First the hack, then the claim: preparing for the data protection class action

Simon Ridding, Barrister
33 Bedford Row

Simon Ridding, Barrister at 33 Bedford Row Chambers, spent his early career as a solicitor conducting data protection group actions for claimants against some of the country's largest data controllers and now acts as junior counsel in several ongoing data protection class actions. Here, he crosses the aisle, distilling that experience into practical guidance for organisations and their Data Protection Officers, who may one day receive the dreaded letter before action.

A significant personal data breach can become two events. The first is the incident itself - the ransomware deployment, credential-stuffing attack or misdirected spreadsheet - and it is usually over within hours or days. The second begins if claimant law firms arrive and can continue for years. For some organisations, the litigation that follows may ultimately prove more expensive and reputationally corrosive than the initial incident.

The term 'class action' is used here as commercial shorthand for several legally distinct mechanisms: representative proceedings under Civil Procedure Rule ('CPR') 19.8, a group litigation order ('GLO') made under CPR 19.22, and multi-party claims managed through lead cases and stays. The crux of this article is that litigation resilience is partly a product of system design: the architecture shapes the potential cohort, the logs help to establish whether fear is well founded, the first notification supplies the language of the pleading, and pre-breach classification may determine what can later be protected during disclosure.

The figures merit attention. IBM's Cost of a Data Breach Report 2025 puts average UK breach costs at £3.78 million for organisations not making extensive use of AI and automation, compared with £3.11 million for extensive users, with financial services costliest at £5.74 million. The Cyber Monitoring Centre treated the 2025 attacks on Marks & Spencer and the Co-op as a single combined event, estimating losses at £270 million to £440 million, and a proposed group claim arising from the M&S incident was announced within weeks. The Information Commissioner's Office ('ICO') has meanwhile rediscovered its appetite for enforcement, fining Capita £14 million, Advanced Computer Software £3.07 million and 23andMe £2.31 million in 2025 alone. Add rising cyber-insurance premiums and eroded customer trust, and the case for treating litigation risk as a board-level concern makes itself.

The procedural landscape: the declining attraction of the GLO

To understand how these claims are now fought, one must first understand how the procedural landscape has changed. *Lloyd v Google LLC* [2021] UKSC 50 closed off the recovery of uniform damages through opt-out representative proceedings without individual proof of damage, stripping that model of much of its economic attraction and leaving claimant firms reliant on opt-in mechanisms. The GLO remains available, but its practical appeal appears to be declining. In *Beck v Police Federation of England and Wales* [2023] EWHC 685 (KB), the claimants abandoned their GLO application after the parties agreed to the defendant's preferred lead claimant model, under which test claimants proceed on the common issues while the remaining claims are stayed. Senior Master Fontaine accepted that the threshold for a GLO was met but penalised the claimants in costs for failing to engage earlier with the more proportionate alternative. The decision does not render the GLO obsolete, but it demonstrates why defendants should propose a lead claimant model early and firmly where it offers a more proportionate means of resolving the common issues.

The substantive law has moved the other way and in *Farley v Paymaster (1836) Ltd (t/a Equiniti)* [2024] EWHC 383 (KB), Nicklin J struck out over 400 claims by police officers whose pension statements were posted to old addresses, absent proof the envelopes were opened. The Court of Appeal ([2025] EWCA Civ 1117) reversed

that decision, holding that third-party disclosure is not an essential ingredient of an infringement claim and that no threshold of seriousness applies to non-material damage. Damage must nevertheless be proved: a claimant relying on fear of future misuse must show that the fear was objectively well founded in his or her circumstances. Paymaster's appeal on the compensation issue is listed to be heard by the Supreme Court on 7th and 8th October 2026. Master Dagnall's refusal to strike out nearly 4,000 templated claims in *Spurgeon v Capita plc* [2026] EWHC 241 (KB), while requiring the parties to address and reformulate exaggerated generic language, completes the picture: mass claims survive, but they must remain grounded in individual instructions.

Before the breach: architecture as advocacy

The most effective defence work is done years before any breach. Data minimisation is also cohort minimisation: deleting personal data that are no longer required can reduce both the scale of a future incident and the number of potential claimants. Retention schedules should therefore operate as practical controls rather than remain filed as compliance artefacts. Databases should likewise be segmented so that a single compromised credential cannot expose the entire customer estate, since the reach of the intrusion will help to define the size of any subsequent claim.

Minimisation should not, however, become indiscriminate deletion. Records demonstrating consent, security decisions and remedial action may form an important part of the organisation's defence. The objective is therefore to delete redundant personal data while preserving, where necessary and legally justified, the evidence needed to explain and justify what was done.

Terms and conditions also deserve attention. They cannot restrict data subjects' statutory rights or impose inappropriate barriers to redress, but they can signpost a clear complaints channel, provide for appropriate alternative dispute resolution and remind customers to keep their contact details current. *Farley* nevertheless shows that collecting an updated address is not enough: the controller's systems must actually use it.

The received wisdom that instructing forensic investigators through external lawyers will secure privilege deserves scrutiny. The author is not aware of any reported English decision ordering production of a defendant's breach investigation report, and in his claimant-side experience such reports were consistently withheld. That experience should not, however, be mistaken for a guarantee. Litigation privilege generally requires litigation to be reasonably contemplated and the relevant communication or document to have been created for the dominant purpose of obtaining advice or evidence for that litigation. A sensible peacetime protocol should therefore distinguish the operational investigation from any separate workstream commissioned by lawyers for contemplated proceedings, restrict the circulation of candid legal analysis, and record clearly why each workstream and document was created.

The first 72 hours: notification as pleading

Once a breach occurs, two obligations must be kept distinct. Article 33 of the UK GDPR requires notification to the ICO without undue delay and, where feasible, within 72 hours of awareness, unless the breach is unlikely to result in a risk to individuals' rights and freedoms. Article 34 requires affected individuals to be informed without undue delay where the breach is likely to result in a high risk. That communication is likely to become a central exhibit in any subsequent claim. It should therefore be accurate, specific about the data affected, and free from both speculation and minimisation. Overstatement may help to establish that a claimant's fear was well founded; understatement may create a damaging narrative of concealment.

The organisation's initial breach communications also establish the vocabulary of the case. 'Accessed', 'exposed', 'exfiltrated' and 'compromised' are not synonyms, and careless movement between them can turn uncertainty into an apparent admission. Remediation should be proportionate to the threat and its purpose explained accurately. The ICO notification, communications with affected individuals and public statements should also remain consistent, as claimant firms will compare them closely. Above all, preserve the logs that establish what was - and was not - accessed or exfiltrated. After *Farley*, that evidence may determine whether a claimant's fear is objectively well founded or merely speculative.

Parallel tracks: the regulator and the claimant firm

ICO scrutiny and claimant activity will run in parallel, and each should be managed with an eye on the other. Representations to the ICO must be candid and accurate, but candour does not require advocacy against oneself. The controller should answer the regulator's questions fully, distinguish established facts from provisional hypotheses, and avoid converting an incomplete technical investigation into an unnecessary legal admission. Those representations may also become a rehearsal of the subsequent defence. An ICO penalty may provide claimant firms with a ready-made narrative of fault, although a regulatory finding does not of itself establish infringement, causation or damage in civil proceedings.

The most effective defence work is done years before any breach

Claimant firms create value by aggregation; defendants recover leverage by identifying the differences that prevent the cohort from being valued as a single block. A lead claimant model can limit the expense of cohort administration, while early challenges may narrow the claimant population. Allocation of low-value claims to the small claims track, contemplated in *Farley*, may also alter the economics because recoverable costs are tightly restricted under CPR Rule 27.14.

Settlement analysis should be evidence-led. Claims can be grouped according to factors that matter in law, including the sensitivity of the data, evidence of access or misuse, remediation, individual vulnerability and proven damage. The defendant should also examine the claimant firm's funding arrangements, cost exposure and incentives rather than make assumptions based on its size. A Part 36 strategy need not involve a single figure: offers sequenced by evidential band can force the claimant firm to confront the differences within a cohort pleaded as homogeneous.

Disclosure: the price of knowing your own systems

No stage frightens defendants more than disclosure, and with good reason. It is the point at which the dispute ceases to be an argument about pleadings and becomes an excavation of the defendant's systems: server logs, security alerts, penetration-test results, patching histories, board papers and internal discussions of what went wrong. The courts will require disclosure to remain reasonable and proportionate, but that cannot remove the core expense of identifying, reviewing and explaining a complex corporate record.

Settlement pressure therefore tends to peak immediately before disclosure, when much of that expense can still be avoided, and again after disclosure, when both parties have seen what the documents reveal. An organisation with segmented systems, disciplined record-keeping and reliable logs approaches both moments on better terms. Those controls reduce the cost of reconstructing the incident and allow the defendant to distinguish evidence of actual compromise from speculation.

The second audience: confidentiality rings and the crown jewels

Disclosure carries a further danger. Network diagrams, security configurations and proprietary detection logic are sensitive twice over: valuable to competitors, and a map for the next attacker, so an organisation that litigates carelessly risks making the courtroom the site of its second breach. CPR Rule 31.22 restrains collateral use of disclosed documents but cannot neutralise the irreversible risk of security material reaching a competitor or a public hearing. The stronger answer is the confidentiality ring, although *OnePlus Technology (Shenzhen) Co Ltd v Mitsubishi Electric Corporation* [2020] EWCA Civ 1562 confirms that external eyes-only restrictions are exceptional and must be justified by the party seeking them, as Roth J likewise emphasised in *Infederation Ltd v Google LLC* [2020] EWHC 657 (Ch). A ring is therefore won on evidence of sensitivity, and generic assertions fail. A company that classifies its security documentation in peacetime, restricts access and records why disclosure would cause harm arrives at the first case management conference better able to justify protection document by document. Such measures may also help to demonstrate that reasonable steps have been taken to keep the information secret, as required by Regulation 2 of the Trade Secrets (Enforcement, etc.) Regulations 2018.

Conclusions for the DPO

The organisation that fares best is the one that has rehearsed the claim rather than merely the breach. The programme is short: minimise and segment the data estate; review notification templates through a litigation lens; agree incident-response and privilege protocols in advance; classify the crown jewels so that a confidentiality ring can be justified from the first hearing; preserve the logs that prove the negative; and coordinate the regulatory and litigation positions.

These claims are rarely defeated by a single doctrinal answer. They are defended by shrinking the affected population, preserving the evidence that tests the individual claim, and proposing a proportionate procedural structure at the earliest opportunity. Data protection class actions will be defended well or defended expensively, and the choice between the two is largely made before the breach ever happens.

Simon Ridding
33 Bedford Row
sr@33br.co.uk