ICO Processor fine – the ICO's approach to assessing technical standards and its impact

20 August 2024

The ICO recently confirmed its provisional decision to fine Advanced Computer Software Group £6.09 million following a data breach that it suffered in 2022.

None of the immediate headlines are necessarily surprising: (i) organisations should ensure that all web facing access is protected by MFA, and (ii) the ICO will turn its sights on data processors where they are the clear point of failure for a data controller's breach. But, like the enforcement notice against the Electoral Commission in July, the decision against Advanced centres on technical failures (rather than process-based failures such as obtaining appropriate consent or data retention). It's worth pausing to consider how the ICO goes about assessing technical standards and what implications these decisions might have on the data subject litigation landscape.

Appropriate technical and organisational measures. What's required and who decides? The ICO's provisional decision criticises the lack of MFA on the customer account that was ultimately used to perpetrate the ransomware attack against Advanced. Given that MFA is seen as a common protective requirement, there may not be many questions in this particular instance over how the ICO formed its view on the adequacy of Advanced's security posture. However, this becomes more of an issue where the attack vector is more complex or nuanced. The enforcement decision against the Electoral Commission leaned heavily on patching and password guidance from the NCIS and NIST. However, technical measures are not a one size fits all, and both decisions prompt an interesting point over whether the ICO considers itself the sole arbiter of what passes muster when it comes to technical standards, particularly in more complex cases. Over the last few years, the ICO has made a point of developing and augmenting its own internal technical capabilities. Nonetheless, most other forums that determine legal liability (Civil Courts, Arbitration, Adjudication) would usually rely on evidence from experts in the relevant fields when reaching findings on highly technical matters.

Data subject litigation: After a period of oscillation, the data subject litigation landscape has reached a relatively settled state for the time being. Authorities such as *Lloyd v Google [2021] UKSC 50* and *Warren v DSG Retail [2021] EWHC 2168* made it clear that the occurrence of a cyber related data breach is not enough to form an actionable claim under Article 82 of the UK GDPR. Data subjects will, amongst other things, need to prove that the cyber event occurred as a direct result of the controller / processor failing to implement appropriate technical and organisational security measures. That's an inherently difficult task without firstly (i) developing a detailed factual knowledge of the incident, and (ii) obtaining early expert input to assess the adequacy of the measures in place. For prospective data subject claimants (and their

lawyers) this means front loading costs and, to some degree, taking a leap of faith – none of which are conducive to the perceived economics of pursuing data subject litigation, which rely on a critical mass of similarly affected individuals, litigation funding and low costs per head given the likely modest awards. We have seen prospective claimants attempt to circumvent these difficulties through threatening pre-action disclosure applications. However, the typical circumstances in which these are threatened are unlikely to meet the stringent criteria for pre-action disclosure.

Against this background, explicit findings from the ICO in relation to technological failures might be enough to prompt potential claims activity.

Who's the target? Data subjects have a direct right of action against processors and controllers. Nonetheless, data controllers are ultimately responsible for the failures of their processors. The fact that the ICO took enforcement action against Advanced as data processor suggests that there was no real direct fault on the part of the NHS as data controller. Even so, the NHS might be seen by potential claimants as a softer target, particularly from a financial viability perspective. Controllers might then look to recover any losses from their processors.

On this, many Managed Service Providers will usually include in their terms and conditions a liability cap limited to the amount of fees paid over a certain period of time. The costs associated with a data breach (including response costs, regulatory action and resulting claims) can significantly exceed these caps. This is why more and more customers seek to negotiate a 'super cap' for the type of damages that result from data breaches.