

Data Breach Litigation



The Curve

There is a marked increase in the volume of data breach claims being pursued by both individual claimants and via proposed group/class actions.

This is likely to be partially related to a number of high profile group actions involving well-known brands/organisations combined with the proactive recruitment of claimants by claims management firms.

In many instances the amount claimed is small and the legal basis of the claim is debatable. However, irrespective of the legitimacy/value of the claim, organisations may be tempted to agree a settlement payment because they consider that it is not cost effective to litigate.

The Trajectory

The claims follow an all too familiar trajectory. An organisation suffers a data breach relating to the personal data of its clients/customers/employees. Consumer-focused claims management firms then seek to sign up affected customers, draft pre-action correspondence (often by way of use of template documents) with a view to either putting pressure on organisations to settle or by way of issuing multiple claims for damages for breach of UK data protection legislation, breach of confidence, misuse of private information and negligence (usually backed by conditional fee agreements and After the Event (ATE) insurance).

In view of the current lack of clear authority regarding quantum and given the cost exposure that can result from associated ATE premiums in these type of proceedings, claims management firms have created a model, which is geared at achieving a payment in settlement.

The Answer

Our team of commercial dispute resolution lawyers are expert in handling all manner of disputes and are highly experienced in resolving and robustly defending claims of this nature. This expertise, when combined with our specialist regulatory and compliance team's understanding of the related regulatory matrix ensures that an informed and robust strategy can be adopted (with a view to preventing a "flood gate" scenario), whilst also taking any relevant commercial/common sense considerations into account.

The Proactive Steps You Should Take Now

- 1 Health Check:** We regularly carry out health check reviews of existing policies, procedures and training with a view to “future proofing” against claims of this nature.
- 2 Act Fast and Mitigate:** Ensure internal protocols and policies are implemented, monitored and followed. Where a breach has or is likely to arise, investigate quickly (maintaining records of any such investigation). Report breaches (or potential breaches) to your data protection team and involve specialist advisers as soon as possible, not least because a report may need to be made to the ICO. Taking quick action is not only a regulatory obligation but may prevent further loss and damage.
- 3 Guidance:** Our knowledge of the market, rapidly developing case law and regulatory matrix means we:
 - ⇒ will guide you through the process and relevant pre-action stages (as required under the Civil Procedure Rules);
 - ⇒ have processes in place to manage claims and conduct reviews in a cost-effective and timely manner;
 - ⇒ can make an informed decision as to the risks and advise upon the options available to you;
 - ⇒ robustly defend claims/ensure an appropriate resolution is achieved.

Please contact one of the team below for advice or assistance.



Gwendoline Davies, Partner
Commercial Dispute Resolution

0113 283 2517 / 0776 469 2321
gwendoline.davies@walkermorris.co.uk



Claire Acklam, Director
Commercial Dispute Resolution

0113 399 1883 / 0782 728 3243
claire.acklam@walkermorris.co.uk



Nick McQueen, Partner
Commercial Dispute Resolution

0113 283 4426 / 0739 213 0513
nick.mcqueen@walkermorris.co.uk



Rebecca Jackson, Senior Associate
Commercial Dispute Resolution

0113 399 1897 / 0778 783 2973
rebecca.jackson@walkermorris.co.uk