Neutral Citation Number: [2025] EWCA Civ 1117

Case No: CA-2024-000578

IN THE COURT OF APPEAL (CIVIL DIVISION)
ON APPEAL FROM THE HIGH COURT OF JUSTICE
KING'S BENCH DIVISION
MEDIA AND COMMUNICATIONS LIST
MR JUSTICE NICKLIN
[2024] EWHC 383 (KB)

Royal Courts of Justice
Strand, London, WC2A 2LL

Date: 22/08/2025

Before:

LADY JUSTICE KING
LORD JUSTICE WARBY
and
LADY JUSTICE WHIPPLE

- -

Between:

(1) Michael Farley **(2) – (431) Individuals identified in Annex 1 to the Claim Form**	**Appellants/ Claimants**
- and -	
Paymaster (1836) Limited (trading as Equiniti)	**Respondent /Defendant**
- and -	
The Information Commissioner	**Intervener**

- -
- -

Oliver Campbell KC and Pepin Aslett (instructed by **KP Law Limited**) for the **Appellants**
Andrew Sharland KC and Hannah Ready (instructed by **Freeths LLP**) for the **Respondent**
Christopher Knight (instructed by **the Information Commissioner**) for the **Intervener**

Hearing dates: 17 and 18 June 2025

- -

Approved Judgment

This judgment was handed down remotely at 10am on 22 August 2025 by circulation to the parties or their representatives by e-mail and by release to the National Archives.

LORD JUSTICE WARBY:

Introduction and summary

1. This is an appeal from an order striking out most of the individual claims in a collective action arising from a data breach. It raises issues about the interpretation and application of the General Data Protection Regulation ("GDPR") and the Data Protection Act 2018 ("DPA").

2. The appellants are 432 members of a pension scheme administered by the respondent. Their annual benefit statements ("ABS") were mistakenly posted to addresses that were wrong because they were out of date. The appellants alleged that this was a misuse of their personal information and an infringement of the GDPR. They and others brought this action seeking compensation for injury to feelings, and in some cases psychiatric injury, suffered due to fear of third-party misuse of their personal data. Fourteen of the claimants could show an arguable case that the mis-addressed envelope had been opened and their ABS had been read. But the High Court held that none of the appellants had any tenable case that this had happened to them. For that reason, whilst allowing the 14 claims to go forward the court struck out the appellants' statements of case as disclosing no reasonable basis for a claim. They now appeal against the dismissal of the data protection claims.

3. The appellants do not challenge the judge's conclusion that they cannot show that their ABS came to anyone's attention. They contend however that the judge was wrong to regard disclosure as an essential ingredient of a viable data protection claim. They say they have a tenable case that the mistake involved infringement of their data protection rights.

4. The respondent does not defend the judge's finding or reasoning on the issue of infringement but invites us to uphold the judge's decision to dismiss the claims on the basis that the claims for compensation are factually incredible, insufficient or untenable as a matter of law, or so trivial that they should be dismissed as an abuse of process of the kind identified in *Jameel v Dow Jones Inc* [2005] EWCA Civ 75, [2005] QB 946. These are all points which the respondent took before the court of first instance, but on which the judge did not rely. As the appellants have pointed out, the respondent needs the court's permission to argue some of them in this court. The respondent has also modified its arguments to some extent. I would however grant the necessary permission, and I understand the other members of the court agree.

5. The main issues can therefore be summarised as follows: (1) have the appellants set out a reasonable basis for claiming that the respondent's mistake involved infringement of the GDPR ("the infringement issue"); if so, (2) have the appellants stated a basis for claiming compensation under the GDPR and DPA that is reasonable, with a realistic prospect of success at a trial ("the compensation issue"); and if so (3) are the claims nonetheless an abuse of process of the *Jameel* variety ("the *Jameel* issue")?

6. We have read and heard argument on those issues on behalf of the appellants, the respondent, and the Information Commissioner, who intervened at the prompting of the court. Having reflected on the helpful submissions of Counsel, and for the reasons given below, I have reached the following conclusions.

(1) The judge was wrong to strike out the data protection claims for the reason he gave. Each of the appellants has pleaded a reasonable basis for alleging that the respondent's mistake involved infringement of the GDPR. Proof that the data were disclosed is not an essential ingredient of an allegation of processing or infringement. The appeal on the infringement issue should therefore be allowed.

(2) As to the compensation issue:-

(a) The respondent is not entitled to judgment on the grounds that the appellants' factual allegations are simply incredible. An allegation of "distress" is not, as the respondent has submitted, an essential ingredient of a tenable claim. Nor can the claims be dismissed for failing to meet a threshold of seriousness. There is no such threshold in EU data protection law. We are not bound to hold that such a threshold exists in domestic data protection law. Nor is there any other good reason to do so. The judge's decision cannot be upheld on any of these grounds. To this extent the cross-appeal should be dismissed.

(b) The respondent is however entitled to contend that the appellants' fears of third-party misuse were not "well-founded" and hence cannot qualify as "non-material damage" for which compensation is recoverable under the GDPR. The question of whether a claim based on the fears alleged could prevail can be determined at this stage. The fate of the claims for consequent psychiatric injury appears to turn on the outcome of that issue. There are no other properly pleaded compensation claims. So the answer to this question could be decisive for at least some of the claims. But the question must be answered case by case. This is not the appropriate court to carry out that exercise. Other things being equal, the case should be remitted to the High Court which may conduct the review itself or give directions for it to be carried out in the County Court.

(3) The *Jameel* jurisdiction does not provide a reason to bypass that process. These claims as a class cannot be categorised as *Jameel* abuse although the question of whether any individual case is abusive will remain for consideration.

The background in more detail

The data breach

7. In late August 2019 the respondent, acting as administrator for the pension scheme covering the Sussex Police, sent ABS by post to members of the scheme. The ABS took the form of a letter headed "Private and Confidential", with the scheme member's name, and the postal address ("the Header"). Under the subject line "Sussex Police Pension Annual Benefit Statement" the body of the letter set out further personal information including the date of birth, and national insurance number of the scheme member, and pension-related details including their police service, salary details, and

their accrued and forecast pension benefits. The ABS were sent in window envelopes. Through the window could be seen the Header. On the outside of the envelope was a return address.

8. A substantial number of these ABS, in excess of 750, were posted to out-of-date residential addresses. The evidence is that Sussex Police had provided the respondent with up-to-date addresses which were uploaded to the respondent's database but when the ABS were produced the system "picked up a previous address" in error.

9. By 24 September 2019 the mistake had come to light. A substantial number of ABS had been returned to the respondent unopened. Some officers had reported not receiving theirs. In early October, Sussex Police sent a notification letter to each affected officer. This informed the officer whether or not the ABS had been returned to Equiniti or Sussex Police. It reported that "the risk of harm arising from this breach is assessed as low", but gave advice on protective steps. Officers were offered the opportunity to sign up to a fraud protection service called CIFAS at the respondent's expense. The evidence is that 37 officers did so. The letter advised recipients that Sussex Police had notified the Information Commissioner's Office ("ICO"). At about the same time the respondent sent out letters of apology with replacement ABS.

10. On 17 October 2019, the ICO wrote to Sussex Police. It noted that "the breach was caused by" the respondent, described as Sussex Police's "data processor". The respondent had been notified of changes of address but had "failed to effectively update their systems". The ICO further noted that Sussex Police had conducted a risk assessment that concluded that the risk of data subjects suffering significant consequences was "unlikely", that advice on identity theft was to be given to the affected data subjects and concluded that no further action was required.

11. Some 102 ABS were returned to the respondent unopened. It seems some may have been forwarded unopened to the scheme member. Around 60 officers were able to retrieve the ABS themselves. The majority of ABS were never recovered and it remains unknown what happened to them.

The claims

12. A substantial cohort of affected officers instructed solicitors who wrote a letter of claim. The respondent admitted that there had been a data breach and that the officers were "entitled to pursue the [respondent] for loss, damage and/or distress allowable at law". The officers' solicitors provided a schedule of damages claimed by those who did not claim to have suffered personal injury, seeking £2,000 each for misuse of private information and figures between £1,064.80 and £2,606.30 for infringement of their data protection rights. By the time of the hearing below the figure had been revised downwards to £1,250 per claimant for both heads of claim.

13. On 22 April 2021, a claim form was issued on behalf of 474 current or former officers, seeking damages for breach of statutory duty under the UK GDPR and the DPA and/or misuse of private information "arising from the [respondent's] failure to keep the claimants' personal data and private information secure by posting the same to incorrect postal addresses." The claim form was accompanied by Master Particulars of Claim setting out the "common or generic claims" of the claimants, with "Heads of Damage" and other details relating to individual claimants to follow.

14. The generic data protection claims asserted that the respondent had acted in breach of its statutory duties as a data controller or alternatively as a data processor. There is a live dispute as to which role the respondent played. But it is common ground that on this appeal we are concerned only with the allegations of breach of duty as a data controller. These fell into four main categories: (1) breaches in August 2018 when the respondent was provided with the claimants' "Original Residential Addresses" and entered these in its system; (2) breaches in August 2019 when, having been supplied with the updated address details, the respondent put these into its system; (3) breaches in August 2019, when it posted the ABS to the Original Residential Address; and (4) generally, failure to implement appropriate technical and organisational measures, (contrary to Articles 24, 25 and 32 of the GDPR).

15. Three generic allegations of damage due to the data protection breach were pleaded. First, each claimant complained of being caused "anxiety, alarm, distress and embarrassment" by "the fact that the Personal Data has passed and/or may have passed into the hands of unknown third parties" which was said to merit "compensation for moral and/or non-material damage". In this regard, the court was invited to infer that the envelope had been opened and its contents read unless the respondent could prove the contrary by providing an ABS that had been returned unopened. Secondly, each claimant advanced a discrete claim for compensation for "loss of control" over the content of the ABS and consequential distress. Thirdly, it was said that "certain of the claimants have suffered an aggravation of pre-existing medical conditions."

16. On 27 April 2022, the court made an order pursuant to CPR 18.1(1)(b) for the claimants to provide further information by way of claimant-specific statements of case. These took the form of individual schedules verified by statements of truth. Features of significance for present purposes are these:

    (1) Each claimant was ordered to state whether they had "suffered any annoyance and/or distress and/or anxiety". Some of the schedules responded by using the word "distress" or the word "anxiety" or both. Other individual schedules did not use the word "distress". Some 34 said in one way or another that the claimant had not suffered "distress". Different forms of words were used to describe the officer's emotional response to the breach, including "stress", "annoyance" and "irritation". Some schedules used qualifying adjectives, characterising their reactions as "mild", "minor", or "temporary".

    (2) Some of the schedules gave explanatory or supporting details. For instance, the first claimant's schedule explained that he had been distressed about "the potential consequences of the information falling into the hands of someone on the other side of the law". Although he considered the risks to be "remote" he suggested they were "live and real". He also said he suffered anxiety over the potential for other misuse of the data, such as its use to open bank accounts, or apply for credit cards in his name. Concern at what might happen if information was accessed by criminals was a common theme. So was concern at the prospect of identity theft. Other worries were identified. Another claimant (no 45) was also "concerned" because the Original Residential Address was owned by the parents of his ex-partner, with whom he had experienced "significant issues" particularly around financial matters. He was fearful of what his ex-partner might do with details of his income and other personal information.

(3) Required to state whether they had "a medical condition caused (or exacerbated) by the misaddressed ABS" a substantial number of the claimants asserted that they did. Among those are 42 of the appellants, each of whom has served a medical report in support of that assertion. We have not been provided with all of these but have been shown three exemplars, each of which contains details of the kinds of distress or concern or other emotional reaction reported by the particular appellant.

17. The respondent's Defence admitted that it processed the Personal Data by recording, organising, structuring and storing it, and by altering it in the course of uploading the revised address data. The respondent did not dispute that the mere posting of the ABS involved processing of the Personal Data. The respondent's case as to infringement was that it undertook these activities as a data processor only, and in any event it denied acting in breach of any of the duties alleged. The respondent denied the pleaded case as to damage and distress and, in the alternative, pleaded that the action failed to overcome the applicable thresholds of seriousness and/or was an abuse of process under the *Jameel* principle. In support of this plea it was asserted, among other things, that the claimants' case that the ABS had been opened and read was purely inferential and rested in part on "an entirely unreasonable inference" that this had occurred.

The respondent's application

18. On 17 October 2022, the respondent filed an application notice seeking an order striking out all the claims in their entirety pursuant to CPR r 3.4(2)(a) and (b) and/or summary judgment entered in its favour pursuant to CPR r 24.2(a)(i) and (b). The application in respect of the data protection claims was made on four grounds:

> "(a) damages cannot be awarded for 'loss of control' of data without proof that it caused material damage or distress; (b) the claimant has not suffered damage or distress above a de minimis level or such as to cross the applicable threshold of seriousness; (c) The claim constitutes an abuse of the court's process pursuant to the principles established in *Jameel v Dow Jones* ...; and (d) with regard to certain claimants identified in the accompanying witness statement ..... no case of actionable damage having been suffered is advanced in the particulars of damage ..."

19. Ground (a) was based on the Supreme Court's November 2021 decision in *Lloyd v Google LLC* [2021] UKSC 50, [2022] AC 1217 which held that pure "loss of control" damages are not available in a claim under the Data Protection Act 1998. By the time the application came on for hearing by Nicklin J on 27 February 2023, this point had been conceded and that part of the claim for damages had been abandoned. Grounds (b) to (d) remained alive, and were argued over two days of hearing in February 2023 and via further written submissions in May and June 2023.

The judgment

20. By his reserved judgment and order dated 23 February 2024 the judge struck out all but 14 of the claims pursuant to CPR r 3.4(2)(a). He did so on the grounds identified in the following passages of the judgment.

> "143. In my judgment, to have a viable claim for misuse of private information and/or data protection, each Claimant must show that s/he has a real prospect of demonstrating that the ABS was opened and read by a third party. Without that, the relevant Claimant would have no real prospect of demonstrating that there had been "*misuse*", an essential element of the tort of misuse of private information. ...
>
> 144. For the purposes of clearly isolating the principle, it is helpful to consider the cases of the cohort of Claimants who ultimately did receive their ABS unopened. For those Claimants, an inferential case that the ABS was opened (and read) by a third party cannot be sustained. On the contrary, there is positive evidence that the ABS had not been opened (or read) by anyone else. Can these Claimants nevertheless bring a claim for misuse of private information and/or data protection in respect of the period before the ABS was returned? In my judgment, the answer is no.
>
> 145. I reject the submission that these Claimants can advance a claim on the basis that, until returned, their personal information/data was "*in danger*" or "*at risk*". The general law of tort does not generally allow recovery for the apprehension that a tort might have been committed; a person crossing a road cannot recover damages (whether for distress or otherwise) for almost being struck by a passing lorry or for a defamatory letter that was never actually received by its intended recipient. To be entitled to any remedy, a claimant must demonstrate that s/he is the victim of a tortious wrong. A near miss, even if it causes significant distress, is not sufficient. Without the contents of the ABS coming to the attention of a third party there is no viable claim for misuse of private information. In simple terms, there has been no interference with the Article 8 rights of the relevant Claimant because the privacy of the information contained in the ABS has not been compromised at any stage.
>
> 146. The same is true for a civil claim for data protection. Data breach cases are premised on the personal data of the relevant claimant having been compromised; usually accessed by, or provided to, a third party. Shorn of the claim for "*loss of control*", the Claimants' claim is essentially one for Unlawful Processing by sending the ABS to the wrong address. But, if the ABS has not been opened or read by a third party, there has been no real "*processing*". It was a near miss. I accept that there are wider policy considerations underpinning the data protection

> regime. Concepts of placing the data "*at risk*" have greater resonance in the regulatory context. A person who leaves a laptop on a train, from which unencrypted personal data could readily be accessed, may face regulatory action even if the laptop is recovered without any data having been compromised.
>
> 147. In consequence, the claims in which the ABS was returned unopened fail to disclose reasonable grounds for bringing a claim for misuse of private information and/or data protection and will be struck out under CPR 3.4(2)(a). In the alternative, I would have found that these claims should be summarily dismissed under CPR Part 24 as having no real prospect of success.
>
> 148. Next, I will consider the cases in which the ABS has not been safely returned and where the relevant Claimant relies upon an inferential case that the ABS has been opened and read by a third party (see [33]-[34] above). In my judgment, in these claims, the relevant Claimant has no real prospect of success. As pleaded, I would also hold that the bare inferential case on publication falls to be struck out pursuant to CPR 3.4(2)(a).
>
> ...
>
> 154. The effect of the decisions I have made would be to leave 14 claims in which the relevant Claimant has a real prospect of demonstrating that his/her ABS was opened and read by a third party."

21. This line of reasoning reflected the respondent's arguments on misuse of private information and aspects of its pleaded case on damage; but it went beyond the three grounds on which the respondent had relied in support of its application to have the data protection claims dismissed. As to those grounds, the judge said that "whether the law in this jurisdiction imposes a threshold of seriousness in data protection claims" was an interesting and important point but he did not need to decide it in relation to these appellants, and in relation to the 14 remaining claimants it was a point which the court should resolve on the basis of facts found after a trial. As the *Jameel* issue now arose in relation to only 14 claims its nature had changed radically from what had been assumed in submissions. The judge had "no difficulty" in concluding that the court could fashion a procedure for adjudicating those claims and declined to strike them out as an abuse of process.

The draft Amended Master Particulars

22. In the light of the judgment below and directions given by this court the appellants have prepared draft Amended Master Particulars of Claim. Relevantly, these abandon the misuse of private information claim and the assertion that the appellants' personal data actually passed into the hands of any third party. Their claim now is that by processing their data in breach of statutory duty the respondent caused them to suffer "anxiety,

alarm, distress and embarrassment" for fear that their personal data "may have" passed into the hands of unknown third parties. They seek to add the words "and/or as a result of uncertainty as to what had become of their ABSs and who may have opened it, and/or by the fact that their Personal Data may be or may have been misused." This all appears legitimate in principle and I would grant permission to amend, without prejudice to the issues that arise about the viability of individual claims.

The appeal

23. The single ground of appeal is that the judge erred in law by striking out the data protection claims. In support of that headline contention Mr Campbell KC argued, in summary, that a cause of action under the GDPR and DPA is complete once there has been an infringement by a data controller or data processor and the data subject has suffered material or non-material harm; the appellants have a sufficiently pleaded case of infringement which the respondent has never alleged to be unarguable or untenable; and the judge was wrong to hold at [146] that in the absence of access to the data by a third party there had not been any "real" processing of the data; as to harm, the judge was wrong in law to reason that a fear or apprehension that personal data may be misused by a third-party is legally insufficient to ground recovery; and as the judge did not (and could not properly) reject the appellants' factual cases as untenable he should have dismissed the respondent's application.

24. The respondent acknowledged that the judge's reasons for dismissing the claims did not reflect the grounds on which the respondent had applied for such an order. The respondent accepted that it was bound by its pleading and Mr Sharland KC advanced no argument in support of the judge's reasoning. Instead, by a respondent's notice, the respondent asked the court to uphold the judge's decision on the three grounds that it had argued before him.

25. At least two of these grounds involve seeking a different order from the one made by the judge: we are invited to enter summary judgment for the respondent pursuant to CPR r 24 or alternatively to dismiss the claims as an abuse of process pursuant to CPR r 3.4(2)(b). For that reason the court's permission was required: see CPR 52.13, PD52C para 8 and *Braceurself Ltd v NHS England* [2023] EWCA Civ 837, [2024] 1 WLR 669. Permission was not sought until the hearing before us. The reason was that the respondent had misunderstood what the rules require. By the time of the hearing all parties had set out in detail their submissions on the substance of all the issues. The appellants had full warning of the arguments the respondent wishes to advance and ample time to prepare. They suffered no prejudice. To enforce procedural discipline by debarring the respondent from presenting its full case would have wasted considerable costs and effort in a case that has already consumed a great deal of both. It was and is clearly in accordance with the overriding objective to grant permission.

26. In support of the respondent's position Mr Sharland submitted that even if Nicklin J's reasoning was mistaken his instincts were correct. He suggested that what the judge was driving at was that the present claims are not sufficiently serious, nor capable of giving rise to a "real and substantial" tort. Mr Sharland invited us to find, as a matter of evidence, that the pleaded claims are simply lacking in reality and credibility. As he put it, "it simply cannot be the case that police officers, used to contending with dangerous and upsetting situations, have been genuinely distressed over a pensions forecast sent to an old address." Mr Sharland invited us to find, as a matter of law, that English data

protection law sets limits on the recognised heads of non-material loss, and that many of the pleaded claims fail to assert any recognised head of loss. He also submitted that the law contains a threshold of seriousness, which these claims do not and cannot surmount. Further and alternatively, Mr Sharland submitted that to allow any of these claims to proceed to a full trial would be highly disproportionate and a concerning waste of valuable court time and costs. He characterised the breach as "an unintentional, one-off and quickly remedied incident of a non-damaging nature" and a trivial, technical breach which should not be troubling the courts.

27. For the ICO, Mr Knight submitted that on a proper analysis there was processing as defined by the UK GDPR; the judge was wrong to find otherwise simply because no unauthorised third party had opened and read the correspondence. On the respondent's notice issues, Mr Knight submitted that we should follow the consistent case law of the CJEU to the effect that no de minimis principle or other threshold of seriousness should be applied in this context; compensation is recoverable for any "damage" suffered whilst recognising that "not all emotional responses to an infringement" will amount to non-material damage for this purpose. Mr Knight suggests that low value claims can and should be addressed as they are elsewhere in the law, through case management and appropriate track allocation under the CPR.

Data protection: the legal framework

28. The GDPR is EU legislation with direct effect in all EU member states. It enacts a number of data protection rights and obligations and contains provision for their enforcement. Article 5 identifies six "principles relating to processing of personal data" with which data controllers must comply. Articles 24, 25 and 32 require data controllers to "implement appropriate technical and organisational measures" to ensure GDPR compliance. Article 82 confers a right to receive compensation for material or non-material damage suffered as a result of an infringement. The GDPR applied with effect from May 2018. By Part 2 of the DPA, Parliament enacted provisions supplemental to the GDPR. Those provisions also came into force in May 2018.

29. These are the legislative instruments that apply to the events of 2019 with which we are concerned in this case. That is because Parliament decided that the GDPR should remain part of English law until the end of the Brexit implementation period on 31 December 2020 ("IP Completion Day") and it continues to be enforceable in respect of that period: see ss 2, 3 and 6 of the *European Union (Withdrawal) Act* 2018 ("EUWA 2018"). Since IP Completion Day a slightly modified domestic counterpart known as "the UK GDPR" has been in effect and Part 2 of the DPA applies in a correspondingly amended form: See the *Data Protection, Privacy and Electronic Communications (Amendments. etc) (EU Exit) Regulations* 2019 (SI 2019/419). We are not directly concerned with the UK GDPR, but it is relevant to note that nobody has suggested that there is any material difference.

30. Brexit has had this relevant legal effect: whereas in EU law decisions of the Court of Justice of the European Union ("CJEU") on the interpretation and application of EU legislation are authoritative and prevail over domestic decisions, our approach to the GDPR is governed by section 6 of EUWA 2018. We are bound by principles laid down by the CJEU and decisions made by it before IP Completion Day. These are "assimilated EU case law". However, we are not bound by any principles laid down, or any decisions made, by the CJEU after that date; we "may have regard" to such

principles or decisions "so far as it is relevant to any matter before the court". In deciding how to approach the latter class of CJEU decisions we are of course bound by the domestic law of precedent.

The infringement issue

31. The first question is whether the appellants have set out a reasonable basis for alleging that the respondent engaged in "processing" of their "personal data" within the meaning of the GDPR and DPA.

32. The appellants' pleaded allegations can be summarised as follows. All the items of information that I have listed above were held by the respondent on its Compendia computer database. The original residential addresses were provided to the respondent, which processed them by "collecting, recording, organising, structuring and storing" them in two locations on that database. The way in which it did this was in breach of the data minimisation principle (Article 5(1)(c)) and the accuracy principle (Article 5(1)(d)). The revised residential addresses were then provided to the respondent and processed in the same ways. This was done in breach of the principle of lawfulness and fairness (Article 5(1)(a)) as well as the data minimisation and accuracy principles. When the respondent came to prepare and print the ABS there was a process flaw in the way it dealt with the addresses. In consequence, the printed ABS bore the original residential address rather than the revised one. That flaw involved a computer error of some kind. The direct result was that the ABS, containing all the other items of information I have listed, were sent to the wrong address. That was done in breach of the principles of lawfulness, fairness, accuracy, and the integrity and confidentiality principle (Article 5(1)(f)). Further and alternatively, there was a breach of Articles 24, 25 and/or 32.

33. The original allegation was that the breaches complained of resulted in the personal data being "passed ... into the hands of unknown third parties". In the cases of these appellants, however, the judge held that they had no sustainable case to that effect. They have now abandoned that aspect of their claim. So the question is whether it can be said that the other alleged conduct involved processing personal data.

34. By Article 4(1) of the GDPR "personal data" means "any information relating to an identified or identifiable living individual ... ". Section 3(2) of the DPA contains all those words, subject only to an immaterial exception. This is language of extremely broad reach. There has never been any dispute that the information at issue here falls within it. Clearly it does.

35. Article 4(2) GDPR defines "processing" as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means". Illustrative examples are then given: "such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." Sections 3(4) of the DPA defines "processing" in identical terms, again subject to immaterial exceptions. As the CJEU said of Article 4(2) in '*SS' SIA v Valsts ieneumu dienests,* Case C-175/20, EU: C: 2022:124, [35]:

> "It is apparent from the wording of that provision, in particular from the expression 'any operation', that the EU legislature intended to give the concept of 'processing' a broad scope. That interpretation is corroborated by the non-exhaustive nature, expressed by the phrase 'such as', of the operations mentioned in that provision."

36. The appellants' pleaded case as to what happened up to the point at which the ABS were printed adopts some of the language of Article 4(2) GDPR and section 3(4) DPA ("collecting, recording, organising, structuring and storing"). The respondent admits that its dealings with the information involved operations of that kind and that they amounted to processing. The admissions are rightly made. These were "operations performed on" personal data "by automated means". In an early passage of his judgment the judge appears to have recognised this. In paragraph [4] he observed that "The error appears to have happened because of the way in which the relevant [appellants'] address details were stored and processed in the database used by the [respondent]."

37. The next steps in the sequence of events involved the respondent printing hard copy documents in the form of the ABS, placing them in envelopes, and sending them by post. It might perhaps have been argued that although these steps followed the automated processing of the data they were essentially separate and distinct manual operations, applied to the ABS as a document, which did not involve "operations ... performed on personal data" and thus did not qualify as "processing". But the judge did not rely on any such reasoning nor has the respondent ever advanced any such argument. On the contrary, its Defence expressly admits that these aspects of their operations did amount to processing. There is no basis for striking out these aspects of the claims.

38. For the ICO, Mr Knight has submitted that a segmented or atomised approach to what went on here would be artificial and wrong in principle. I can see the force of that. As the issue does not arise for decision, I confine myself to the as prevfollowing observations.

    (1) The definition of processing in the GDPR is essentially the same as it was in the predecessor Directive (95/46/EC), which was implemented in this jurisdiction viha the Data Protection Act 1998. Both definitions include "any operation or set of operations" performed on personal data. In *Campbell v MGN Ltd* [2002] EWCA Civ 1373, [2003] QB 633 the Court of Appeal rejected a submission that the publication of a hard copy newspaper fell outside the notion of "processing" for the purposes of the 1998 Act, holding (at [106]) that "where a data controller is responsible for the publication of hard copies that reproduce data that has previously been processed by means of equipment operating automatically, the publication forms part of the processing and falls within the scope of the Act". The later Court of Appeal decision in *Johnson v Medical Defence Union* [2007] EWCA Civ 262, [2008] Bus LR 503 seems to me to turn on the particular and unusual facts of that case.

(2) The objectives of the GDPR include the protection of fundamental rights and in particular the right to the protection of personal data (Article 1(2)). The material scope of the GDPR encompasses the processing of personal data "partly by automated means" and "the processing other than by automated means of personal data which form part of a filing system" (Article 2(1)). Recital (15) states that "the protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained ... in a filing system."

(3) In *Endemol Shine Finland Oy,* Case C-740/22 (EU:C:2024:216) [29]-[39] the CJEU, having regard to these features of the GDPR, held that the oral disclosure of personal data falls within the concept of processing under the GDPR and comes within the material scope of the Regulation "where the information forms part of a filing system". Put another way, where a data controller is responsible for the oral disclosure of personal data that have previously been processed by automated means the oral disclosure forms part of the processing. We are not bound by this decision but I see no reason to take a different view in this jurisdiction. The court's reasoning is persuasive and appears consistent with the approach in *Campbell.*

39. In the present case there was no "publication" of the personal data which had previously been held and otherwise processed automatically. The claimants could not, therefore, legitimately assert that the processing here involved (to quote the definition) "disclosure by transmission [or] dissemination" of the data. On a strict analysis they did not make such an allegation. Their contention that the data "passed ... into the hands of unknown third parties" was not pleaded as part of their case on breach but only in support of the allegation that the pleaded breaches caused damage and distress. In any event, for the reasons I have given it was not essential for the appellants to allege or prove third-party disclosure. Despite the rejection of that aspect of their case the appellants are still entitled to complain that the respondent's conduct involved processing of the appellants' personal data. The respondent rightly accepts that this is so.

40. Mr Campbell advanced an alternative submission, that even if there was no processing there is a tenable case of infringement based on Articles 24, 25 and 32. This appears to be a novel proposition. It found no support from Mr Knight on behalf of the ICO who argued that it is the concept of processing that lies at the core of the data protection regime. There can certainly be infringements without disclosure or publication of personal data: see *Data Protection Commissioner v Facebook Ireland Ltd* (Case C-311/18) [2021] 1 WLR 751. But it does not follow that there can be infringement without processing. As I have shown, the concept of processing embraces a great deal more than disclosure or publication. It includes mere recording. For my part I have found it hard to envisage any circumstance in which a data subject could advance any tenable claim for compensation for an "infringement" that did not involve some form of "processing" of the subject's personal data. But in the light of my conclusions on the question of processing it is unnecessary to decide the point.

The compensation issue

The GDPR and DPA

41. Article 82 of the GDPR provides, so far as relevant:

> "(1) 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 ... for the damage suffered."
>
> (2) Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation ..."

42. Section 168(1) of the DPA provided at the material time that "In Article 82 of the GDPR (right to compensation for material or non-material damage), '*non-material damage'* includes distress."

The pleaded claims

43. The appellants' case, as set out in the draft Amended Master Particulars, now includes just two generic allegations. First, that the breaches complained of led each appellant to experience "anxiety, alarm, distress and embarrassment" at the prospect or possibility that their personal data may have come into the hands of third parties and been misused or exposed to the risk of misuse. This is expressly pleaded as "non-material damage". Secondly, 42 of the appellants allege that the breaches caused them to suffer an aggravation of a pre-existing medical condition. For this, general damages are claimed. The Particulars do not categorise this head of loss as material or non-material. The individual schedules, being pleaded by way of additional information, must be read in the context of the Master Particulars.

Incredible?

44. It is convenient to begin with Mr Sharland's invitation to reject the factual allegations pleaded by the appellants as simply incredible and to enter summary judgment for the respondent on that basis.

45. Referring to well-known passages in *Three Rivers DC v Bank of England (No 3)* [2001] UKHL 16, [2003] 2 AC [95] and *E D & F Man Liquid Products v Patel* [2003] EWCA Civ 472 [10] Mr Sharland submitted that we could "say with confidence ... that the factual basis for the claim is fanciful" and that it was "clear that there is no real substance" in the appellants' factual assertions. Mr Sharland pointed to the distinction between statements of primary fact on the one hand and, on the other, inferences, assertions of law and matters of comment, which the court is not bound to accept as correct (*Korea National Insurance Corporation v Allianz Global Corporate & Speciality AG* [2007] EWCA Civ 1066, [2007] 2 CLC 748 [11]). Developing the headline submission I have quoted at [26] above, Mr Sharland argued that it was "simply unreal" to suggest that any of the appellants had a genuine belief that their data had gone to someone unknown let alone that it had been misused, and that the "levels of distress referred to [are] entirely improbable". He submitted, further, that the individual schedules contained clear indications of the unreal and artificial nature of the claims and "cast serious doubt" on their authenticity and credibility. He pointed to the use of certain "stock phrases" which appeared to have been "cut and pasted" into multiple individual schedules.

46. There certainly is a considerable degree of overlap in the language used to plead the claimant-specific schedules. An Annex to the respondent's skeleton argument identifies more than 15 distinctive phrases that appear and reappear verbatim on multiple occasions. By way of example, some 85 claimants allege that they were "conscious that this information could be used to fraudulently apply for documentation, such as some forms of identification". Some 82 say they were "baffled and frustrated" by the mis-addressing of their ABS. Some 53 cite concerns about what might be done by persons with "malevolent intent". Forty seven complain that "the defendant has sought to trivialise the breach".

47. In the end, though, this aspect of the respondent's argument is unconvincing. It is true that the court is not bound to accept as credible everything said by the respondent to a summary judgment application. The court may conclude that the respondent has no real prospect of establishing its factual case at trial. The paradigm case in which it may do so is where the respondent's evidence is contradicted by a contemporaneous document the authenticity is not in doubt. This is not such a case. Nor is there anything comparable. The key allegations are not matters of inference or legal argument but matters of primary fact. The appellants have asserted that upon learning of the data breach they experienced certain emotional (and in some instances physical or psychological) responses. These are facts the truth or falsity of which is within the appellants' own knowledge.

48. The point about repetition is not strong enough to justify summary judgment. The "stock phrases" are not contained in witness statements, which must be in the witness's own words or at least their own language (PD32 para 18.1). They are in statements of case served pursuant to Part 18. The natural inference is that they were drafted by the appellants' legal team, as Mr Campbell submitted was the position. In that context the sheer scale of the exercise makes repetition understandable. The words used in the schedules may not be those which the appellants would have used but that is not a breach of the rules or practice directions. And they have verified what is said as a matter of substance. It would be a strong thing for the court to reject the statements of truth without hearing from the individual concerned. I do not consider we would be justified in taking that step.

Out of scope (no distress)?

49. The next issue is whether some of the appellants have failed to plead a case of actionable damage. Mr Sharland submitted that on the true construction of the GDPR and DPA compensation is not recoverable for emotional responses other than distress. The claim of any appellant whose individual schedule failed to assert distress should therefore be dismissed. Mr Sharland identified 34 such appellants, being those who had pleaded that they (i) would not describe the feelings they suffered as distress; (ii) did not suffer distress; (iii) considered distress too strong a word to describe their experience, or said that they were too resilient to have suffered distress; and/or (iv) confine their pleading to "stress" as distinct from "distress". In support of this submission Mr Sharland relied on the language of s 168(1) of the DPA.

50. In my judgment this submission is too stark and formalistic. I think there is much to be said for the view that compensation is not available in respect of (to adopt Mr Knight's terminology) "all emotional responses to an infringement". I shall come back to that.

But I can see no justification for confining the right to compensation in the way suggested in this part of the respondent's argument.

51. The governing provision is Article 82, which refers to "non-material damage" without limitation. Section 168(1) of the DPA tells us that this term "includes distress" but it is plain that this is an illustrative point. Section 168 does not purport to define or limit the scope of the term "non-material damage" in Article 82. Indeed, it seems clear that Parliament's aim in enacting s 168(1) was not to limit the ambit of the right to compensation but rather to confirm its breadth. Notoriously, section 13(2) of the 1998 Act, which restricted the right to compensation for distress, had to be disapplied for incompatibility with Article 23 of the parent Directive: *Vidal-Hall v Google Inc* [2015] EWCA Civ 311, [2016] QB 1003. It would be understandable for Parliament to make clear that it was not committing the same error in the 2018 Act. The Explanatory Notes to the DPA appear to confirm this was the aim, stating (at paragraph 481) that the right conferred by Article 82 "is broadly equivalent to section 13 of the 1998 Act, with the exception that the type of damage that can be claimed is broader...".

52. In addition, it seems to me that Mr Sharland's argument depends on an unjustifiably narrow interpretation of the term "distress". In English law this term is not usually deployed to distinguish between forms or degrees of emotional harm. It is typically, and most commonly, used as an umbrella term for various forms of emotional harm (including, for instance, stress and anxiety) to distinguish harm of that kind from material damage (as in s 13 of the 1998 Act) or from other kinds of intangible loss (such as "loss of control"). The point is reflected in paragraph [92] of *Lloyd v Google* where Lord Leggatt observed that "The term 'material damage' is sometimes used to describe any financial loss or physical or psychological injury, but excluding distress (or other negative emotions not amounting to a recognised psychiatric illness)".

53. In any event, our approach to the Regulation should not become bogged down in arguments about the meaning of "distress" in domestic law. We should have regard to the language of the GDPR, which is part of our law for this purpose. This includes the Recitals which state, among other things, that the kinds of "material or non-material damage" that a person may suffer as a result of a personal data breach include "limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage ..." (Recital (85)). All of this is clearly at odds with Mr Sharland's submission. The Recitals also state that "The concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice" (Recital (146)). We should therefore have regard, at least, to the way the CJEU approaches compensation for "non-material harm" in the context of the GDPR.

Too trivial (below a threshold of seriousness)?

54. In a series of decisions of 2023 and 2024 the CJEU has consistently held that it is impermissible for the domestic courts of EU countries to require proof that the damage suffered reaches a minimum degree of seriousness.

55. In *UI v Österreichische Post AG,* Case C-300/21, [2023] 1 WLR 3702, the data subject complained of the use of an algorithm which relied on various social and demographic criteria to infer that the data subject had a high degree of affinity with a certain political

party. There had been no communication of the subject's personal data but he felt offended and claimed compensation against the data processor for "upset, loss of confidence and public exposure". The domestic court rejected the claim on the basis that domestic law required the damage suffered to reach a certain level of seriousness. On a reference by the Austrian Supreme Court the Advocate-General advised (at [112]) that Article 82 was not a suitable vehicle for countering infringements which only caused "annoyance or upset" . He proposed (at [117]) that the court should hold as follows:

> "The compensation for non-material damage provided for in the Regulation does not cover mere upset which the person concerned may feel as a result of the infringement. It is for the national courts to determine when ... a subjective feeling of displeasure may be deemed, in each case, to be non-material damage."

56. The CJEU took a different approach. It made clear (at [32]) that the existence of damage which has been suffered is one of the preconditions to that right to compensation; and (at [42]) that mere infringement is therefore not enough to confer such a right; but (at [44]) that the concept of "non-material damage" must be given an autonomous definition in EU law, independent of the domestic law of member states; and (at [51]) that this definition cannot permit the imposition of a threshold of seriousness:

> "article 82(1) of the GDPR must be interpreted as precluding a national rule or practice which makes compensation for non-material damage, within the meaning of that provision, subject to a condition that the damage suffered by the data subject had reached a certain degree of seriousness".

57. *VB v Natsionalna agentsia za prihodite*, Case C-340/21, [2024] 1 WLR 2559 arose from a cyber-attack on the Bulgarian National Revenue Agency which resulted in the personal data of six million people being published on the internet. One of these sought compensation for non-material damage in the form of fear that her personal data might be misused, or that she might be blackmailed, assaulted or kidnapped. Her claim was dismissed by the domestic court. On a reference from the domestic appellate court the CJEU confirmed that the claim was not wrong in principle, and (at [78]) reiterated and endorsed the proposition at [51] of the *UI* case.

58. *VX v Gemeinde Ummendorf,* Case C-456/22 (EU:C:2023:988) related to a German municipality which had published on the internet the agenda of a council meeting containing the names and addresses of the applicants. One of the questions referred to the CJEU was whether Article 82 contained a de minimis threshold. The court recalled (at [16]) its decision on that point in the *UI* case and (at [18]) affirmed in terms that Article 82 "does not require that, following a proven infringement ... the 'non-material damage' alleged by the data subject must reach a 'de minimis threshold' in order for that damage to be capable of compensation."

59. In *BL v MediaMarktSaturn Hagen-Iserlohn GmbH* Case C-687/21, [2024] 1 WLR 2597 the claimant went to the data controller's shop and bought an electrical appliance. Another customer who had jumped the queue was mistakenly given the appliance and related documents. The documents contained personal data, including the claimant's full name and address, his employer's name and his income and bank details. Within half an hour the documents had been returned to the data subject without the other customer becoming aware that he had been in possession of the personal data. A claim for compensation for non-material damage was stayed by the domestic court pending a reference to the CJEU. The court was asked, among other things, whether a person claiming compensation under Article 82 is required to establish that the infringement led to non-material or material damage. Unsurprisingly, the court's answer was affirmative. In reaching that answer the court (at [59]) again reiterated with approval the proposition in paragraph [51] of the *UI* case.

60. The principle enunciated in this line of decisions would seem to rule out not only the respondent's contention that "distress" is an essential ingredient of a viable claim but also the respondent's alternative submission that the appellants' claims should be dismissed as falling short of a threshold of seriousness.

61. Mr Sharland did not dispute this but made three main submissions in response. First, he said that this CJEU jurisprudence all post-dates IP Completion Day and is thus non-binding. Secondly, he submitted that domestic authority binds us to conclude that data protection law in England and Wales does include a threshold of seriousness. He relied on the Supreme Court's decision in *Lloyd v Google* and the decision of this court in *Prismall v Google UK Ltd* [2024] EWCA Civ 1516, [2025] 2 WLR 1224. Thirdly, and in the alternative to his second submission, Mr Sharland invited us to depart from the CJEU jurisprudence. He said that we are not required to follow post-completion-date decisions which appear to be flawed or inconsistent (*Tower Bridge GP v HMRC* [2022] EWCA Civ 998, [2023] 1 CMLR 16 [119] (Lewison LJ)). He submitted that the CJEU's reasoning was flawed; that the reasoning of the Advocate-General in the *UI* case was to be preferred; that if the domestic authorities are not binding they (and a number of first instance decisions he also cited) are nonetheless persuasive; and that the imposition of a threshold of seriousness would serve the beneficial aims of eliminating trivial claims and achieving coherence in the law.

62. Mr Sharland's first submission is clearly correct: we are not bound by the CJEU decisions I have cited. But I do not accept Mr Sharland's submissions about the effect of the domestic authorities. Nor do I agree that we should choose to depart from the CJEU jurisprudence.

63. The first point to make about *Lloyd v Google* is that the case was concerned with the interpretation and application of the provisions of s 13 of the 1998 Act the language of which provided for awards of compensation for "damage" or "distress". The GDPR was not in issue and was specifically excluded from the court's analysis: see the judgment of Lord Leggatt (with whom the other Justices agreed) at [16]. Secondly, no issue arose as to whether a person claiming compensation for non-material damage must prove that the damage crossed a threshold of seriousness. The claimants did not allege any material damage nor any distress. Their contention was that pursuant to s 13 "an individual is entitled to compensation for any non-trivial contravention of [the 1998 Act] without the need to prove that the individual suffered any financial loss or distress": [88]. The argument was that so long as the contravention was serious enough

to count as "non-trivial" the mere fact that it resulted in a "loss of control" was enough to merit compensation, which could be awarded at a standard minimum rate. Accordingly, a representative action could be brought successfully without the need for individualised proof of damage or distress. The court's decision was that this is wrong; on a true construction of the statute it was necessary for each claimant to prove not only infringement but also that this caused some material loss or distress to them; there was no right to compensation for the "loss of control" complained of which, on a proper analysis, was one and the same as the fact of breach. All of this is clear from the headnote and the body of Lord Leggatt's judgment: see in particular, paragraphs [105]-[107], [115], [143].

64. The passages of the judgment on which the respondent relies are in paragraph [153]. That paragraph includes a reference to a "threshold of seriousness" and an assertion that it is "impossible to characterise such damage as more than trivial". But those words must be read in their context. They appear in a section of the judgment in which Lord Leggatt, having rejected the claimants' primary case that individualised proof of damage was unnecessary, addressed a separate issue namely, "The need for individualised evidence of *misuse*" (emphasis added). In this part of the judgment (at [144]-[157]) Lord Leggatt identified a further reason why the representative claimant's attempt to recover damages under s 13 by means of a representative action could not succeed. This was that

> "Even if (contrary to my conclusion) it were unnecessary in order to recover compensation under this provision to show that an individual has suffered material damage or distress as a result of unlawful processing of his or her personal data, it would still be necessary for this purpose to establish the extent of the unlawful processing in his or her case".

Lord Leggatt reasoned that "on the claimant's own case" there could be no compensation unless the infringement crossed a threshold of seriousness (that is, that it was "non-trivial"); yet on analysis the claimant was attempting to recover damages on behalf of millions of individuals without proving that this threshold was crossed in any individual case. The passage relied on is thus both obiter and not in point for present purposes.

65. It is not arguable that *Prismall* binds us to conclude that English data protection law incorporates a threshold of seriousness. *Prismall* was a representative action for damages for misuse of private information. In the passages relied on the court did no more than summarise features of the facts and reasoning in *Lloyd v Google,* so far as they were relevant to the issues in dispute in the case before the court. None of those issues called for, or resulted in, a decision on the threshold of seriousness in data protection law. I therefore reject the submission that the domestic cases dictate the answer to the legal issue raised by the respondent.

66. The other domestic cases relied on are *Rolfe v Veale Wasbrough Vizards Ltd* [2021] EWHC 2809 (QB), *Johnson v Eastlight Community Homes* [2021] EWHC 3069 (QB), and *Driver v Crown Prosecution Service* [2022] EWHC 2500 (KB). These do not assist the respondent. They are all first instance decisions, two by High Court Masters and

one by a High Court Judge. One of them does not address at all the question of a threshold of seriousness. All of them ante-date the CJEU cases I have cited. They do not even assist on the facts. In *Johnson* the claim was deemed to be of very low value yet survived a strike-out application and was transferred to the County Court. In *Driver* the claim went to trial before Julian Knowles J who found that the claimant had suffered only "a very modest degree of distress" yet made an award of £250.

67. That brings me to the question of whether we should choose to plot a different course from the one taken by the CJEU. That is open to the UK as a political choice and a legislative option. But a judicial decision to do so would call for sufficiently compelling legal reasons. In that context I think it right to attach some weight to the fact that the GDPR is an international legal instrument which had direct effect in this jurisdiction at the material time. Further, its domestic successor, the UK GDPR, is post-Brexit legislation in which Parliament decided to adopt the identical language, so far as material to this case. Self-evidently, divergent interpretations of the same legislative text tend to undermine legal certainty. It seems to me that, other things being equal, it makes good legal sense for the court to interpret and apply the GDPR in conformity with settled CJEU jurisprudence.

68. A threshold of seriousness clearly does exist in the law of misuse of private information. There is ample authority for that proposition, which is rooted in the Strasbourg jurisprudence under Article 8 of the Convention. But I do not find this a persuasive reason for introducing such a threshold in the context of the separate and distinct legal regime for the protection of personal data. One of the arguments advanced in *Lloyd v Google* was that compensation for loss of control should be available under s 13 of the 1998 Act because it is available in misuse of private information and the two torts share a "common source" in the fundamental right to privacy guaranteed by Article 8. The Supreme Court rejected that argument as flawed. At [124] Lord Leggatt explained that it did not follow from the fact that the two legal regimes aimed at a general level to provide protection for the same fundamental value "that they must do so in the same way or to the same extent or by affording identical remedies".

69. This seems to me to apply with equal force to the question I am now considering. Data protection law has an international dimension, and covers a much wider field than the domestic tort of misuse of private information. There is no inherent reason why the contours of these different wrongs should be identical. More generally, whilst I agree that it is a good thing for the law to be coherent the mere fact that differences exist between the ingredients of individual torts is not proof of incoherence.

70. I can see that the CJEU might have taken a different line. The reasoning of the Advocate-General in the *UI* case has some attractions. He said, among other things, that "compensation arising as a result of a mere feeling of displeasure ... is easily confused with compensation without damage, which has already been ruled out" ([113]); that "the inclusion of mere upset in the category of non-material damage eligible for compensation is not efficient" ([114]); that "refusal of the right to compensation for vague, fleeting feelings or emotions ... does not leave the data subject without any protection at all" ([115]); and that there is "a fine line between mere upset (which is not eligible for compensation) and genuine non-material damage..." ([116]). Some support for a threshold of seriousness might have been found in the language of Recital (85), quoted above, which speaks of "*significant* economic or social disadvantage" (emphasis added).

71. However, the CJEU, having considered the arguments of the Advocate-General, decided to answer the question that had been referred in a different way. Its reasons were, in summary, that Article 82 contains no reference to a threshold of seriousness; that Recital (146) tends to indicate that there is not and should not be such a threshold; and that the imposition of a threshold to be applied by domestic courts would undermine the level of protection afforded to natural persons, and risk incoherence in the application of the GDPR: see [44]-[49]. That same reasoning has been reflected or adopted in the subsequent cases. The reasoning is logical and sufficient. I am not persuaded that the approach of the CJEU is fundamentally flawed. Importantly, I think the significance of the passages cited has been overstated. Those passages focus on the question of whether a claimant alleging non-material harm must establish that the harm reached a certain degree of seriousness. The decisions unequivocally reject that proposition. The respondent has treated that as tantamount to a conclusion that compensation is always recoverable under Article 82 for any negative emotional response to an infringement, however transient and minimal the data subject's displeasure might have been. But the court's reasoning does not go that far. And the cases show that there is a separate and prior issue, namely whether the consequences alleged by the data subject qualify as "non-material damage" within the meaning of Article 82. The court has addressed the interpretation of that term in some limited but important respects.

72. The general principle was stated in *UI* at [50]:

> "The fact remains that the interpretation thus adopted cannot be understood as meaning that a person concerned by an infringement of the GDPR which had negative consequences for him or her would be relieved of the need to demonstrate that those consequences constitute non-material damage within the meaning of article 82 of that Regulation."

In *VX* at [21]-[22] the court reiterated the point, emphasising that mere infringement is not sufficient to confer a right to compensation; damage within the meaning of Article 82 must be proved.

73. In *VB* the court was asked to interpret the notion of "non-material damage". The specific question was, in essence, whether Article 82 must be interpreted as meaning that the fear experienced by a data subject with regard to a possible misuse of his or her personal data by third parties as a result of an infringement of the GDPR was "capable in itself, of constituting 'non-material damage'". The answer was in the affirmative. Having reiterated that the imposition of a threshold of seriousness was impermissible, the court went on to hold that the GDPR "does not rule out the possibility" that the concept of non-material damage encompasses the fear that the data subject's personal data will be misused by third parties. But the court added these qualifications:

> "84. However, it must be pointed out that a person concerned by an infringement of the GDPR which had negative consequences for him or her is required to demonstrate that those consequences constitute non-material damage within the meaning of article 82 of that Regulation (see *Österreichische Post*, para 50).

> 85. In particular, where a person claiming compensation on that basis relies on the fear that his or her personal data will be misused in the future owing to the existence of such an infringement, the national court seised must verify that that fear can be regarded as well founded, in the specific circumstances at issue and with regard to the data subject."

74. In *BL* the court took this line of thinking a step further. The question posed by the referring court was, in essence whether "if a document containing personal data was provided to an unauthorised person, and it was established that the unauthorised third party did not become aware of those personal data, 'non-material damage' is likely to consist of the mere fact that the person concerned fears that, following that communication which made it possible to make a copy of that document before returning it, a dissemination, even abuse, of those data may occur in the future": [62]. Building on *VB*, the court affirmed (at [67]) that Article 82 encompasses a situation in which "the data subject experiences the well-founded fear, which is for the national court to determine, that some of his or her personal data be subject to dissemination or misuse by third parties in the future, on account of the fact that a document containing those data was provided to an unauthorised third party who was afforded the opportunity to take copies before returning it." But the court added this qualification:

> "68. However, the fact remains that it is for the applicant in an action for compensation under article 82 of the GDPR to demonstrate the existence of such damage. In particular, a purely hypothetical risk of misuse by an unauthorised third party cannot give rise to compensation. This is so where no third party became aware of the personal data at issue.
>
> 69..... 'non-material' damage, within the meaning of that provision, does not exist due to the mere fact that the data subject fears that, following that communication having made possible to the making of a copy of that document before its recovery, a dissemination, even abuse, of those data may occur in the future."

75. These cases seem to me to provide a touchstone by which most if not all of the remaining issues in this case can be fairly resolved. I would put it this way: in principle a claimant can recover compensation for fear of the consequences of an infringement if the alleged fear is objectively well-founded but not if the fear is (for instance) purely hypothetical or speculative.

76. In all these circumstances I do not see any sufficiently weighty reason for departing on this appeal from the settled CJEU jurisprudence on the threshold of seriousness issue. It follows that there is no need to consider whether the individual claims would cross such a threshold.

Hypothetical or ill-founded? (Fear of third-party misuse)

77. It may be helpful to recapitulate at this stage. The CJEU decisions make clear that in principle a data subject whose rights have been infringed may claim compensation for "non-material damage" consisting of a fear that the infringement might have harmful consequences. The appellants' pleaded case on that score cannot be dismissed as incredible, out of scope, or below a threshold of seriousness. But it remains to consider whether the pleaded fears can be characterised as "well-founded" as opposed to being based on a "purely hypothetical risk" or similar, within the meaning of those terms as used by the CJEU.

78. I take the language used by the Court in *VB* and *BL* to import an objective standard or test of reasonableness. It is not necessary to decide whether a similar approach would be adopted if this were a claim in some other, purely domestic tort.

79. Mr Sharland invited us to hold that, taking the appellants' pleaded case at its highest, all of the claims based on fear of the unknown fail the test identified in *BL*. The essence of this submission is that we should uphold the judge's order and dismiss the appeal on the grounds that although each of the appellants has a tenable case of infringement none has pleaded a reasonable basis for claiming compensation for fear of what might happen. Mr Sharland submitted that "the fears and concerns referred to ... are entirely irrational". Mr Sharland offered to take us through each schedule but pointed to some illustrative examples and some salient common features of the factual position in each case. He argued that many of the claimants came to know for certain that their ABS had never been opened and read, and that none of them ever had any good reason to fear that this would happen or that it might have happened. On this latter point Mr Sharland relied on the reasons given by Nicklin J for concluding that no inference of disclosure could be drawn. He argued that it followed that the appellants' fears could not be well-founded. Further, submitted Mr Sharland, none of the appellants had any good reason to fear that if the envelope was opened its contents would be misused in any of the ways suggested. The information was not sensitive data and was limited in scope.

80. I am not able to accept these submissions. The fact that these appellants cannot prove that their ABS were opened and read does not of itself show that the fears they entertained were not well-founded. The test of reasonableness cannot depend on hindsight. It must be applied with reference to the facts and matters that were or should have been known to the appellant at the time they experienced the stated fear. That is implicit in paragraph [85] of *VB* and clearly correct in principle. It is obvious that a person can hold well-founded fears about future harm even if no such harm in fact results. If an illustration were needed, the facts of *George v Cannell* [2024] UKSC 19, [2024] 3 WLR 153 provide one.

81. That said, none of these claims can succeed unless the individual appellant pleads and ultimately proves a reasonable basis for fearing (1) that their ABS had been or would be opened and read by one or more third parties and (2) that this would result in identity theft or one or the other consequences which that appellant feared might follow. And in assessing whether such a basis has been identified, aspects of the judge's reasoning are pertinent.

82. At [149]-[152] the judge contrasted the drawing of inferences with "speculative guesswork". He observed that:

> "absent some facts that would compel a different conclusion the court will not draw the inference that a letter addressed to a named recipient, clearly marked 'private and confidential' will be opened by a third party who is not the named recipient or authorised by him to open correspondence addressed to [the] named recipient."

The judge held that the evidence did not support any such inference but tended if anything to support an inference that "private correspondence is not generally opened by someone who is not the addressee". In only 14 of the 450 cases was there evidence that the ABS had been opened and in only 2 of those cases was there evidence that it was opened by someone other than a family member or colleague: ibid. That, it seems to me, is exactly as one would anticipate. Anyone receiving one of these envelopes would see at a glance that it was a private communication, of an expressly confidential nature, which had been sent to the right person but the wrong address. The overwhelming majority of people do not open such correspondence but return it (as happened in more than 100 cases here) or keep it, or throw it away. Looking at the matter generally, the chances of such a letter being opened are remote.

83. So too, in my judgment, are the chances of the information in an ABS being misused if, exceptionally, the envelope was opened and the document was read. The reader would immediately appreciate that the document contained personal financial information. They would be able to infer that the addressee was a police officer. But speaking generally, the chances of a police officer's former home being occupied by a criminal or other "malevolent actor" are slight. In this context, it is relevant to note that of the 750 persons affected only 37 took up the offer of free fraud insurance and that nearly six years after the event no evidence has emerged of any actual misuse. Other contextual factors that require consideration when addressing the reasonableness of the appellants' fears include the respondent's assessment of the level of risk, that of the ICO, and what the appellants were told about those assessments.

84. The generic factual allegations in the Master Particulars (and the draft Amended Master Particulars) cannot provide the necessary objective foundation for the fears alleged. All that is alleged there is the fact of infringement, the fact of the fears, and an allegation of causation. Nor can the mere fact that an appellant came to know that their ABS had been sent to the wrong address be enough to found a well-founded fear that it would be opened and read. In my judgment, individual schedules can only be sufficient if they state a specific and reasonable basis for fearing that in the particular case of the appellant in question the envelope would be opened by someone and its contents read. If that much is pleaded, an individual schedule will still fall short unless it also sets out particular circumstances amounting to a reasonable basis for fearing that the information in the ABS might be misused in one of the ways set out in the draft Amended Master Particulars.

85. Accordingly, the question raised by this aspect of the respondent's case is whether any of the appellants have set out a reasonable basis for a claim to compensation which might succeed at trial in the light of the principles I have identified above (and in particular at [75], [78] and [81]). Having reviewed a sample of the individual schedules I am confident that a decisive answer to that question can be produced in each case. An

answer could, for instance, be given in respect of the first claimant and claimant no 45, whose claims I have outlined above, by scrutiny of their individual schedules. I see no reason in principle why such determinations should not be made at this stage. The appellants have had a sufficient opportunity to state their case and to provide supporting evidence.

86. The exercise could be carried out by this court. I would however decline the respondent's application for that to be done. It is not possible to do it fairly without a proper examination of each individual schedule. The number of claims here means that the scale of the exercise proposed is considerable. We have been provided with four files of individual schedules, running to some 2,696 pages. This is not a court of first instance. Generally, our function is to review or, exceptionally, re-hear issues that have already been decided at first instance. Here, we are being asked to uphold the judge's order for different reasons. That is legitimate. However, for each member of this court to review all of these schedules would represent an inappropriate allocation of judicial resources.

87. I would therefore remit the respondent's application on this point to the High Court. A judge can then determine whether the task of answering the question I have identified should be allocated to a Judge, a Master, or even the County Court, and give any appropriate case management directions.

Aggravation of existing medical conditions

88. This is the second remaining head of damage pleaded in the Master Particulars. It arises in only 42 of the claims. In those claims the individual schedules summarise the appellant's case and a medical report has been served which amplifies the pleading. In each of the three exemplar reports what is alleged is that the appellant suffered psychological effects consequential on distress or some other emotional reaction they experienced upon learning of the data breach. One of the exemplar reports identifies symptoms of "stress, mood disturbance and general anxiety" suffered for about five months, all being wholly or partly attributable to "the index accident". The cause of these is identified as "persistent worries of what could happen to his children and wife ... when he was not at home if it was targeted by criminals."

89. A second report identifies all of the above-mentioned symptoms, as well as "concentration problems" and "social withdrawal" partially attributable to the index event. These are said to flow from fear of the appellant's data getting into the wrong hands, including fear of identity theft and a belief that people who want this appellant dead would be able to track him down using the "leaked" information which "could be easily sold and accessed on the dark web".

90. The third exemplar report identifies the self-reported problems "immediately after the accident" in this way: the appellant was "distressed by the initial notification", felt that it "did not recognise or acknowledge the gravity of the data breach or its implications" and was "worried about fraud and, more so, about the possibility of her sensitive personal information falling into the wrong hands". The psychologist's opinion in this case is that as a result of the "index event" this claimant suffered exacerbation of pre-existing symptoms of anxiety, low mood and symptoms of Obsessive Compulsive Disorder. These were "moderate" for about six months becoming "mild/minimal" thereafter.

91. It may be that for the purposes of Article 82 harm of these kinds should be classified as "material damage". In domestic law recognisable psychiatric harm has long been categorised as personal injury and that approach appears consistent with international law: see *Lloyd v Google* [92], cited above, *Shehabi v Kingdom of Bahrain* [2024] EWCA Civ 1158, [2025] 2 WLR 467, and the recent decision of the Irish Supreme Court in *Dillon v Irish Life Assurance* [2025] IESC 37. We received no argument on that issue. I do not think the classification matters in this case, however. The principal reaction identified in these reports was the one I have discussed earlier: fear of what might be done with the information in the ABS. That is clearly pleaded as a head of loss.

92. We have no basis on which to reject the expert opinions in the psychologists' reports or the factual assertions on which they are based. But the viability of these claims seems to me to depend on the issue I have already discussed. If the appellant's fears of what might happen were objectively well-founded, compensation for any consequential impact on the appellant's mental health is in principle recoverable. If, on the other hand, the fears were not well-founded, the claim for compensation must fail in its entirety. To that extent, it appears to me that this category of case raises no separate issue. These claims will stand or fall according to the court's conclusions on the objective reasonableness of the stated fears.

Annoyance or irritation

93. Almost all of the individual schedules allege that the appellant experienced one or more of these reactions to learning of the data breach. Similar responses are detailed in the exemplar medical reports. A claim to be compensated for annoyance or irritation caused by fear of third party misuse is tenable, provided the fear is well-founded. The CJEU jurisprudence tells us that such complaints cannot be dismissed for falling short of a threshold of seriousness. But many, if not all the annoyance or irritation complained of is said to have stemmed from other causes. For example, claimant 113 pleads that he suffered "considerable annoyance" as well as anger that his ABS had been posted to an address he had not occupied for more than 18 years and "frustration and annoyance" at the delay between the breach and notification. The issue is whether claims of those other kinds can be maintained. I do not consider that they can.

94. In my judgment, claims to be compensated for reactions of irritation or annoyance at the mere fact of the breach, or at the way in which the respondent notified it, or dealt with it, fall outside the scope of the Master Particulars and are not maintainable in the absence of an amendment to that document. The point is straightforward. The Master Particulars asserted three main heads of damage, as I have explained. Fear of what third parties might do with the appellant's information was among them. So was exacerbation of a medical condition. Irritation or annoyance of the kinds I have mentioned was not. The respondent sought and obtained an order for further information about the claims asserted in the Master Particulars. The purpose was to gather details about the individual claims. It was not, as I see it, to afford the appellants an opportunity to expand the scope of the overarching case. If that is correct then arguably, no properly pleaded claim for harm of these kinds is before the court nearly six years after the data breach complained of. Nor is there a draft amendment to that effect. The draft Amended Master Particulars do not seek to advance a claim for irritation or annoyance at the way the respondent behaved.

95. I would add that it seems to me there may be room for the view that fleeting or transient subjective reactions of this nature do not qualify as "non-material damage". It is unnecessary to develop this point in any detail. I refer however to paragraphs [111]-[116] of and footnotes 64, 73, 76 to the Advocate-General's Opinion in *UI* and paragraphs [79]-[83] of and footnotes 22, 26 and 27 to the Opinion in *VB*, and the cases there cited. These can be read as advancing not only the "threshold of seriousness" argument which the Court rejected but also a contention that some forms of emotional harm do not count as "damage" at all. As I read the CJEU decisions the Court has not rejected that latter analysis. It has held that a claimant who asserts and proves harm that does fall within the concept of "non-material damage" does not need to go further, and show that the damage reaches a certain level of gravity, before compensation may be awarded.

The *Jameel* issue

96. The *Jameel* jurisdiction is well-established. A detailed exposition is contained in paragraphs [111]-[115] of the judgment below. The central proposition on which the respondent relies is captured in this passage from *Municipio de Mariana v BHP Group (UK) Ltd* [2022] EWCA Civ 951, [2022] 1 WLR 4691 [175], cited by the judge:.

> "[P]roceedings may ... be abusive if, even though they raise an arguable cause of action, they are (objectively) pointless and wasteful, in the sense that the benefits to the claimants from success [are] likely to be extremely modest and the costs to the defendants in defending the claims wholly disproportionate to that benefit"

A touchstone that has commonly been used is whether "the game is worth the candle". This is derived from a passage in the judgment of Lord Phillips MR in *Jameel.*

97. Since the judgment below, the *Jameel* jurisdiction has been reviewed by the Supreme Court. In *Mueen-Uddin v Home Secretary* [2024] UKSC 21, [2024] 3 WLR 244 [81] Lord Reed (with whom the other Justices agreed) highlighted two important points about *Jameel.* The first was that it was a libel case in which the defendant's Convention right to freedom of expression was engaged. The problem which gave rise to the need to strike out the claim was that "for the court to allow the proceedings to continue in the absence of more than minimal damage would have been incompatible with" that right. The second point was that it is not a question of simply weighing the value of the claim against the cost of the proceedings. In *Jameel* "The game was not worth the candle ... because the action could not achieve, to any significant extent, the legitimate objective of protecting the claimant's reputation". I do not think the Supreme Court was saying here that only defamation cases are amenable to *Jameel* strike-out. But it was drawing attention to some key features of the underlying rationale.

98. By the time the Judge addressed this aspect of the respondent's application he had struck out all but 14 of the claims. He considered the *Jameel* issue on the basis that the court was "no longer dealing with an unwieldy number of claimants litigating a pseudo-class action in a way that is alleged to be wholly disproportionate to the likely sums that would be achieved in compensation were the claims to succeed." Instead, he had to

consider whether it was possible to fashion a procedure for adjudicating the few remaining claims in a proportionate way.

99. Mr Sharland submitted that it is wrong to look at the claims, however many there may be, in bulk. The right approach is to concentrate on the individual claims and to ask, in each case, whether the claim is an abuse of process. Mr Sharland submitted that each of them is.

100. Mr Sharland is right on the point of principle. An individual claim is either abusive or it is not; it cannot amount to an abuse of process merely because it is linked with or brought in conjunction with one or more other claims, even if those other claims have features of abuse: see *Municipio de Mariana* [176]. But I do not think this point helps the respondent.

101. First, it brings into sharp focus the true nature of the respondent's submission. At its heart is the proposition that any stand-alone claim of the kind brought by these appellants should be dismissed without a trial even if the claimant was able to prove infringement and had sufficiently alleged a legally sustainable and factually credible case for compensation. That would be an extreme conclusion. The damages claim and the likely recovery may in many of the cases be modest. The Irish Supreme Court has said that victims of data breaches who seek compensation "solely for mental distress, upset and anxiety ... cannot expect anything other than very, very modest awards": *Dillon v Irish Life Assurance* (above) at [56]. But some of the claims in this case encompass psychiatric injury. And the modest scale of the likely recovery cannot of itself be sufficient to justify dismissal of the claim. As Lewison LJ observed in *Sullivan v Bristol Film Studios* [2012] EWCA Civ 570, [2012] EMLR 27, [29]:

> "The mere fact that a claim is small should not automatically result in the court refusing to hear it at all. If I am entitled to recover a debt of £50 .... it would be an affront to justice if my claim were simply struck out."

102. Secondly, in deciding whether any individual claim represents an abuse of its process the court must consider all the circumstances of the case. These include the issues in the case, the procedural context in which the claim is brought, and the case management powers available to the court. As Lewison LJ went on to observe in paragraph [29] of *Sullivan*, the right approach to a modest claim is to see whether there is a proportionate procedure by which its merits can be investigated. Only if that is not possible should the court adopt the last resort of striking out. The judge held that but for the issues as to liability these claims would have been apt for resolution on the County Court small claims track. I agree. It is the issues of principle the case involves that have so far provided the justification for starting and retaining these claims in the High Court. That brings with it a higher level of cost recovery. But in all the circumstances I do not think the respondent can rely on the appellants' choice of venue as a ground for striking out the claims. Nor do I consider that any of the appellants can fairly be criticised for participating in a collective action of the present kind. That approach will normally achieve savings compared to the separate pursuit of hundreds of individual claims.

103. It seems to me that the real driver of the respondent's position on this point, and the real nub of their argument, is the scale of the costs which that the appellants' legal team have run up and seek to recover in the event of success, coupled with the way the litigation has been conducted. Much was made before the judge of the figures for incurred pre-action costs and estimated costs. These are certainly very large. It was also argued that the litigation had been pursued in a disproportionate way. It was said that no sensible litigant would conduct litigation on that basis given the very modest levels of compensation at stake. Similar arguments were deployed before us. These are serious points, worthy of consideration. But I do not find either of them persuasive.

104. Notoriously, litigation of limited merit can be used as a weapon of oppression and in particular (though not only) where there is an imbalance of resources. A disproportionate approach can be a feature of such cases. Litigation with such characteristics can amount to an abuse of process especially (though not only) where the defendant's free speech rights are at stake. But it is not *Jameel* abuse. Nor was this aspect of the respondent's case developed in any sufficient detail on this appeal. For my part, I am not convinced that the appellants' conduct of the claims has involved procedural impropriety. Nor do we have evidence or reason to think there is an inequality of arms. The respondent is, to all appearances, a substantial and well-resourced corporation.

105. When it comes to the *Jameel* jurisdiction, the appellants' stated objectives are legitimate. I do not think we can say that a successful outcome would not achieve those objectives to any significant extent. On the other side of the equation it is relevant to note that this is not a case that engages (at least in any meaningful way) Article 10. Mistakenly sending the ABS to the wrong address was not in substance an exercise of the respondent's right to freedom of expression. It was essentially a commercial exercise. The respondent's key interests are purely financial. The scale of the costs incurred is partly explained by the fact that the respondent has chosen to contest issues of principle. That is the respondent's right, but the resulting expense cannot fairly be weighed in the balance against the appellants, at least at this stage. If costs have been incurred that are excessive and unreasonable in all the circumstances of the case the right response is to make appropriate costs orders. As for future expense, the issue is whether this can be kept within the bounds of reasonableness and proportionality by costs and case management. For the reasons I have given, a generic or bulk answer cannot be provided. The question of whether any individual case is abusive can be added to the question I have already identified as fit for consideration by the High Court. The answer may be influenced by how many and which claims survive the applications to strike out or for summary judgment.

106. For these reasons I would dismiss the cross-appeal on the *Jameel* issue and make orders to the effect I have already indicated.

LADY JUSTICE WHIPPLE :

107. I agree.

LADY JUSTICE KING :

108. I also agree.