Neutral Citation Number: [2024] EWHC 2127 (KB)

Case No: KB-2024-002288

IN THE HIGH COURT OF JUSTICE
KING'S BENCH DIVISION

Royal Courts of Justice
Strand, London, WC2A 2LL

Date: 15/08/2024

Before :

Mrs Justice Stacey

- -

Between :

SYNNOVIS SERVICES LLP	**Claimant**
- and -	
PERSON(S) UNKNOWN	**Defendant(s)**

- -
- -

Adam Wolanski KC & Ben Hamer (instructed by **Mills & Reeve LLP**) for the Claimant
No representation and no appearance
Hearing date: 12th July 2024

- -

Approved Judgment

This judgment was handed down remotely at 10.30am on 15th August 2024 by circulation to the parties or their representatives by e-mail and by release to the National Archives.

.....

MRS JUSTICE STACEY

Mrs Justice Stacey :

1. The claimant seeks an in private hearing for its application for an urgent, without notice, interim injunction against the defendant or defendants whose identities are not known who are responsible for engaging in a cyber attack on the claimant's IT systems. The claimant is part of a pathology partnership with SYNLAB and part of its business is to provide laboratory services to two London based hospital trusts – Guy's and St Thomas' NHS Foundations Trust ("Guy's") and King's College Hospitals Foundation Trust ("King's").

2. On 3 June 2024 a cyber attack on the claimant's IT systems took place and the defendant(s) left a ransom note on the system. The claimant released a public update the next day on 4 June 2024 explaining that it had been the victim of a ransomware cyberattack affecting all its systems resulting in interruptions to many of its pathology services. and a further update on 17 June 2024 informing of the continuing problems and delays in providing its services and the work being undertaken to restoring services as quickly as possible.

3. On 19 June the ransomware gang, Qilin, spoke to the BBC and took responsibility for the attack and the BBC published an article stating that Qilin are a well known ransomware gang who have carried out criminal hacks for extortion purposes of a range of public and private services and companies since 2022. Some data from the cyber-attack was published via Telegram on 20 June 2024. Telegram is a could-based messaging service. On 21 June 2024 the MailOnline published an article stating that the ransomware attackers had obtained confidential information of medical conditions and blood test results of more than 100,000 patients. Much of the information and data obtained by the defendant(s) is confidential as it is commercially sensitive, private and is the confidential medical records of patients served Guy's and King's ("the information").

4. The claimant released further public updates about the cyber attack on 21 and 24 June 2023 again seeking to reassure the public as best as possible. The BBC published a further article on 24 June 2024 about the cyber attack with similar information to that contained in the MailOnline article. On 27 June 2024 there was a post of information and statement published on a website called "Wikileaksv2".

5. The Claimant emailed Telegram requesting the Telegram Information be taken down on 2 July at 11.55am. No response has been received. On 10 July 2024 the clamant notified Telegram that it would seek an urgent injunction in the Royal Courts of Justice on 12 July 2024, asking if it intended to make any representations or if it required any further information. Once again no response has been received.

6. The claimant also emailed Wikileaksv2 at abuse@nicenic.net asking for the information published on a website bearing that name be taken down from their platform. After initially receiving an auto-response in acknowledgement there was a substantive reply on 6 July 2024 stating that the domain name was not available in their system. The claimant believes that Wikileaksv2 is suspicious as a clone site and may be an offshoot of the defendant(s) organisation and did not inform them of their intention to seek this injunction.

7. The defendant(s) identity is not known, but they have invited communication to an email address. The defendant(s) do not have permission or lawful authority to obtain the claimant's data and information on its servers. The claimant has drafted and issued a claim form setting out its cause of action as breach of confidence. It has undertaken to serve it by 19 July 2024. It seeks three remedies: a non-disclosure order, an unmasking order and an order for delivery up and destruction of the information and material obtained in breach of confidence.

8. Today's application is for an order pursuant to CPR 25.1(1)(a) granting an interim injunction preventing the release or publication of data stolen from the claimant during the ransomware cyber incident which occurred on or around 3 June 2024 and prohibiting further attempted cyber attacks and orders for derogation from open justice.

9. I have read the skeleton argument, bundle served in support including the confidential witness statement of UGX and the bundle of authorities, most particularly, *Armstrong Watson v Persons Unknown* [2023] EWHC 762 KB.

10. I am satisfied that the claimant has addressed points that might have been raised by the defendants had they been present and represented.

11. Dealing with the matters in turn.

12. Holding this hearing in private requires a derogation form the open justice principle see CPR 39.2(3)(a), (c), (e) and (g) and s. 11 Contempt of Court Act 1981.

13. I am satisfied that exceptional circumstances apply and it is strictly necessary for the hearing to be held in private to secure the proper administration of justice. A private hearing is no more than is strictly necessary. The reason is obvious: this application relates to the theft of confidential, highly personal medical information, some of which has already been disclosed in a limited way and there is an ever present threat of further or more widespread disclosure. It is an ongoing and fast moving incident. Without a private hearing it will not be possible to ventilate the issues and discuss the evidence to enable a just decision to be reached: see *Armstrong* @ [19], the same reasoning applies here. The claimant does not seek anonymity, merely for this hearing to be held in private.

14. Next, the without notice application. The default position is that any party to proceedings is entitled to be on notice and able to appear and be represented at any hearing in which his interests may be affected. However an interim remedy may be granted without notice if there are good reasons for not giving notice (CPR 25.3(1)). In this case the procedural requirements have been satisfied. S.12 Human Rights Act 1998 ("HRA 1998") is engaged since the relief sought may affect the exercise of the ECHR right to freedom of expressions. By s.12(2)(b) the court must be satisfied that there are compelling reasons why the defendant should not be notified. I find that there are bot good and compelling reasons why the hearing should take place without notice. On the evidence before me there is a real risk that further unauthorised, damaging disclosures would be made if the defendants were on notice of this application. The obtaining of the data and its dissemination are prima facie criminal acts – theft and blackmail as well as the tort of confidence.

15. I proceeded to hear the application in private and without notice to the defendant(s). The appropriate and necessary undertakings were provided by the claimant as set out in the draft order and as per the witness statement of UGX, as to pay damages, to serve documents put before the court (subject to the modifications as set out in the draft order) and for a suitable return date. The claimant had recognises its obligations as to full and frank disclosure to the court. I have considered, and accept, that it is strictly necessary for the contents of UGX witness statement and its exhibits should not be provided to a non party without further order of the court. Any non-party other that a person notified or served with the order seeking access to, or copies of the witness statement and exhibits of UGX, must apply to the court, on notice to the claimant and any defendant(s) that comply with this order. Should the defendant(s) identify themselves and provide an address for service they must be provided with all the documents put before the court.

16. The injunction sought is to restrict the defendant from using, publishing, communicating or disclosing the confidential information; requiring him, it or them from using, publishing or disclosing the confidential information; to require the delivery up and/or deletion and/or destruction of the confidential information in its possession, custody or control (and provide a witness statement explaining this and giving details of any disclosure to third parties); and to provide their full names and addresses for service.

17. Applying the principles in *American Cyanamid v Ethicon* [1975] AC 396 and s, 12(3) HRA 1998, I remind myself 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 [22].

18. The defendant(s) have come into possession of the claimant's confidential information or property through criminal and unlawful actions. It has done so for the purpose of commercial gain. It is engaging in extortion. The claimant has established that publication of the information should not be allowed and that its use should be restricted. It has also established that it is entitled the mandatory delivery up injunction in the terms sought which are reasonable and proportionate (See *Armstrong Watson* @ [46]-[48]). I am also satisfied that the defendant(s) must identify themselves – their actions appear unlawful and they it appears that they are seeking to hide their identity behind a cloak of anonymity and an organisation, Qilin, which has no legal identity (see Armstong @ [49] and *PML v Persons Unknown* [2018] EWHC 838 (QB) @ [17]. There is no rational basis on which the defendant(s) could resist the relief sought under this part of the order.

19. The proposed order also includes a prohibition preventing further unauthorised access of the claimant's IT systems by the defendant(s) – a so-called anti-hacking injunction. This is plainly desirable and the objective is to prevent further cyber-attacks. It is plainly just and convenient to make such an order in the terms sought using the High

Court's broad discretionary power to grant an interim or final injunction set out in s.37(1) of the Senior Courts Act 1981, "in all cases in which it appears to the court to be just and convenient to do so". I grant the order.

20. I have considered the possible defences or justifications that a defendant might have made had they been present and represented. The defendant(s) have threatened to disclose information if a ransom is not paid, establishing a prima facie breach of confidence. The information is not in the public domain – it is still and remains confidential – and there is no public interest in its disclosure any of it. (see *LJY v Person(s) Unknown* [2017] EHC 3230 (QB) at [28]-[30]. Damages are not an adequate remedy after the horse has bolted. Should it be said that the defendant(s) may not be minded to comply with the order and it may not have the intended effect, this argument was rejected in *Armstrong Watson @* [31] and for the same reasons would not be a successful argument in this case.

21. **Service and territorial jurisdiction**. It is not possible for the claimant to know where the defendant(s) are based or located or where the contact address provided by the defendant(s) is based. I am satisfied that they have taken in the time available and are continuing to take reasonable steps to find out. The claimant seeks an order for alternative service via the email address provided by the defendant(s) to the claimant to communicate with them. Since that is the address that the defendant(s) have provided I am satisfied that the order and proceedings will reach them if they are served by this method, and that the conditions stipulated in CPR 6.6, 6.15, 6.27, 6.37(5)(b)(i) and (ii) and 6.38 are satisfied and by CPR 6.27, CPR 6.15 applies not just to the claim form, but other documents. It is the only realistic method available in the circumstances of this case. Once the defendant(s) comply with the order and unmask themselves, service can be effected differently, if necessary (*Armstrong* [29]).

22. Service by the alternative method I have allowed may mean that service is out of the jurisdiction. I am satisfied that the tests and body of case law helpfully summarised in *Armstrong Watson @* [20] – [31] for service out of the jurisdiction is met. The breach of confidence gateway applies; the claim has a reasonable prospect of success; and England and Wales is the proper place in which to bring this claim. The claimant is based in England. Even if the defendant(s) is or are outside of this jurisdiction, once they have been validly served they will be within the reach of the Court and may be restrained from acts both within the jurisdiction and more widely: See Injunctions (14th edn) at 4-50 citing Re *J (a child)* [2013] EWHC 2694 (Fam) and *In re Liddell's Settlement Trusts* [1936] Ch 365.

23. The claimant intends to serve the order on Telegram and Wikileaksv2 in light of their knowledge of some of the confidential information. Both have been served and not agreed to comply with take down letters, beyond a Hong Kong based intermediary, the host of Wikileaksv2, stating that the "domain name is not available in our system." Telegram is on notice of today's application and have not responded. The fact that the domain name provided for Wikileaksv2 was not available in the Wikileaks system corroborates the claimant's fear that it is a clone site under the control of the defendant(s) and I agree that in those circumstances they were entitled not to put Wikileaksv2 on notice of the application. Paragraph 21 of the draft order is granted.

24. I also allow for NHS England and/or any other person who is a data controller of the data in the confidential information may apply to the court to be joined as an additional claimant, if so advised, on less than 3 days notice if necessary, for the purposes of enforcing or seeking variations to the order or seeking further orders on the case.

25. We have discussed and I have amended some of the proposed wording in the draft order during the course of this hearing which is reflected in the final order. The return date was set at 30 July 2024.