Neutral Citation Number: [2023] EWHC 762 (KB)

Claim No: KB-2023-001440

**IN THE HIGH COURT OF JUSTICE**
**KING'S BENCH DIVISION**
**MEDIA AND COMMUNICATIONS LIST**

Royal Courts of Justice
Strand, London, WC2A 2LL

Dated: 31st March 2023

**BETWEEN:-**

**Armstrong Watson LLP**

**Claimant/Applicant**

**- and -**

**Person(s) Unknown**
responsible for obtaining data from the Applicant's IT systems on or about 28 February to 6 March 2023 and/or who has disclosed or is intending or threatening to disclose the information thereby obtained

**Defendant(s)/Respondent(s)**

---

**Adam Speker KC** (instructed by DAC Beachcroft LLP) for the **Claimants**
No one appeared for the Defendant/s

Hearing dates: 28 March 2023

- - - - - - - - - - - - - - - - - - - - -

**APPROVED JUDGMENT**

**Mr Justice Ritchie:**
(Sitting as the urgent applications judge)

**The Parties**

1. The Claimant is limited liability partnership who have 18 offices around the UK and are accountants, tax and business advisers.

2. The Defendants are persons unknown ("PUs").

**Bundles**

3. For the hearing I was provided with a digital bundle containing the notice of application, Claim Form, a witness statement and exhibits and a draft order. A hard copy bundle of authorities was handed up during the hearing with a skeleton argument.

**Summary**

4. These are the reasons why I granted an interim injunction at a private hearing.

5. The Claimant sought an urgent ex-parte injunction because, as is apparent from the witness statement of Paul Dickson sworn on 27.3.2023 ("Dickson"), PUs have very recently hacked the Claimant's IT system and stolen the information therein relating to their staff, their customers and their business. The information is confidential and commercially sensitive.

6. The hack became apparent when on 9.3.2023 an email was received from the PUs by a senior employee. The PUs were seeking to blackmail the Claimant company and threatening to release the information to buyers on the dark web or the world at large unless a blackmail payment was made in Bitcoin. This state of affairs is current and ongoing.

7. The PUs then sent similar emails to 499 of the Claimant's staff.

8. I will not set out in the judgment the subsequent facts because doing so would or might enfranchise or enable the PUs to further their nefarious activities.

9. There are two channels of communication open to the Claimant created by the PUs, one at an email address provided and another using a specialised browser to a website which is "off grid" so not available using normal internet browsers.

**The Issues**

10. There were several issues to be determined:
    a) Should the ex-parte application be permitted without notice?
    b) Should the hearing be held in private?
    c) Should the injunctions requested be granted?
    d) How should service be carried out?

e) Should service out of the jurisdiction be permitted?
f) The terms of the Order.
g) The return date.
h) The documents to be provided to the PUs and others.

## The applications

### Without notice and in private hearing

11. An interim remedy may be granted without notice if it appears that there are good reasons for not giving notice: CPR 25.3(1). An application must be supported by evidence, unless the Court orders otherwise, stating why the application is made without notice: CPR 25.3(2) and (3). If the application engages section 12 of the *Human Rights Act 1998* ("HRA") then by section 12(2), no relief which might affect the exercise of the Convention right to freedom of expression is to be granted unless the Court is satisfied: (a) that the applicant has taken all practicable steps to notify the respondent; or (b) that there are compelling reasons why the respondent should not be notified.

12. This application was made ex-parte so the PUs are not on notice (Dickson, paras. 29-33). The PUs have demonstrated through their communications that they have information that they know they should not have. They know that their actions are criminal, they are motivated by money and are threatening to damage the Claimant and its clients. On the evidence before me there is a real risk that notice will trigger the PUs to misuse or disseminate the confidential information before an Order is made, in an attempt to deprive this application of any substantive or practical effect. On the evidence before me I do not consider that the HRA is engaged.

13. The Courts have accepted in similar blackmail cases that it is appropriate to proceed, in the first instance, without notifying the defendant: see, for instance: *PML v Persons Unknown* [2018] EWHC 838 (QB) ('*PML*'), at para. 5; and *The Ince Group plc v Person(s) Unknown* [2022] EWHC 808 (QB) ('*Ince*'), at para. 4.

14. In addition providing notice would have given the PUs the opportunity to read what the Claimant has been doing in relation to the negotiations and investigations.

15. At the hearing I was satisfied that these were good reasons under CPR r.25.3(1) for the application to be ex-parte.

### In private

16. The Claimant did not seek anonymity. It did seek a private hearing pursuant to CPR r. 39.2(3)(a), (c), (e) and (g) and S.11 of the *Contempt of Court Act 1981*.

17. The *Practice Guidance on Non-Disclosure Orders* [2012] 1 W.L.R. 1003, at paras. 9 to 15 covers exceptions to the principle of open justice. The general rule is that hearings are carried out, and judgments and orders are made, in public. This applies to applications for interim non-disclosure orders. Derogations can only be justified in exceptional circumstances when they are strictly necessary as measures to secure the proper administration of justice. Where justified, they should be no more than strictly necessary to achieve their purpose. This Court should carefully scrutinise any application for such derogations. They should be reviewed on the return date. The leading case is *JIH v News Group Newspapers* [2011] 1 WLR 1645, CA, see paras. 19 to 25.

18. There is ample support for a private hearing on an application relating to theft of confidential information and blackmail, see: *PML*, at para. 14; *Ince* at para. 4. See also *XXX v Persons Unknown (no1)* [2022] EWHC 1578 (QB), per Chamberlain J at para. 6; and *Pendragon v Persons Unknown* [2022] EWHC 2985 (QB), per Collins Rice J, at para. 3.

19. The PUs could have raised an argument against a private hearing on the basis that it is not necessary to explore the underlying information because it was obtained through theft. The application could have been made without making reference to the content of the stolen documents, see *Imerman v Tchenguiz* [2011] Fam 116 at paras. 68-69 and 78. However, from the Dickson evidence it is clear that this is still an ongoing incident and the submissions and evidence of the Claimant encompass more than the contents of the information stolen. They include what is known to date and the steps taken to deal with the incident, so in my judgment there is a weighty need not to hamper efforts to deal with and trace the PUs or to encourage others to search for or store the information. What can legitimately come out now can be controlled better through a private hearing and the provision of this public judgment restricted to the facts necessary to explain the reasons for the Order. I consider that this route satisfies the principle of open justice whilst having proper regard to the rights of the Claimant and its clients.

**Service and territorial jurisdiction**

20. The Claimant sought a form of alternative service on the PUs, as explained in paras 24-8 of Dickson and the Order. Given that the Claimant does not know the location of the PUs, the Claimant also seeks, permission to serve the Claim Form and other documents out of the jurisdiction.

21. The Claimant does not know the identity the PUs. The Claimant knows that they exist, that they are real people and that they have provided two means of contact.

22. The Court can order alternative service of the Claim Form, Particulars of Claim and other documents under CPR rs. 6.6, 6.15, 6.27, 6.37(5)(b)(i) and (ii) and 6.38. CPR r. 6.27 explains that CPR 6.15 applies to any other document as it applies to the Claim Form.

23. The Court has the power to authorise alternative service out of the jurisdiction where there is good reason to do so, see *Abela v Baadarani* [2013] 1 WLR 2043. Under CPR r. 6.37 the Court must also be satisfied that one of the gateways contained in PD6B paragraphs 3.1(1) – (21) apply. Those require that the claim has a reasonable prospect of success, and that England and Wales is the proper place in which to bring the claim. Gateway (21) is relied on by the Claimant. That provides:

> "(21) A claim is made for breach of confidence or misuse of private information where–
> (a) detriment was suffered, or will be suffered, within the jurisdiction; or
> (b) detriment which has been, or will be, suffered results from an act committed, or likely to be committed, within the jurisdiction."

24. In *Linklaters LLP v Mellish* [2019] EWHC 177 (QB), Warby J granted an interim injunction to restrain a former employee of a large law firm from breaching his contractual duty of confidence after he threatened to disclose details of internal complaints made by women working for the firm. Although the identity of the defendant was known, his location was unknown. Warby J dealt with the issue of alternative methods of service out of the jurisdiction, for example by email, as follows:

> "20. I was satisfied that, if [the Defendant] was in France, another EU jurisdiction, service could be effected without the Court's permission, on the basis of the exclusive jurisdiction clause, pursuant to the Judgments Regulation and CPR 6.33(2)(b)(v). If, by chance, the defendant was in Australia or another non-EU country, and permission was required for service abroad, that could be granted because the claims pass through the gateways in 6BPD 3.1(6)(a), (c) and (d) (claims in relation to contracts) and, if necessary, 3.1(21)(a) and/or (b) (claims for breach of confidence or misuse of private information). The detriment threatened would be suffered within the jurisdiction. On the merits, I was satisfied that the relevant threshold requirements were met.
> 21. Given the claimants' ignorance of the defendant's whereabouts, I granted permission, pursuant to CPR 6.15 and 6.27, for service of the claim form and other documents in the case to be effected by an alternative method, namely email in combination with text messages to alert the defendant to the existence of the emails. I was satisfied that this was legitimate, notwithstanding the limits on the permissible methods of service abroad that are laid down by CPR 6.40. Email is not a method of service allowed under French law, so

> I am told. But, as Mr Caldecott pointed out, the prohibition in r 6.40(4) relates to methods of service that are "contrary to the law of the country where the claim form or other document is to be served". There is nothing to suggest that French or for that matter Australian law prohibits the service of English proceedings by email or text. And CPR 6.15 applies to authorise service "by a method or at a place not otherwise permitted" *Abela v Baadarani* [2013] UKSC 44, [2013] 1 WLR 2043 at [24]."

25. See also *Ince* at para. 17. In addition service via email on a hacker who it was thought might be outside of the jurisdiction was permitted in *PML* in which Nicklin J said at para. 18:

> "18. Included within the Injunction Order were provisions as to service of the Claim Form (amongst other documents required to be served). There is the potential in this case that the Defendant is resident in a country which would require the Court's permission to serve the Claim Form outside the Court's jurisdiction. The claim is for breach of confidence and the detriment would be suffered within the jurisdiction where the threatened publication to take place. The Defendant is also threatening to do an act (i.e. publication) that would take place within the jurisdiction. I am satisfied that England & Wales is the proper place in which to bring the claim and I have therefore granted the Claimant permission pursuant to CPR Part 6.37 and CPR Part 6 PD6B §3.1(21) to serve the Claim Form and other documents required to be served out of the jurisdiction should that prove to be necessary."

26. The Claimant is based in Carlisle. The loss and damage will be suffered in England. In my judgment these tests are met on the evidence. The breach of confidence gateway applies. The claim has a reasonable prospect of success for the reasons set out below and England and Wales is the proper place in which to bring this claim.

27. Even if the PUs are outside of this jurisdiction, once they have been validly served (with the permission of the Court) they and the companies storing the confidential information may be within the reach of the Court and may be restrained from acts both within the jurisdiction and more widely.

28. The Order contains the standard wording from the Model Order regarding the effect of the Order on persons outside of England and Wales: see para 20.

29. Service either via the website through which the Claimant has been communicating or by using the original email address used by the PUs appear to be the only realistic methods available in the circumstances of this case: see

Dickson at paras. 25-6. The PUs can, of course, challenge whether the service was valid, if they choose to identify themselves. Indeed, if that happens, service can be effected differently, if necessary.

30. The Claimant recognised its duty to continue to try to identify and locate the PUs. It has had regard to the note of caution sounded in recent Persons Unknown cases, which largely relate to harassment proceedings. The circumstances here are very different to those pertaining in that line of cases.

31. A point which may be made against the Claimant is that the injunction may not be effective in practice but there are two answers to that. Firstly, the Court does not proceed on that basis, see *Smith v Blackhouse* [2022] EWHC 3011 (KB) at para. 20, where Nicklin J cited Lord Bingham in *South Buckinghamshire District Council v Porter* [2003] 2 AC 558, at para. 32 to this effect; and secondly, it cannot be said to be so at this stage, see *PML* at para. 17.

**Service on Third Parties**

32. The Claimant is not aware of any third party who is threatening to disclose the information. It is possible that the PUs will use third parties to assist them and if this happens, or the Claimant becomes aware that the PUs are intending to do so, then Claimant will notify them of any Order made. The Claimant will also inform the Court on the return date having given an undertaking to that effect in Schedule A to the Order.

**Pleadings and cause of action**

33. The Claim Form was issued on the day of the hearing.

34. The cause of action relied upon is breach of confidence. In my judgment the economic torts of intimidation and causing loss by unlawful means may also be made out on the evidence before me. It has been held in many similar cases that extortion demands following the unlawful obtaining of a company's confidential information gives rise to a claim for breach of confidence, see *PML*, at para. 13 and *Ince*, at para. 10.

35. The foundation of the law on breach of confidence was summarised by Lord Neuberger in *Imerman v Tchenguiz* [2012] Fam 116, [2010] EWCA Civ 908, at para 55 et seq.:

> "55 The earliest cases on the topic pre-date even the days of Lord Eldon LC. However, the jurisprudence really starts with a number of his decisions and then continues throughout the 19th century. There are many reported cases but it is convenient to start with the celebrated case of *Prince Albert v Strange* (1849) 1 Mac & G 25, the facts of which are too well known to require repetition. It suffices to say that the claim was brought against various defendants who

> were involved in the copying and proposed publication of etchings of the Royal Family made by Prince Albert which, as Lord Cottenham LC put it, at p 41, had been "surreptitiously and improperly obtained".
>
> 56 Lord Cottenham LC stated the general principle as follows, at pp 44—45:
>
> > "a breach of trust, confidence, or contract, would of itself entitle the plaintiff to an injunction. The plaintiff's affidavits state the private character of the work or composition, and negative any licence or authority for publication . . . To this case no answer is made, the defendant saying only that, he did not, at the time, believe that the etchings had been improperly obtained, but not suggesting any mode by which they could have been properly obtained . . . If, then, these compositions were kept private . . . the possession of the defendant, or of his intended partner judge, must have originated in a breach of trust, confidence or contract . . . and . . . in the absence of any explanation on the part of the defendant, I am bound to assume that the possession of the etchings by the defendant or judge has its foundation in a breach of trust, confidence or contract . . . and upon this ground . . . I think the plaintiff's title to the injunction sought to be discharged, fully established."
>
> 57 He added, at pp 46—47:
>
> > "The cases referred to . . . have no application to cases in which the court exercises an original and independent jurisdiction, not for the protection of a merely legal right, but to prevent what this court considers and treats as a wrong . . . arising from a . . . breach of . . . confidence, as in the present case and the case of Mr Abernethy's lectures . . . In the present case, where privacy is the right invaded, postponing the injunction would be equivalent to denying it altogether. The interposition of this court in these cases, does not depend upon any legal right, and to be effectual, it must be immediate."
>
> 58 The relief sought against the defendants included the delivery up of all copies of the plaintiff's etchings."

36. The Claimant is the proper party to bring this application. It is entitled to sue to protect its own confidential information and also to protect information which it holds (pursuant to a contract or a duty) that is confidential to third parties, such as its clients. As Tugendhat J explained in *AVB v TDD* [2014] EWHC 1442 (QB) at para. 80:

> "An important difference between a claim in breach of confidence and a claim for misuse of private information is that a claimant suing for breach of confidence may sue in respect of information relating to third parties. The three elements of the cause of action do not include a requirement that the information relate to the claimant, and in many cases it does not. For example an employer can sue to restrain the publication of information relating to employees or customers, whether or not that information also relates to the employer. Claimants suing for misuse of private information sue in respect of information relating to themselves."

37. A duty of confidence extends to a PU who has obtained information intentionally and without authorisation: see *Imerman v Tchenguiz*, at paras. 68-69. The PUs in this case know or appreciate that the information is confidential because of the means they used to obtain it and because of the demands they are making of the Claimant to pay a ransom, see Dickson para 7.

38. I consider that the documents have the necessary quality of confidence and/or there is a reasonable expectation that all the information is confidential or private. The documents are clearly commercially sensitive. They are not publicly accessible, see Dickson paras 22-3 and that is the reason why the PUs needed to deploy improper means to obtain them, why the ransom is being demanded and why the PUs say they can be offered for sale on the dark web.

**Substantive and procedural requirements**

39. The guidance for applications for interim injunctions or non-disclosure orders is principally to be found in the following sources:
    a) CPR 25 (Interim Remedies) and PD 25A, paras 1 to 5.3;
    b) Practice Guidance (Interim Non-Disclosure Orders) [2012] 1 WLR 1003;
    c) *The Human Rights Act 1998* s. 12.

40. The application is supported by:
    a) A draft order modelled on the Model Order;
    b) The witness statement of Paul Alan Dickson with exhibits;
    c) The necessary undertakings which are required to be offered.

**The test for the non-disclosure injunction**

41. In summary, I have made prohibitory orders for the PUs not to publish or communicate the confidential information and mandatory orders for the PUs to deliver it up to the Claimant or to destroy it and to provide a witness statement evidencing delivery up or destruction and to admit any prior publication.

42. On any interim injunction application, the Court is required to apply the well-known principles in *American Cyanamid v Ethicon* [1975] AC 396, namely the balance of convenience in relation to justice between the parties.

43. In this case I am satisfied on the evidence before me that the PUs came into possession of the Claimant's confidential information through criminal and unlawful actions. They have done so for the purpose of commercial gain. They are engaged in attempting to blackmail the Claimant. They have threatened to sell or publish it. In my judgment the application plainly meets the American Cyanamid test for the need to protect the Claimant on an interim basis by a non-disclosure Order.

44. Section 12(3) of the HRA 1998, if engaged, imposes a higher test and provides that interim relief which might affect the exercise of the right to freedom of expression will only be granted before a full trial if the Court is satisfied that the Applicant is likely to establish at trial that publication of the information in question should not be allowed. "Likely" in this context means more likely than not, however, the test has some flexibility, such that if the publication of the information could cause serious damage and it is not possible for the Court in the time available to reach a decision as to the likelihood of success, an injunction may be granted for a short period of time to hold the ring until the issue can be more fully considered: *Cream Holdings v Banerjee* [2005] 1 AC 253 at para. 22; *ABC (Sir Philip Green) v Telegraph Media Group Ltd* [2019] EMLR 5 at para. 11 to 17, CA.

45. On the evidence before me, the PUs are not seeking to exercise any justifiable rights to freedom of expression or to use the information for the purposes of legitimate public discourse. In such circumstances, I do not consider that article 10 is engaged, see, *Ince* at para. 8 and *XXX v Persons Unknown (no1)* [2022] EWHC 1678 (QB), at para. 17. In any event, if it was engaged, again as found in *Ince* and *XXX*, I am satisfied that the Claimant has comfortably met the higher s12(3) test, on the facts.

**The delivery up injunction**

46. Paragraphs 8 and 9 of the Order are the mandatory provisions and require the PUs to deliver up and/or delete and/or destroy the confidential information which they have stolen or obtained and to provide a witness statement confirming the same. In *Imerman v Tchenguiz* [2011] Fam 116, at para. 73 the Lord Neuberger said:

> "73 An injunction to restrain passing on, or using, the information, would seem to be self-evidently appropriate-always subject to any good reason to the contrary on the facts of the case. If the defendant has taken the documents, there can almost always be no question but that he must return them: they are the claimant's property. If the defendant makes paper or electronic copies, the copies should be ordered to be returned or destroyed (again in the absence of good reason otherwise). Without such an order, the information would still be "out there" in the possession of someone who should not

> have it. The value of the actual paper on which any copying has been made will be tiny, and, where the copy is electronic, the value of the device on which the material is stored will often also be tiny, or, where it is not, the information (and any associated metadata) can be deleted and the device returned."

47. The principles to be applied for granting mandatory injunctions under S.37 of the *Supreme Courts Act 1981* are those summarised in *Nottingham Building Society v Eurodynamics Systems* [1993] F.S.R. 468 by Chadwick J:

> "In my view the principles to be applied are these. First, this being an interlocutory matter, the overriding consideration is which course is likely to involve the least risk of injustice if it turns out to be "wrong" in the sense described by Hoffmann J.
> Secondly, in considering whether to grant a mandatory injunction, the court must keep in mind that an order which requires a party to take some positive step at an interlocutory stage, may well carry a greater risk of injustice if it turns out to have been wrongly made than an order which merely prohibits action, thereby preserving the status quo.
> Thirdly, it is legitimate, where a mandatory injunction is sought, to consider whether the court does feel a high degree of assurance that the plaintiff will be able to establish his right at a trial. That is because the greater the degree of assurance the plaintiff will ultimately establish his right, the less will be the risk of injustice if the injunction is granted.
> But, finally, even where the court is unable to feel any high degree of assurance that the plaintiff will establish his right, there may still be circumstances in which it is appropriate to grant a mandatory injunction at an interlocutory stage. Those circumstances will exist where the risk of injustice if this injunction is refused sufficiently outweigh the risk of injustice if it is granted."

48. I also take into account the guidance given by Jack J in *Tullett Orebin v BGC Brokers* [2009] EWHC 819, about orders to try to undo the harm unlawfully done and to support the injunction. Given what the PUs have threatened in their messages, I consider that there is a high degree of assurance that an order of this kind would be made at trial. There is no basis for the PUs to resist the relief sought on the evidence before me or reasonably to be anticipated.

**Self-identification**

49. The Court has the power to order that a defendant whose actions appear to be unlawful and whose identity is not known must identify himself, see *PML*, at para. 17:

> "Where a defendant in a case of threatened unlawful publication hides behind anonymity, the Court has the power to include within the injunction order a requirement that s/he identify him/herself and provide an address for service ("a self identification order"). Once a claimant has satisfied the Court that s/he is likely to demonstrate that publication should not be allowed, that may well justify the Court making a self- identification order. Such an order is necessary if, in the event of success in the claim, the remedies to which the claimant would be entitled are to be effective. In my judgment there is no rational basis on which any PU could resist the relief sought under this part of the Order."

**Possible defences or justifications**

50. The PUs have threatened that they will disclose the information if the ransom demanded is not paid. I consider that it is established that there is a prima facie breach of confidence so it is necessary to have regard to whether article 10 of the HRA 1998 is engaged and, if so, the strength of that right on the present facts or any other arguable just cause or excuse. The information is not in the public domain according to Dickson at para. 23. Nor is there a public interest in disclosing all or any of the information, see *LJY v Person(s) Unknown* [2017] EWHC 3230 (QB), [2018] EMLR 19, in which Warby J said at paras. 28 to 30:

> "Blackmail is defined by s.21(1) of the Theft Act 1968 : "A person is guilty of blackmail if, with a view to gain for himself or another …he makes any unwarranted demand with menaces". The subsection goes on to explain that "a demand with menaces is unwarranted unless the person making it does so in the belief – (a) that he has reasonable grounds for making the demand; and (b) that the use of the menaces is a proper means of reinforcing the demand."

51. In my judgment blackmail represents a non-use or a misuse of free speech rights. Such conduct will considerably reduce or abolish the weight attached to the right to free speech, and correspondingly increase the weight of the arguments in favour of restraint. Courts recognise the need to ensure that no encouragement or help is provided to blackmailers, and no deterrence is imposed on victims of blackmail from seeking justice before the Court. All these points were recognised in *YXB* at para. 17. It can properly be said that the grant of a privacy injunction to block a blackmail serves the additional legitimate aim of preventing crime.

52. I consider that damages are not an adequate remedy in a case of this kind, see *Ince* at para. 10. The purpose of the injunction is to try to prevent the Applicant's confidential information from being leaked when such could cause irreparable or serious damage to the business in financial ways and other ways.

**Access by PUs and others to hearing papers**

53. The Claimant sought to place restrictions on (1) the service of certain information and documents on the PUs at this stage and (2) on the dissemination of and access to the hearing papers to and by third parties.

54. In relation to the Defendant, the Order includes provision at para. 5 that certain documents are not, at this stage, served on the PUs. The provisions in CPR r. 25APD, para 5.1(2) require that an applicant on a without notice application must undertake to serve the respondent with the application notice, evidence in support and any order made as soon as practicable. However, the Claimant sought an order in the form first made in *Clarkson PLC v Persons Unknown* [2018] EWHC 417 (QB), and then followed in extortion cases. The Claimant does not wish to serve the confidential witness statement on PUs unless and until the PUs identify themselves and provide addresses for service. This was the way forward used in *Ince* at para. 14. If the PUs identify themselves properly, they should (probably, but depending on the facts) be provided with all documents put before the Court.

55. In the interim, because the identity of the PUs is unknown and they are blackmailing and threatening to harm the Claimant, to send the evidence relied upon to them may lead to misuse of the evidence, or the confidential information or it could provide the PUs with valuable information to further their nefarious ends.

**Third parties**

56. Regarding access to documents by third parties, the restrictions sought are in a slightly modified form to the standard wording in the Practice Guidance, see the Order at paras. 24-28. These revisions were accepted in previous similar cases, *Ince*, para. 15 and *XXX (no1)*, para. 12. The Order (without the confidential schedule) will be accessible to anyone searching the Court file and may be published on the Judiciary Website, see CPR r. 39.2(5).

57. The wording in the model draft Order (which preceded CPR r. 39.2(5)) is largely premised upon protecting the rights of the media and would allow anyone who had notice of the Order to receive a copy of the documents read by the Judge provided they gave an irrevocable written undertaking. Yet in this case such people would not necessarily have a legitimate interest in receiving the documentation or have any justification or standing to apply to vary or discharge the Order.

58. Therefore, it was proposed and allowed with the Court's approval, to include the wording that third parties: *'must be in possession of, or the Claimant knows or believes are in the possession of, the Information'.* This wording fitted with paragraph 19 of the Master of the Rolls' Practice Guidance: Interim Non-Disclosure Orders which reads as follows:

> "HRA s12(2) applies in respect of both (a) respondents to the proceedings and (b) any non-parties who are to be served with or otherwise notified of the order, because they have an existing interest in the information which is to be protected by an injunction (*X & Y v Persons Unknown* [2007] EMLR 290 at [10] – [12]). Both respondents and any non-parties to be served with the order are therefore entitled to advance notice of the application hearing and should be served with a copy of the Application Notice and any supporting documentation before that hearing."

59. If a party does not have knowledge of or access to the information which is protected and therefore has no existing interest in it, it was submitted that he should not be entitled to the documents put before the Court, particularly at a private hearing, even if he were willing to provide a written undertaking. I am not at all sure that I would go that far in other cases but I do consider that this is appropriate in this case.

60. Those who would or might have an existing interest (e.g. Internet Service Providers), should be provided with the documents provided they give an irrevocable written undertaking and are within the jurisdiction and can be subject to the contempt jurisdiction.

**Conclusions**

61. For the above reasons I granted the injunctive Order made on 28.3.2023.

END