Judgments

PML v Person(s) Unknown (responsible for demanding money from the claimant on 27 February 2018)

[2018] EWHC 838 (QB)

Queen's Bench Division

Nicklin J

17 April 2018

Judgment

Adam Speker (instructed by **Taylor Wessing LLP**) for the **Claimant**

The Defendant(s) did not attend and was not represented

Hearing date: 11 April 2018

- -

Judgment Approved

The Honourable Mr Justice Nicklin :

1. This is another blackmail case in the Media & Communications List. PML is a UK company. In February 2018, its computers were secretly hacked and a very large quantity of data stolen. On 27 February 2018, the Defendant sent an email to three directors of the Claimant. Its terms were unsubtle and unambiguous:

"As an Executive Director you should know that your company's servers are hacked. All the information from your servers – documents… databases, reports client's databases, private documents, internal workflow, all correspondence in fine (sic) ALL the DATA has been copied, safely hidden and well protected. Proofs of my words attached below (some files which I could

not ever possibly have)…

[details of a website which was hosting the stolen document was provided together with the login and password details (“the Cache Website”)]

I offer you a simple deal. All future business of the company depends upon this deal, as a result. You know, you have two ways:

(1) To pay. I delete all the data. I'll also explain how to prevent such attacks in future to be safe and we forget about each other, forever.

(2) Not to pay. And in this case, I publish all information in public. I think you will understand what happens next: the shares of the company will collapse; the company's credibility will be undermined; all contracts, documents, databases and all internal correspondence of the company – everything is going to be public. I can arrange it, no doubt. It's going to be the dead end for the reputation of your company.

There are simply no other ways. I won't be looking for any private buyer who can also pay me for this information. I don't need that. I will never contact you again, because I'll delete all the information, so you either pay me or the data goes in total public access.

As for guarantees, I act as a private person and money is all I interested in (sic). As soon as I receive money, I will delete the data and forget about your company, as I said, I don't care about it. So, you'll never hear from me again. I will not try to resell the data, because it's very dangerous and may end badly for me, as a result.

Here are the terms:

The cost is 300,000 (three hundred thousand Great British Pounds) paid via Bitcoin money system. Deadline – 2 weeks. (The term is based on life experience. It is enough time to verify that the data is really mine, hold meetings and/or consult regarding this matter (if necessary) and finally buy enough Bitcoin coins). In 2 weeks time, if I won't receive the money (sic) I post the data in public access (available for anyone in the world), as it is written below. I can't accept a delay if there's no VERY reasonable cause.

P.S.

1) Please do not try to close the server with the data, it's just a mirror, as a proxy, it will not help you. Data is securely archived, hidden and protected.

2) Please do not make any noise; any appeal to the police, the Europol or anything else will cause an immediate publication of ALL the Information.

I will explain how it will look like.

[details are given of how the Defendant threatened to release the Claimant's data via various forums and portals, week by week]

3) So, please, do not pretend that I do not exist, do not ignore me or break the deadlines. It will simply cause the publication of all the information. You will also incur huge losses and I will go further.

4) Nothing personal – just business…

Best regards. [name redacted]"

2. The email attached a selection of different documents which appeared to have come from the Claimant's computer systems. The Claimant's investigations established that someone had hacked into the Claimant's servers and extracted information and data. The threat in the email appeared to be genuine.

3. The Claimant reported the matter to the police immediately. Their investigations are ongoing.

4. Email communications between the Claimant and the Defendant continued through early March. In summary, the Claimant had no intention of paying the sum demanded but, by requesting extensions of the deadline and assurances as to the promise to delete the data if the money was paid, kept the Defendant engaged. After the expiry of one of the revised deadlines, the Defendant increased the sum he demanded to £350,000. The Defendant also threatened to start looking for buyers for the stolen data. He did, however, offer to accept payment in instalments.

5. On 21 March 2018, the Claimant applied to the Court, without notice to the Defendant, for an interim non-disclosure order to restrain the threatened breach of confidence and for delivery-up and/or destruction of the stolen data. The application came before Bryan J as interim applications Judge. The Judge sat in private, granted the injunction and made a series of further orders including anonymising the Claimant and restricting access to the Court file ("the Injunction Order"). Bryan J gave an *extempore* judgment. He was satisfied that the requirements of s.12(3) Human Rights Act 1998 were met (i.e. that the Claimant was likely to demonstrate at trial that publication of the stolen documents would not be allowed). He was also satisfied that under s.12(2) the fact that the Claimant appeared to be a victim of blackmail and that there was a risk that, were the Defendant to be given notice of the application, he would publish the information, were compelling reasons why the Defendant had not been notified. Finally, the Judge was satisfied that the Claimant, as an apparent victim of blackmail, ought to be anonymised (***ZAM -v- CFM and TFW*** **[2013] EWHC 662 (QB)** [39]-[41] and [44] *per* Tugendhat J; ***LJY -v- Person(s) unknown*** **[2017] EWHC 3230 (QB)** [2] *per* Warby J). The injunction was granted until a return day fixed for 11 April 2018.

6. The Injunction Order was served on the Defendant at 11am on 23 March 2018 using the only method available, the email account from which he had been corresponding with the Claimant. The Defendant replied at 11.09, defiantly: "*you made [your] choice, I make my own. On Monday the information will be published. Good luck*". At 14.06 he emailed to state that he had removed the password protection on the Cache Website thereby allowing them to be

accessed by any user of the Internet who had the website address. At 14.30 he stated that he intended to email customers of the Claimant on Monday (presumably having harvested their email addresses from the stolen data) and added: "*shares of your company will collapse all developments will be revealed you will be an excellent example to my next customers*".

7. Separately, having established that the Cache Website was hosted by a company in another European jurisdiction ("the European Server"), the Claimant applied for and obtained an order from a Court in that jurisdiction directed at the European Server requiring it to block access to the Cache Website ("the European Order"). This order was served on the European Server at the same time as the Injunction Order was served on the Defendant. Complying with the European Order, the European Server blocked access to the Cache Website at some point in the afternoon on 23 March 2018.

8. The following morning, the Defendant emailed the Claimant: "*why did you block the proxy. I wrote that it does not make sense all the information is kept by me. On Monday, I will send you new links*…" On 26 March 2018, the Defendant renewed his threat that he was looking for buyers for the stolen data. On 27 March 2018, he told the Claimant that he had set up another website to host the documents and that this was not password protected and said: "*Do you understand that this is the end? You have a little more time to get in touch with me and start a dialogue.*"

9. As a result of their own investigations, between 23-26 March 2018 the Claimant was able to identify further websites hosting the stolen documents. The hosting companies blocked access to the documents or deleted them following service of the Injunction Order.

10. On 27 March 2018, the Claimant became aware of postings on a financial forum which referred to the Claimant and contained links to another website hosting the documents. The relevant posts also included file names of several stolen documents. On the assumption that these postings were made by the Defendant, prima facie those actions were in breach of the Injunction Order. The Claimant served the Order on the company hosting the financial forum and the relevant posts were removed. The operators of the website hosting the documents themselves also removed them, on 29 March 2018, after being contacted by the Claimant's solicitors.

11. On 9 April 2018, the Defendant made further threats of publication of the stolen data but reduced the asking price to £100,000. By the time of the hearing on 11 April 2018, no further communication had been received from the Defendant.

Application for a continuation of the Injunction Order

12. In compliance with undertakings given to Bryan J, the Claimant issued a Claim Form on 22 March 2018. Particulars of Claim were served on 9 April 2018. On 23 March 2018, the Claimant issued an Application Notice seeking the continuation of the Injunction Order until trial. A draft of the order sought was served on 9 April 2018.

13. The Claimant seeks the continuation of the Injunction Order. I granted that application. Little has changed since the Injunction Order was granted by Bryan J. The Defendant has continued to threaten to publish the stolen data unless he is paid a substantial sum of money.

Indeed, as set out in Paragraph 10 above, it appears that the Defendant has tried to publish some of the data. I am quite satisfied therefore that there is a continuing threat to publish the stolen documents in breach of confidence. Bryan J was satisfied, as I am, that the Claimant is likely to demonstrate at trial that the circumstances in which the Defendant came to be in possession of the relevant documents and information (i.e. by computer hacking) imposes an obligation of confidence on the Defendant (***Tchenguiz -v- Imerman*** **[2011] Fam 116** [69]). Unsurprisingly in the circumstances, the Defendant has not suggested that there is any public interest that could justify his threatened (or actual) publications. I am satisfied therefore that the Claimant is likely to establish at trial that publication of the stolen data should not be allowed. The Defendant's failure to deliver up or delete the stolen data (a) is a further prima facie breach of the Injunction Order; but (b) justifies the continuation of that order.

Hearing in private, anonymity and restrictions on access to the court file

14. I was satisfied that it was strictly necessary to hear the application in private pursuant to CPR Part 39.3(a), (c) and (g). There is a powerful (if not overwhelming) case that this Defendant is blackmailing the Claimant. Police investigations were underway and at the hearing I had necessarily to hear evidence and submissions relating to the activities of the Defendant and the data that was stolen. The purpose of these proceedings would have been frustrated (or at least harmed) had the hearing been conducted in public. Largely, this public judgment sets out as full an explanation as I can give of the underlying facts and the reasons for the Court's decision. That mitigates, at least in part, the derogation from the principle of open justice that the Court sitting in private represents.

15. I am also satisfied that the Claimant should continue to be anonymised in these proceedings for the same reasons as Bryan J gave (see Paragraph 5 above); the Claimant is a victim of blackmail.

16. The order restricting access to certain documents on the Court file continues to be necessary in order not to defeat the injunction and anonymity order.

Order requiring the Defendant to identify himself and an address for service and service out of the jurisdiction

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. Of course, a defendant may disobey the Court's order and not comply with a self-identification order as well as the non-disclosure order. But it cannot be assumed that all defendants will choose defiance. Few defendants can remain confident that they will ultimately manage to evade identification. If they fail, punishment for contempt of court would then loom large. I have recent experience in ***NPV -v- QEL & Another*** **[2018] EWHC 703 (QB)** (another blackmail case) in which a self-identification order was made against the (anonymous) Second Defendant. The Second Defendant complied with the order and provided his name and address for service.

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 were 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.

19. I have made further ancillary orders including service of a Defence. There is a clear risk that the Defendant will refuse to participate in the proceedings. To ensure that an interim non-disclosure order is not left in near permanent suspension, the order includes the usual direction that, in the event that the Defendant does not file a Defence, the Claimant must take steps to conclude the action whether by applying for default and/or summary judgment by a particular date, in this case by 23 May 2018.