the multitude of notification and reporting requirements which may be applicable, dependent on the nature of the incident, who is affected by it and where they live.

Supply and Demand

One of the principal wrongs that the GDPR sought to remediate was the lack of reporting of data breaches, with particular concern over cover-ups, including the criticisms made in the U.K. of large corporations such as Yahoo! and Uber for failing to report data breaches. The new law drives transparency and organizational accountability, fueled by concerns from consumers at large at a time where the media coverage of data breach incidents is running at an all-time high. And organizations appear to be responding — the ICO recently reported that is that it is receiving around 500 calls each week to its data breach hotline since the GDPR became effective.

Clearly, with the ongoing vulnerability of many big businesses in cybersecurity, there remains a threat of legal action following a breach. However so far, group actions and cases of this type are few and far between, so the level of culpability and remedy are largely untested under the GDPR, which brings with it significantly enhanced scope for enforcement.

That said, there is an opportunity for plaintiff firms to exploit. As was seen in the U.S. class action "stock drop" surge in the late 1990s and early 2000s to the lower-end "whiplash" road traffic accident boom and the incessant PPI program, the appetite to bring cases — whether fully justified or spurious — as a tactic to get a quick-fix settlement is high. The central idea behind such actions is, of course, that it is cheaper for a company to settle a claim than fight it through the courts, a pattern which has established itself already state-side.

Company-Led Remedies

No organization wants to fall foul of a data breach. It is important to respond accordingly when faced with one and not descend into a conflict (or perceived conflict) with customers, and to comply with the new legal obligations on companies to make necessary notifications. In that regard, the new regime is much stricter, allowing only 72 hours from becoming aware of a security incident to make a report to the regulator.

Measured and personalized communications in response to a data breach are a good start, as is a thorough review of the breach and the potential exposure. Innovation around addressing customer concerns around how to repair damaged credit ratings is also welcomed by consumers. The full scope of what is at stake for companies affected by data breaches is, as yet, difficult to gauge: depending on the type of business concerned, with potentially multiple regulators involved and not least with the GDPR's

vague criteria about what damages might entail. However, having a strong company-led response must be the starting point to set the appropriate tone.

Kim Roberts is counsel at King & Spalding LLP.