BCLP. Client Intelligent

Insights

COLLECTIVE REDRESS SCHEMES CAN MANAGE DATA BREACH SUITS

Mar 17, 2020

Recent court decisions, both in the U.K. and abroad, have potentially increased the exposure of firms to group litigation in relation to data security events. An intensified consumer litigation risk, coupled with greater regulatory scrutiny on data security, may cause firms to reassess the way in which they respond to security incidents. In this environment, a voluntary collective redress scheme may now be one of the most attractive ways to manage a firm's exposure.

The Decisions

The courts have recently held that every individual whose data is compromised in principle suffers the same minimum level of harm, i.e., a "loss of control" of their data (without proving any pecuniary loss/distress). This has led the Court of Appeal recently to determine that every data subject whose data is compromised would have the same interest in a class action, a key requirement for bringing a representative action in this jurisdiction pursuant to Civil Procedure Rules Part 19.

This type of opt-out group action has historically been limited, but where it is permitted, it can expose firms to very significant damages awards, and currently the odds seem to be stacked in favor of the consumer claimants.

Given firms may also face regulatory penalties for the same incident, it must be in their interest to manage the significant litigation risk, as well as to present themselves in the best possible light to the regulator.

Learning From Other Schemes

Voluntary redress schemes are widely used in the financial services industry by the firms who want to establish their own private, standardized scheme to compensate consumers and settle any legal claims outside the court process.

Such schemes have been used to compensate a particular class of individuals from inappropriate conduct committed by entities in well-publicized events, such as the missale of interest rate hedging products, or IRHP, and payment protection insurance, or PPI. The PPI scheme, widely thought to be the largest redress exercise in the U.K., was praised by the FCA as vital to rebuilding the public's confidence and illustrated a proactive approach taken by firms to address consumer detriment.[1]

There is scope for public relations benefits if a firm is being proactive and decisive in offering redress to its data subjects through a structured scheme. Following a high-profile security incident, recovery of reputation may be as important to a company and its investors as recovery of its cybersecurity.

Take-up of some redress schemes in the financial services industry has been high. For example, 95% of policyholders accepted redress offers in the 2012 IRHP scheme.[2] Every individual agreeing to settle directly through a voluntary scheme is one less individual to enter or encourage a collective litigation action, mitigating the litigation risk faced by the organization and reducing the appeal to a claimant law firm and funder contemplating building and financing a collective action.

Characteristics of a Workable Scheme

There is no regulator-recommended scheme in the U.K. for data security incidents, so decisions on structure and implementation remain largely with firms. They will need to design a scheme in a way which is commercially viable for them, but fair and accessible for affected data subjects.

The competition sector offers a good example to learn from: the Competition Act 1998 (Redress Scheme) Regulations 2015[3] empower the Competition and Markets Authority to approve redress schemes, which are described as an invaluable mechanism for infringing companies to avoid follow-on damages claims.

The CMA's guidance[4] for such schemes prompts organizations to consider numerous aspects such as how they will ask consumers to provide evidence of loss and entitlement to compensation, what the application process would be, and how affected consumers would be notified of entitlements.

The guidance is a useful starting point for companies faced with data infringements, but will warrant further considerations such as:

- What type of data incident/loss of control will merit a compensation scheme (especially in a legal environment which allows claims for compensation even where there is no financial loss)?
- How to fund, calculate, quantify and pay compensation (in a private scheme this will be in the organization's discretion);
- Duration of the scheme (the CMA requires schemes to operate for a minimum of 9 months, a period substantially shorter than a protracted piece of High Court litigation or even the usual limitation period to bring a legal claim); and
- How will the organization deal with outstanding claimants whose claims have not been settled?

Notably, firms may already have a legal requirement under the General Data Protection Regulation to make data subjects aware of a data incident or breach. Notice of the redress scheme could be incorporated into the general notification process, providing consumers as soon as practicable with clarity about an avenue for redress instead of leaving them anxious about data security and vulnerable to joining a collective litigation action.

Regulatory Benefits

Redress schemes could also be instrumental in demonstrating a proactive approach to data protection regulators. Although designing a scheme during an investigation may appear as an admission of liability, there is potential for a reduction in fines or sanctions in recognition for providing redress.

The CMA guidance[5] is prescriptive: the authority expects that most cases will result in a reduced penalty, up to a maximum of 20% where a scheme has been approved at the same time as the infringement decision.

While less explicit, the Information Commissioner's Office's regulatory action policy could be interpreted in a similar way. It makes clear that measures taken to mitigate the risk of harm will be a factor in determining whether to pursue an investigation and, where it does take enforcement action, the action taken to mitigate harm will be a factor in determining the appropriate sanction. This is a substantial benefit for organizations and demonstrates that regulators are attracted to this form of voluntary compensation.

A regulator-endorsed scheme may also be a barrier to a representative or collective action proceeding in the courts. In the competition sphere, a CMA-approved scheme may, if accepted by the tribunal as an appropriate form of alternative dispute resolution, be taken into account when the tribunal makes costs orders against parties. The court, faced with a potential collective action against a data controller which has proactively set up a redress scheme, may respond in a similar way.

Moreover, there may be an argument that the existence of a regulator-approved scheme which will offer affected individuals financial redress (plus potentially other benefits such as credit monitoring services), should be taken into account when the court exercises its discretion under CPR Part 19 to decide whether a representative action may continue at all.

The Future of Voluntary Redress

While not provided for under GDPR, there is an increasing trend towards voluntary redress schemes within the U.K. which is likely to extend into the data protection arena. Firms would be well placed to consider the merits of redress schemes to retain control and discourage expensive collective litigation following a security incident. The commercial (and possible financial) imperatives of the schemes are likely to attract organizations and regulators going forward.

The authors would like to thank trainee solicitor Eleanor Durcan for her contribution to this article.

First published in Law360 on 6 March 2020.

Endnotes

[1] https://www.fca.org.uk/publication/policy/ps17-03.pdf

[2] https://www.fca.org.uk/consumers/interest-rate-hedging-products

[3] SI 2015/1587

[4] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/453925/Voluntary_redress_schemes_guidance.pdf

[5] Ibid

MEET THE TEAM

Oran Gelb

London

oran.gelb@bclplaw.com
+44 (0) 20 3400 4168