Neutral Citation Number: [2023] EWHC 425 (KB)

Case No: QB-2022-000181

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

Royal Courts of Justice
Strand, London, WC2A 2LL

Date: 28/02/2023

**Before** :

**MR JUSTICE LAVENDER**

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

**Between :**

| | |
|---|---|
| **GLOBAL PROCESSING SERVICES (UK) LIMITED** | **Claimant** |
| **- and -** | |
| **(1) VLADIMIR YANPOLSKY**<br>**(2) ALLA YANPOLSKY** | **Defendants** |

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

**Guy Vassall-Adams KC and Kirsten Sjøvoll** (instructed by **Orrick, Herrington & Sutcliffe (UK) LLP**) for the **Claimant**
**Gervase de Wilde** (instructed by **Brett Wilson LLP**) for the **Defendants**

Hearing dates: 3 November 2022

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

# Approved Judgment

.....

MR JUSTICE LAVENDER

**Mr Justice Lavender :**

## (1) Introduction

1. The Claimant applies for summary judgment against the Defendants on its claim for breach of confidence. The hearing was held in public, but, since it was concerned with the alleged unlawful use and disclosure of confidential information, the parties took care not to disclose any of the information which is the subject matter of the claim and the Claimant invited me to make an order restricting access to the court files, so that non-parties may only have access to the underlying evidence with the permission of the court. I will make such an order.

## (2) Background

### *(2)(a) The Parties and the Cyber-Attack*

2. The Claimant is a technology service provider in the financial payments processing sector and provides payments services to a range of clients, using a platform which works with various payment card schemes, including Visa and Mastercard. The First Defendant worked for the Claimant as its Chief Technical Officer from 18 August 2014 until his resignation on 6 January 2017. On 5 March 2017 there was a cyber-attack against the Claimant's information technology systems, which caused a system failure and put the Claimant's business out of operation for about 12 hours

3. The Claimant blamed the First Defendant for the cyber-attack and he was arrested on 8 March 2017 and subsequently charged with an offence under the Computer Misuse Act 1990. The First Defendant pleaded not guilty and continues to assert his innocence, but he was convicted at trial on 22 January 2020 and sentenced to 3 years and 6 months' imprisonment. He remained in prison until 21 May 2021. He has not applied for permission to appeal against his conviction. Any application which he now made would require an order from the Court of Appeal extending the time limited for filing a notice of appeal, which expired 28 days after his conviction, i.e. on 19 February 2020.

### *(2)(b) The Exhibit and the Disclosed Data*

4. Prior to the trial, the Crown Prosecution Service ("the CPS") served Exhibit LHG/04 on the First Defendant, by sending it to his solicitors in electronic form. It was an exhibit to a witness statement made by Lisa Grahame, an employee of the Claimant. The First Defendant's solicitors then provided it to him. Further versions of this exhibit were disclosed, but nothing turns on any differences between the different versions, and I will refer to them simply as "the Exhibit".

5. The reason for the disclosure of the Exhibit was that the First Defendant had alleged that the Claimant had tampered with the logging information collected by the Claimant's information technology systems, which was relied on as part of the evidence against the First Defendant in order to show who had logged into the Claimant's systems and who, therefore, could have been responsible for the cyber-attack.

6. The Exhibit contained over 11 gigabytes of data from the Claimant's computer system. If printed out, this would amount to over 7 million pages. I will refer to the contents of the Exhibit as "the Disclosed Data". It included some data in "tokenised" form, i.e. data, such as a 16-digit credit card number, which had been converted into a random string of characters, known as a "token", using a database, known as the "token vault", which stores the relationship between the original data and the token. It appears, and the contrary was certainly not suggested, that tokenised data would be of no use to anyone to whom the Disclosed Data was disclosed. However, as will appear from the emails to which I will refer, the Defendants were able to extract from the Disclosed Data the names and contact details of individual cardholders, as well as their credit card numbers, expiry dates, PINs and CVV2 numbers.

7. The First Defendant referred to the Exhibit in an amended defence statement dated 15 August 2018, when he said that the Exhibit:

> "… contains abundance of 16-digits card numbers, card holder full names and addresses, and 4-digits clear PINs as examples of the type of information that a 'hacker' might seek."

8. However, no part of the Exhibit was read out at the First Defendant's trial and there was no evidence before me as to whether or not the First Defendant's counsel advanced at trial the First Defendant's contention that the presence of real, rather than tokenised, credit card numbers in the Exhibit was an indication that the cyber-attack might have been the work of a hacker.

### *(2)(c) The Alleged Breaches, or Threatened Breaches, of Confidence*

9. The Claimant complains of 13 emails sent by one or other of the Defendants in the period from February to November 2021 as constituting either the unlawful misuse and/or disclosure of confidential information contained in the Disclosed Data or threats to misuse and/or disclose confidential information contained in the Disclosed Data.

10. In those emails, the Defendants repeatedly asserted that there had been a data breach when the Exhibit was provided to the First Defendant, who says in his witness statement that he was concerned that the Claimant had not properly notified relevant parties about the cyber-attack and that this might point to the Claimant having covered up other evidence which he believed might assist his case. Unsurprisingly, Mr De Wilde did not submit that the assertion that there had been a data breach was correct. Indeed, he acknowledged that the Defendants were misguided in this respect.

11. The first time this assertion was made in the emails which I have seen was in emails which the Second Defendant sent on 8 July 2020, at the request of the First Defendant, to data protection officers in: (a) the CPS; and (b) the Metropolitan Police. In her email to the Metropolitan Police she complained that there had been a data breach: (1) when the Exhibit was first sent to the First Defendant; (2) when subsequent versions of the Exhibit were sent to the First Defendant; and (3) curiously, when the First Defendant referred to the Exhibit in his additional defence statement. She asked what actions the Metropolitan Police had taken to comply with their obligations under the Data Protection Act 2018 and how the Metropolitan Police had

notified the Information Commissioner's Office ("the ICO") and relevant cardholders and financial institutions.

12. In August 2020 the Second Defendant made a complaint (which I have not seen) to the ICO about the CPS. It seems that she also made a complaint to the Financial Conduct Authority ("the FCA").

13. The First Defendant claims in his witness statement that he believed that investigations into the alleged data breach by the Metropolitan Police, the CPS and the ICO might turn up fresh evidence which might assist him in a proposed appeal against his conviction. The Claimant contends that the Defendants were simply trying to cause trouble for the Claimant.

14. It is relevant to note that:

    (1) On 27 July 2020 the Second Defendant forwarded to Mark Jones of MJP Solicitors, the First Defendant's solicitors, her complaint to the CPS and subsequent correspondence, thanking Mr Jones for having a conversation with the First Defendant and saying that the First Defendant had asked her to forward to Mr Jones a few emails, including the emails exchanged with the CPS.

    (2) On the same day, the Second Defendant forwarded to Mr Jones emails which she had exchanged with Detective Inspector Suzanne Grimmer of the Metropolitan Police.

    (3) On 23 October 2020 the Second Defendant sent to Mr Jones copies of her complaints to the Metropolitan Police, to the CPS and to the FCA, saying:

> "I am writing on Vlad's behalf as there is finally some material, he thinks can be sufficient for Legal Aid supplication to fund either judicial review or appeal of his conviction."

*(2)(c)(i) 17 February 2021: email to the ICO*

15. The Second Defendant complained about the way in which her complaint to the ICO had been handled. That led to her sending an email to the ICO on 17 February 2021, in which she said as follows:

> "The amount of evidence is really extensive - ~36 GB, so I am attaching only initial material and sending it via two emails. Please forward it to the Reviewing Officer. If he/she requires all data I can send it via USB memory stick or any way you will advise.
>
> 1. Examples of private and sensitive data of members of public, included in the CPS material:
>
> Visa/Mastercard unencrypted PANs, PINs, CVV2s, Expiry dates, cardholders addresses, emails, phone numbers, Passwords and million of records of corresponding card payments transactions. …"

16. I have not seen the attached emails. It appears that they were deleted by the Defendants in response to the order of Collins Rice J made on 15 December 2021.

However, it is clear that they included information derived from the Disclosed Data. In his fifth witness statement the First Defendant said that, from memory, they consisted of screenshots of credit card data, i.e. credit card numbers, PINs, CVVs, expiry dates and cardholder details.

17. This is the first of the emails about which the Claimant complains. The complaint is not only that the Second Defendant disclosed some of the Disclosed Data to the ICO, but also, as appears from this and subsequent emails, that the First Defendant had disclosed the Disclosed Data to the Second Defendant.

*(2)(c)(ii) 19 March 2021: emails to Mastercard and Visa*

18. On 17 March 2021 Detective Superintendent Stuart Ryan wrote to the Second Defendant and set out the results of the investigation into the complaint which she had made on 10 July 2020. He enclosed a 15-page report, prepared by DI Grimmer ("the Grimmer Report"), the conclusion of which was that there had been no data breach by the Metropolitan Police. It appears that the CPS conducted a similar investigation and reached the same conclusion.

19. It appeared from the Grimmer Report that at some time before 9 October 2020 Ms Grahame had told John Gardner of the CPS that the Exhibit did not contain any real credit card numbers and only contained tokenised credit card numbers. Ms Grahame has confirmed in a witness statement that she did say this "initially".

20. The First Defendant rightly believed that what Ms Grahame had said was incorrect. He claims that that is why, on 19 March 2021, the Second Defendant, at his request, sent emails to Mastercard and Visa, in each of which she provided a list of credit card numbers and said:

> "I was provided with a big volume of files that contain data I believed should be protected. Along with card numbers the files contain CVV2s with corresponding expiry dates and unencrypted PINs. So please respond to this email so I can report this data breach accordingly."

21. These are the second and third emails about which the Claimant complains. The complaint is one of use, rather than disclosure, of the Disclosed Data, since Mastercard and Visa already knew their customers' credit card numbers.

22. On 19 March 2021 an employee of Mastercard replied and said that she had reviewed the sample data provided and the accounts appeared to be aged with little recent activity.

23. Then on 20 March 2021 an employee of Visa replied and said as follows:

> "The file you have been given would have been served to you via the Crown Prosecution Service (CPS). The reason they would have sent this file would be to do with disclosure which they have to do with all criminal cases. The data would have been blocked by the banks when it was seized by the Police back in 2017. Therefore, the data is no longer valid data and therefore not subject to PCI DSS, therefore no data protection breach.

> I would advise that you should be careful about sharing such material, where you have stored this information and where it is viewed, as the police may see this as being in possession of fraud data and you could be committing further offences [sic] by having it in your possession and distributing it.
>
> The CPS are the ones that served you with the information. I suggest you contact them if you believe you have been sent the data in error and return it to them.
>
> We thank you for bringing this to our attention but as the data is dead data this matter is not a Visa issue and we deem the matter closed."

24. The Defendants appear to have regarded these responses as confirmation that the Disclosed Data contained credit card numbers which were real, rather than tokenised. On 20 March 2021 the Second Defendant forwarded her email correspondence with Mastercard to Mr Jones, saying that Mastercard's response was that the credit card numbers in the Exhibit were actual card numbers rather than token numbers. On 24 March 2021 the Second Defendant also forwarded her email correspondence with Visa to Mr Jones.

25. As I have said, the First Defendant was released from prison on 21 May 2021.

*(2)(c)(iii) 10 June 2021: email to Newsquest*

26. On 23 January 2020, i.e. the day after the First Defendant's conviction, the Metropolitan Police had published a press release about the case on their web-site and the Surrey Comet, a newspaper published by Newsquest, had published a story on its website, entitled "Weybridge man jailed for cyber attack on former employers", which was based on the Metropolitan Police's press release. On 3 June 2021 the First Defendant complained to the editor of the Surrey Comet about the article, which he alleged was defamatory, and was told that the information in it had been provided by the Metropolitan Police. The First Defendant's subsequent emails to Newsquest focused on his allegation that the article was defamatory and that he wanted it taking down.

27. Those emails included an email dated 10 June 2021 from the First Defendant to Will Harrison and Orlando Jenkinson of Newsquest, to which the First Defendant attached a copy of a letter which the Defendants had written to DSU Stuart Ryan on 1 April 2021. The email of 10 June 2021 is not referred to in the Amended Particulars of Claim, because it was not produced by the Defendants until after the hearing, but it is the fourth email about which the Claimant complains, because the attached letter contained what the Claimant contends is confidential information, namely a certain IP address and the names and details of the Claimant's clients, Mastercard and Visa, although the First Defendant contends that they were named in open court at his trial.

*(2)(c)(iv) 13 July 2021: email to the IPOC*

28. It appears that, by an email dated 27 June 2021, the Second Defendant made a complaint to the Independent Office for Police Conduct ("the IOPC"). Having received a response, the Second Defendant sent a further email to the IOPC, which is the fifth email about which the Claimant complains, and in which she said as follows:

> "Further to my request for review of April 1, 2021 please add to the 2021/151245 case the attached my email communications to Visa and Mastercard organisations (Correspondence to Visa and Mastercard (emails).docx) ..."

29. Attached to the email to the IOPC were the emails to and from Visa and Mastercard to which I have referred.

*(2)(c)(v) 29 July and 4 August 2021: emails to the Metropolitan Police and Newsquest*

30. On 5 July 2021 the First Defendant made a complaint to the Metropolitan Police about the press release of 23 January 2020 and Jack Griffith of the Metropolitan Police replied on 29 July 2021. This prompted the First Defendant to send an email on 29 July 2021 to Mr Griffith, which was copied to, amongst others, Charlotte Ikonen of Newsquest, and to which he attached copies of the Second Defendant's emails to Mastercard and Visa. The First Defendant's email of 29 July 2021 is the sixth email about which the Claimant complains.

31. The seventh email about which the Claimant complains is a subsequent email in the same chain, sent on 4 August 2021, in which the Claimant alleges that the First Defendant republished the correspondence with Mastercard and Visa, although the copy of the email which I have seen does not indicate that it had any attachments. This is another email which was only disclosed after the hearing.

32. Although the First Defendant contends (in paragraph 19 of his seventh witness statement) that his engagement with Newsquest was "part and parcel of my wider ongoing efforts to investigate the facts of my prosecution with a view to clearing my name, and not for the purpose of causing embarrassment to [the Claimant] or for any other improper purpose", the first reference in the First Defendant's many emails to Newsquest to the possibility of a journalist investigating the First Defendant's case came in an email dated 6 August 2021 from the First Defendant to Charlotte Ikonen of Newsquest, in which he said:

> "Also please would you be able to advise a journalist who can be interested in my story where several hundred thousands of Visa/MasterCard details (card number, expiry date, CVV2, unencrypted PINs, cardholder names/addresses/emails etc) were sent to my home address and what Police did to cover that up."

*(2)(c)(vi) 19 October 2021: email to the Metropolitan Police and the CPS*

33. On 19 October 2021 the First Defendant sent an email to various individuals within the Metropolitan Police and the CPS and to the barristers who had appeared at his trial. This is the eighth email about which the Claimant complains. The subject of the email was said to be "Letter before action" and in the email the First Defendant said as follows:

> "This email is to let you know that due to Metropolitan Police and CPS failure to inform the members of the public affected by the data breaches (Police ref PC4361/20, CPS ref 431-2020-2021) and enforce Data Protection Act and The Payment Services Regulations 2017 s73, s99, starting November 6, 2021 we

> will be contacting the affected people and businesses via direct email communications.
>
> According to available to us information, hundreds thousands of holders of Visa and MasterCard cards, which were issued and processed by [at the time of the incident] Dubai/Isle of Man-based company Global Processing Services on behalf of numerous FCA-regulated "Fintech" companies such as Wirecard, Revolut, Monzo and Starling Bank were affected, and their private data was distributed to various parties, including ourselves.
>
> The data contains clear Visa/MasterCard card numbers, unencrypted PINs, CVV2, expiry dates, unencrypted usernames and passwords, cardholder names, email addresses, phone numbers, residential addresses and history of their financial transactions, and based on our communication with Visa and MasterCard organisations no cardholders were informed about the use of their data, neither their active payment instruments were cancelled.
>
> No actual private data will be sent within our emails but the affected people will be offered to receive their personal data along with detailed evidence coming from the investigation material into conducts of MPCCU, CPS and a specific Global Processing Services employee as summarised in the attached 'Data breaches Met Police investigation report.pdf' and corresponding 'Correspondence to Visa and Mastercard (emails).pdf' documents."

34. Attached to the email were copies of the Grimmer Report and of the Second Defendant's emails to Mastercard and Visa. The Claimant contends that this email constituted a threat to use the Disclosed Data in breach of confidence. I note that the Defendants' stated intention was to contact "the affected people and businesses" and that the affected people would be offered to receive their personal data. In other words, the Defendants intended to contact individual cardholders and inform them of their allegation that there had been a data breach.

35. On 26 October 2021 the First Defendant sent an email to the Queen's Counsel whom he was proposing to instruct in relation to a possible appeal against his conviction. The First Defendant wrote:

> "Please see attached a draft grounds I currently think of. I will very likely have more once I receive/not receive a response to my enquiries to Met/CPS."

36. On 28 October 2021 DI Grimmer sent an email to the Defendants in which she drew their attention to section 170 of the Data Protection Act 2018 and advised them not to make unlawful disclosures and to seek legal advice on their proposed action.

*(2)(c)(vii) 29 October 2021: email to the Metropolitan Police and the CPS*

37. On 29 October 2021 the Defendants sent an email to DI Grimmer, to various individuals in the CPS and to trial counsel, in which they asserted that their proposed action was lawful by virtue of section 170(2) of the Data Protection Act 2018 and made clear that they intended to continue with their proposed action. This is the ninth email about which the Claimant complains, alleging that it was a repeat of the threat to use the Disclosed Data in breach of confidence.

*(2)(c)(viii) 1 November 2021: email to the Metropolitan Police and the CPS*

38. On 1 November 2021 the Head of the CPS's Data Protection Compliance Team, Miss H Hardaker, wrote to the Defendants and said that, in the light of DI Grimmer's email and the CPS's earlier investigation, the CPS did not propose to take any further action in response to the Defendants' "Letter before action" email of 19 October 2021. This prompted the Defendants to reply to Miss Hardaker on the same day, challenging the findings of the Metropolitan Police and the CPS that the Disclosed Data did not contain sensitive and private data belonging to members of the public and giving examples of cardholder names, addresses, email addresses, usernames and passwords and credit card numbers taken from the Disclosed Data. The Defendants concluded by stating that they intended to proceed with their action on 6 November 2021. This is the tenth email about which the Claimant complains, again alleging that it was a repeat of the threat to use the Disclosed Data in breach of confidence.

39. On 2 November 2021 the Claimant's solicitors wrote to the Defendants to say that any disclosure of the Disclosed Data would be a criminal offence, contrary to section 170 of the Data Protection Act 2018. Then on 5 November 2021 the Claimant's solicitors wrote to the Defendants to say that the disclosure of the Exhibit fell within section 17 of the Criminal Procedure and Investigations Act 1996 ("the 1996 Act") and that any disclosure of the Disclosed Data would be a criminal offence, contrary to section 18 of the 1996 Act. (It is now common ground that the Exhibit was not subject to section 17 of the 1996 Act.) They requested both an undertaking by the Defendants not to use or disclose any of the Disclosed Data and delivery up of all copies of the Exhibit. They threatened an application to the High Court if the Defendants did not confirm by 9 November 2021 that they would provide the undertaking and delivery up as requested.

*(2)(c)(ix) 8 November 2021: email to Monzo Bank*

40. On 8 November 2021 the Defendants sent an email to Monzo Bank, one of the Claimant's clients, which is the eleventh email about which the Claimant complains, and in which they said as follows:

> "We are writing to you concerning the 2017 data breaches caused by Global Processing Services (Dubai/IoM).
>
> The breached data was distributed to various parties, including ourselves and contains clear MasterCard card numbers of your customers, unencrypted PINs, CVV2, expiry dates, unencrypted usernames and passwords, cardholder names, email addresses, phone numbers, residential addresses and history of the financial transactions for period of 01/09/2016 – 03/04/2017, and based on our communication with MasterCard no cardholders were informed about the exposure of their data, neither their active payments instruments were cancelled.
>
> Until very recent we were barred from contacting you and remained subjected to attacks from Global Processing Services (UK) in their aim to conceal the evidence, but now can write to you so you are informed about the exposure of your customers data.

> We assure you that the ~36Gb of data distributed to us is safe and shall you have any questions we are will to cooperate with any of your regulatory enquiries."

*(2)(c)(ix) 11 November 2021: emails to CBH Bank and Curve*

41. In the morning of 11 November 2021 the Defendants sent emails to two more of the Claimant's customers, CBH Bank and Curve, which were in the same terms as the email to Monzo Bank. These are the twelfth and thirteenth emails about which the Claimant complains. The Claimant contends that, by sending these emails to Monzo Bank, CBH Bank and Curve, the Defendants used the Disclosed Data in breach of confidence.

***(2)(d) The Injunction Application and the Claim***

42. In the afternoon of 11 November 2021 the Claimant's solicitors served an application notice and supporting evidence on the Defendants. The Defendants replied by email, quoting passages from the Grimmer Report, one of which said that the Exhibit was exhibited evidence and not unused material (which was relevant to the question whether section 17 of the 1996 Act applied), and the others of which referred to the incorrect statement which Ms Grahame had made that all of the credit card numbers in the Disclosed Data were tokenised.

43. On 12 November 2021 Collins Rice J imposed an injunction prohibiting the disclosure of the Disclosed Data and she continued this at the return date hearing on 15 November 2021. It is not suggested that there has been any breach of this prohibition by the Defendants, who delivered up their copies of the Exhibit on 5 January 2022 and served witness statements identifying uses made of the Disclosed Data. There are issues about the adequacy of the disclosure made on that occasion, but I need not concern myself with those issues.

44. The claim form was issued on 19 January 2022, the Particulars of Claim were served on 2 February 2022, the Defence was served on 27 April 2022 and the application for summary judgment was issued on 21 July 2022. A curious feature of the statements of case is that the Claimant asserted, and the Defendants admitted, that the Exhibit was subject to section 17 of the 1996 Act, but Mr de Wilde challenged this in his skeleton argument for the hearing of the summary judgment application and at the hearing it was common ground that section 17 of the 1996 Act did not apply, although Mr Vassall-Adams submitted that this made no practical difference, for reasons which I will explain.

45. Moreover, having read the Particulars of Claim, I sought clarification whether the Claimant was alleging breach of statutory duty, but Mr Vassall-Adams confirmed that the only cause of action relied on by the Claimant was in breach of confidence.

46. In these unusual circumstances, I heard argument from the parties, but I also directed that the Claimant should amend its Particulars of Claim after the hearing, that the Defendants should amend their Defence and that the parties should have the opportunity to make any further submissions arising out of the amendments in writing. Those submissions were received on 1 December 2022.

47. In addition, the Defendants filed and served after the hearing a witness statement made by the First Defendant, who exhibited and commented on his email correspondence with Newsquest. The Claimant objected to this witness statement, but I have taken account of it, not least because it disclosed for the first time two of the emails about which the Claimant complains, namely the emails dated 10 June and 4 August 2021 to which I have referred. I do not consider that the Claimant was prejudiced in any way by the late service of this evidence.

**(3) The Issues**

48. The amended statements of case filed after the hearing show that the principal issues between the parties are as follows:

i) The Claimant alleges, and the Defendants deny, that the Disclosed Data had the necessary quality of confidence. In particular, the Defendants assert that the credit card numbers in the Disclosed Data were out of date and no longer in use.

ii) The Claimant alleges that the Disclosed Data was imparted in circumstances which imposed a duty of confidence on the Defendants. The Defendants' pleaded response to this allegation is ambiguous:

a) The Claimant's allegation is made in paragraph 14 of the Particulars of Claim. That paragraph is denied in paragraph 11 of the Defence, but the reasons given for the denial are solely concerned with the Defendants' denial of the Claimant's allegation (also made in paragraph 11 of the Particulars of Claim) that the credit card numbers in the Disclosed Data had the necessary quality of confidence.

b) The Claimant alleges in paragraph 16 of the Particulars of Claim that the Defendants were and are under an obligation of confidence to the Claimant in relation to the Disclosed Data. That allegation is admitted by the Defendants in paragraphs 13 of the Defence, "subject to paragraphs 18-21 pleaded in relation to Defences below." Paragraphs 18 to 21 of the Defence concern the Defendants' use of the Disclosed Data and are therefore focused on an assertion that that use did not involve a breach of the alleged obligation of confidence or the alleged implied undertaking.

c) Paragraph 19 of the Defence repeats paragraph 11 of the Defence, but only addresses the question whether the Disclosed Data had the "necessary quality of confidence" and does not assert a positive case that the Disclosed Data was not imparted in circumstances which imposed a duty of confidence on the Defendants.

d) It is asserted in paragraph 20.2 of the Defence that the Defendants acted in the public interest by seeking to establish that the Claimant had committed breaches of its legal and regulatory obligations.

iii) The Claimant alleges, and the Defendants deny, that the Disclosed Data was subject to an implied undertaking to the Court that the First Defendant would

only use it for the purposes of the criminal proceedings, including any application for permission to appeal and/or any appeal.

iv) In the alternative, the Defendants allege that:

a) Any implied undertaking which might otherwise apply did not apply to them because they were not informed of it.

b) If they were subject to an implied undertaking, they were not in breach of it because they only used the Disclosed Data for the purposes of a proposed application for permission to appeal against the First Defendant's conviction.

v) In the alternative, the Defendants contend that there was a public interest in their use of the Disclosed Data in an attempt to have the First Defendant's conviction quashed and/or to establish that there had been a data breach.

vi) There is a difference between the parties as to how the court should approach the question of whether the Defendants' use of the Disclosed Data falls within an exception to the scope of the implied undertaking and/or any obligation of confidence:

a) The Defendants contend that it is sufficient that they acted in good faith in a manner which they believed was for the purpose of the proposed application for permission on appeal or in the public interest and that it is for the Claimant to prove that they were not acting in good faith.

b) The Claimant does not accept that the Defendants were acting in good faith and also contends that it is for the Defendants to prove that they were acting reasonably, and that what is reasonable is to be determined objectively by the court, rather than by reference to the Defendants' subjective beliefs.

vii) In the further alternative, the Defendants allege that the Claimant has not suffered any loss, damage or detriment and that this not an appropriate case of an injunction.

49. Pursuant to CPR 24.2, the issue on this application is whether or not the defendants have a real prospect of successfully defending the claim. This is not a case in which there is some other compelling reason why the case should be disposed of at a trial.

**(4) The Alleged Implied Undertaking**

50. Mr Vassall-Adams clarified that the Claimant is not seeking by this action to enforce the alleged implied undertaking, which, if it was given, was given to the Crown Court. Instead, the allegation that the Disclosed Data was subject to an implied undertaking is part of the Claimant's case that the Disclosed Data was imparted in circumstances which gave rise to a duty of confidence on the part of the Defendants.

51. Evidence which is provided by the prosecution to a defendant in connection with a Crown Court trial can be divided into two categories, "used" and "unused" material.

It is common ground that the Disclosed Data was used material. It is also common ground that:

i) the Disclosed Data was not communicated to the public in open court; but

ii) if and insofar as the Disclosed Data had been communicated to the public in open court, it would no longer be subject to the alleged implied undertaking.

***(4)(a) Unused Material: the Statutory Prohibition***

52. Subsections 17(1) to (4) of the 1996 Act apply to unused material and provide as follows:

> "(1) If the accused is given or allowed to inspect a document or other object under—
>
> (a) section 3, 4, 7A, 14 or 15, or
>
> (b) an order under section 8,
>
> then, subject to subsections (2) to (4), he must not use or disclose it or any information recorded in it.
>
> (2) The accused may use or disclose the object or information—
>
> (a) in connection with the proceedings for whose purposes he was given the object or allowed to inspect it,
>
> (b) with a view to the taking of further criminal proceedings (for instance, by way of appeal) with regard to the matter giving rise to the proceedings mentioned in paragraph (a), or
>
> (c) in connection with the proceedings first mentioned in paragraph (b).
>
> (3) The accused may use or disclose—
>
> (a) the object to the extent that it has been displayed to the public in open court, or
>
> (b) the information to the extent that it has been communicated to the public in open court;
>
> but the preceding provisions of this subsection do not apply if the object is displayed or the information is communicated in proceedings to deal with a contempt of court under section 18.
>
> (4) If—
>
> (a) the accused applies to the court for an order granting permission to use or disclose the object or information, and
>
> (b) the court makes such an order,
>
> the accused may use or disclose the object or information for the purpose and to the extent specified by the court."

53. However, as I have said, it is common ground that this section did not apply in the present case and there is no equivalent statutory provision in relation to used material.

### *(4)(b) Used Material: The Authorities*

54. *Mahon v Rahn* [1998] Q.B. 427, CA was a case in which the plaintiffs alleged that the defendants had made defamatory statements in a letter which the defendants had sent, or caused to be sent, to the Serious Fraud Office ("the SFO"), which the prosecution subsequently disclosed to the plaintiffs as used material in advance of their trial in the Crown Court and which was read out in open court during the trial. The defendants applied for an order striking out the action as an abuse of the process of the court, alleging that the claimants were in breach of their alleged implied undertaking not to use material disclosed in the course of criminal proceedings in any other proceedings without the leave of the court.

55. The letter was disclosed before section 17 of the 1996 Act came into force. The Court of Appeal held that at common law no undertaking was implied when the prosecution disclosed material to a defendant in criminal proceedings, whether that material was used or unused.

56. The decision in *Mahon v Rahn* was considered by the Court of Appeal and the House of Lords in *Taylor v Director of the Serious Fraud Office* [1999] 2 A.C. 177 ("*Taylor v SFO*"). The plaintiffs in *Taylor v SFO* alleged that the defendants had defamed them in a letter sent by an employee of the SFO to the Attorney-General of the Isle of Man and in a conversation between that employee of the SFO and an employee of the Law Society, who made a file note of that conversation. The letter was written and the conversation took place in the context of the SFO's investigation into two individuals who were prosecuted for, and convicted of, conspiracy to defraud. The letter and the file note were disclosed to those individuals as unused material in the criminal proceedings. The solicitors for one of those individuals showed the letter and the file note to the plaintiffs, in the context of requesting their assistance in the criminal proceedings.

57. As in *Mahon v Ryan*, the documents were disclosed before the 1996 Act came into force, so the courts had to decide the case on the basis of the common law. The judge at first instance struck out the writ and statement of claim as an abuse of the process of the court, on the basis that the plaintiffs were bound by an implied undertaking not to use the documents for purposes collateral to the proceedings in which they were disclosed.

58. The Court of Appeal dismissed the appeal. They did so on the basis that the defendants were immune from suit in respect of what was said in the letter, in the conversation and in the file note. Another ground of appeal was that the judge was wrong to hold that the documents were subject to an implied undertaking not to use the documents for purposes collateral to the proceedings in which they were disclosed. As to that ground of appeal:

    i) All three judges said that, were it not for *Mahon v Rahn*, they would have held that all documents disclosed in criminal proceedings are subject to an implied undertaking: see the judgments of Kennedy LJ at 196G-197D, Millett LJ at 197H to 198G and Sir Brian Neill at 200B.

    ii) However, all three judges held that they were bound to follow *Mahon v Rahn* and that they could not distinguish it, as they were invited to, on the basis that

> it only concerned used material and not unused material: see the judgments of Kennedy LJ at 197E-G, Millett LJ at 198G to 199E and Sir Brian Neill at 200C.

59. The House of Lords dismissed the appeal on two grounds. They agreed, by a majority of four to one, that the allegedly defamatory statements were subject to absolute privilege. They also held that there was an implied undertaking not to use for any collateral purpose documents which were disclosed by the prosecution as unused material in criminal proceedings. On this point, Lord Hoffmann, with whom the other judges agreed, expressed his conclusions as follows, at page 212E-G:

> "In my opinion, therefore, the disclosure of documents by the prosecution as unused material under its common law obligations did generate an implied undertaking not to use them for any collateral purpose. I agree with the reasoning of Brooke J. on this point *in Mahon v. Rahn* and I think that Sir Michael Davies was right to strike out the action for the reasons which he gave.
>
> I do not propose to express a view on the further points which arose in *Mahon v. Rahn* [1998] Q.B. 424, namely whether the undertaking applies also to used materials and whether it survives the publication of the statement in open court. I do not do so because these questions may well have been overtaken by the express provisions of the Criminal Procedures and Investigations Act 1996. But I would draw attention to the comments of Brooke J. in *Mahon v. Rahn* on the question of whether the provisions of Ord. 24, r. 14A (which was introduced in response to a decision of the European Court of Human Rights holding that the previous law unduly limited freedom of expression) and, by parity of reasoning, section 17(3)(6) of the Act of 1996, are not too widely drawn. There seems to me much force in his view that the court should nevertheless retain control over certain collateral uses of the documents, including the bringing of libel proceedings."

60. The effect of *Taylor v SFO* is therefore that *Mahon v Rahn* was wrongly decided insofar at it decided that an implied undertaking does not arise at common law on the disclosure of unused material to a defendant in a criminal case, but it remains open for decision whether *Mahon v Rahn* was wrongly decided insofar at it decided that an implied undertaking does not arise at common law on the disclosure of used material to a defendant in a criminal case. Both the Court of Appeal and the House of Lords in *Taylor v SFO* expressed obiter opinions to the effect that *Mahon v Rahn* was wrongly decided in relation to used material, but the Court of Appeal decided that it was obliged to follow *Mahon v Rahn* and the House of Lords did not decide whether *Mahon v Rahn* was correctly decided in relation to used material, but expressly left that question open.

61. As Tugendhat J said in paragraph 71 of his judgment in *Bell v Brown* [2007] EWHC 2788 (QB):

> "… it is apparent from Lord Hoffman's words that the law is not clear, …"

62. I was also referred to paragraph 100 of Toulson LJ's judgment in *R (Guardian News Media Ltd) v City of Westminster Magistrates' Court* [2013] QB 618, which is in the

following terms:

> "Whether the defence has an unfettered right to release documents served on it by the prosecution during the proceedings and vice versa is a more difficult topic. The Criminal Procedure and Investigations Act 1996 in sections 17 and 18 makes special provision for the confidentiality of unused material served on the defendant by the prosecution. Section 17(3) allows the defence to use or disclose unused material only to the extent that it has been displayed to the public in court or to the extent that it has been communicated to the public in court. As far as material relied upon by the prosecution as part of its case and not covered by the Sexual Offences (Protected Material) Act 1997 is concerned, the defence do not in practice give any undertaking about its use and nor do the prosecution give any undertaking in relation to material received from the defence. As to whether there are any implied restrictions on the use of such material, see *Mahon v Rahn* [1998] QB 424 and *Taylor v Director of the Serious Fraud Office* [1999] 2 AC 177 both in the Court of Appeal and in the House of Lords, where Lord Hoffmann (with whose speech the other members of the Appellate Committee agreed) said, at p 212:
>
> > "I do not propose to express a view on the further points which arose in *Mahon v Rahn* [1998] QB 424, namely whether the [implied] undertaking applies also to used materials and whether it survives the publication of the statement in open court.""

***(4)(c) Used Material: Commentary***

63. Mr Vassall-Adams relied on the 2023 edition of *Archbold on Criminal Pleading Evidence & Practice, which* sets out section 17 of the 1996 Act in paragraph 12-88 and then states, inter alia, as follows in paragraph 12-89:

> "Disclosure not falling within s.17(1) (such as that made before "the relevant time", § 12-49) is subject to an implied undertaking not to use the material for any purposes other than the proper conduct of the particular case: *Taylor v Director of the Serious Fraud Office* [1999] 2 A.C. 177, HL."

64. However, this statement does not address the distinction drawn in *Taylor v SFO* between used and unused material.

65. Mr Vassall-Adams also relied on the 5th edition of *Arlidge, Eady & Smith on Contempt*, paragraphs 11-93 and 11-94 of which state, inter alia, as follows:

> "11.93 … In criminal cases, it was thought for a time that there was no implied undertaking of confidentiality analogous to that applying to documents disclosed in civil proceedings.[182] It is now clear, however, from the decision of the House of Lords in *Taylor v Serious Fraud Office*[183] that documents seized during a criminal investigation are to be treated as confidential.
>
> 11.94 The provisions of the 1996 Act apply only to unused material; that is to say, there is no protection for material which has been read out or exhibited in open court. …"

66. However, this is unhelpful, since the first sentence of paragraph 11-94 equates used material with material which has been read out in open court, which is not what is meant by used material.

67. Paragraph 19.63 of the 5th edition of *Malek on Disclosure* begins:

> "Compliance by the prosecution with its obligation to disclose material to the defence generates an implied undertaking at common law not to use unused (and probably also used) material for any purpose other than the conduct of the defence.[218]"

68. Mr de Wilde stressed the use of the word "probably". In addition, he referred to footnote 218, which is in the following terms:

> "*Taylor v SFO* [1999] 2 A.C. 177 HL. In Canada it has been held that no undertaking exists in relation to documents provided by the Crown: *Consolidated NBS Inc v Price Waterhouse* (1992) 94 D.L.R. (4th) 176 Ont. Ct.; though see also *P (D) v Wagg* (2004) 239 D.L.R. (4th) 501 Ont. CA. In *Breslin v McKenna* [2008] IEHC 122, the Irish High Court left open the question whether there was an implied undertaking in respect of documents disclosed for the purposes of criminal proceedings."

69. I was not taken to the Canadian and Irish cases, but they lend support to the proposition that this is a difficult topic.

***(4)(d) The Alleged Implied Undertaking: Conclusion***

70. Were the question free from authority, I would see strong arguments, of the kind identified by the Court of Appeal and by Lord Hoffman in *Taylor v SFO*, for holding that a defendant to criminal proceedings who receives used material from the prosecution is subject to an implied undertaking not to use that material for any collateral purpose. However, the question is not free from authority. On the contrary, *Mahon v Rahn* is a decision of the Court of Appeal in which it was held that a defendant to criminal proceedings who received used material from the prosecution was not subject to such an implied undertaking. The decision in *Mahon v Rahn* was overturned by the House of Lords insofar as it related to unused material, but it was not overturned, although it was doubted, by the House of Lords insofar as it related to used material.

71. In those circumstances, I consider that I am bound to follow *Mahon v Rahn*. However, even if I were wrong about that, I would not consider that the present application was an appropriate occasion for departing from *Mahon v Rahn*, given my other findings.

**(5) Breach of Confidence**

72. My conclusion in relation to the alleged implied undertaking is not a bar to the success of the Claimant's application, since the Claimant's cause of action lies in breach of confidence and the Court of Appeal in *Mahon v Rahn* was not concerned with a claim in beach of confidence.

73. As stated by Megarry J in *Coco v A.N. Clark (Engineers) Ltd* [1969] RPC 41, at 47:

> "… , three elements are normally required if, apart from contract, a case of breach of confidence is to succeed. First, the information itself, in the words of Lord Greene M.R. in the *Saltman* case on p. 215, must 'have the necessary quality of confidence about it.' Secondly, that information must have been imparted in circumstances importing an obligation of confidence. Thirdly, there must be an unauthorised use of that information to the detriment of the party communicating it. ..."

74. There are issues in this case as to at least two of these elements.

***(5)(a) "The Necessary Quality of Confidence"***

75. I have already cited a number of documents in which the Defendants themselves asserted, in effect, that the Disclosed Data was confidential. These include:

i) The First Defendant's amended defence statement of 15 August 2018, in which he said that the Exhibit contained "the type of information that a "hacker" might seek."

ii) The Second Defendant's emails of 20 July 2022 complaining that there had been a data breach when the Exhibit was disclosed and her subsequent complaints to the ICO and the FCA.

iii) The Second Defendant's email of 17 February 2021 to the ICO, in which she said that the Exhibit included "private and sensitive data of members of the public".

iv) The Second Defendant's emails of 19 March 2021 to Mastercard and Visa, in which she said that the Exhibit contained "data I believed should be protected."

v) The First Defendant's email of 19 October 2021, which referred to the Disclosed Data as including "private data".

vi) The Defendants' email to 1 November 2021 to Miss Hardaker, asserting that, contrary to the Grimmer Report, the Exhibit contained sensitive and private data.

76. Having regard to what the Defendants themselves have said about the Disclosed Data, there is no realistic prospect of them successfully resisting at trial the Claimant's case that the Disclosed Data had the necessary quality of confidence. The Defendants' only pleaded case in that respect is that the Disclosed Data had lost its quality of confidence insofar as the credit cards had expired between 2017 and 2021. However:

i) This only applies to part of the Disclosed Data. It does not apply, for instance, to the cardholder details which the Defendants were proposing from 19 October 2021 to use in order to contact individual cardholders and tell them (incorrectly) that there had been a data breach.

ii) Moreover, the only evidence for the expiry of the credit cards relied on by the Defendants was contained in the emails from Visa and Mastercard:

a) The employee of Mastercard said that the accounts referred to in the sample data provided "appear to be aged with little recent activity." However, "aged" is not the same as "expired" and "little recent activity" is not the same as "no activity", so it appears that some of the credit cards may well have remained active.

b) The employee of Visa referred to the data as "dead data", but this description was based on the mistaken premise that the data would have been blocked by the banks when it was seized by the police.

***(5)(b) "Imparted in Circumstances Importing an Obligation of Confidence"***

77. What the Defendants have themselves said about the Disclosed Data also indicates that there is no realistic prospect of them successfully resisting at trial the Claimant's case that the Disclosed Data was imparted to them in circumstances importing an obligation of confidence. As I have indicated, their pleaded case on this issue appears ambiguous, but they certainly did not contend, for instance, that they would have been at liberty to publish the Disclosed Data.

***(5)(c) "Unauthorised Use of Information"***

78. As I have said, there is a dispute as to how the court should approach the question of whether the Defendants' use of the Disclosed Data fell within any exception to the obligation of confidence. The Defendants rely on two exceptions. They claim that they were entitled to use the Disclosed Data as they did either because they were using it for the purposes of a proposed application for permission to appeal ("the purposes exception") or because there was a public interest in them doing so ("the public interest exception").

79. In the case of each exception, the Defendants contend that it is sufficient that they were acting in good faith and that the burden is on the Claimant to prove that they were acting with malice. Mr de Wilde compared this to the position in a libel case where malice must be proved to defeat qualified privilege. I did not find that to be a helpful analogy.

*(5)(c)(i) The Public Interest Exception*

80. Insofar as the Defendants contended that they were acting in the public interest, either by seeking to have the First Defendant's conviction quashed or by reporting what they mistakenly believed to be a data breach, there are a number of authorities which establish that a party's subjective intentions are not determinative of the question whether their use of confidential information falls within the public interest exception. These authorities are considered in *Toulson & Phipps on Confidentiality*, 4th Edn., paragraphs 5-103 to 5-118. I do not accept, therefore, the Defendants' contention that it was sufficient that they were acting in good faith insofar as it applies to the public interest.

81. The Defendants allege in their defence that they made only limited and proportionate efforts to seek to have the First Defendant's conviction quashed and to report what they mistakenly believed to be a data breach. The nature and scope of the use made by a party of confidential information in what is said to be the public interest is

relevant to, but is by no means determinative, of the question whether the public interest exception applies. In any event, however, the threatened use of the Disclosed Data to contact individual cardholders was clearly neither limited nor proportionate and was plainly not in the public interest. For that reason alone, in my judgment there is no realistic prospect of it being found at trial that all of the Defendants' actual or threatened use of the Disclosed Data fell within the public interest exception. In those circumstances, I need say no more about the public interest exception.

*(5)(c)(ii) The Purpose Exception*

82. As I have said, it is common ground that the First Defendant was entitled to use the Disclosed Data for the purposes of the criminal proceedings, including any application for permission to appeal and/or any appeal. The Defendants contend that they acted as they did in the belief, albeit mistaken, that their conduct would, or might, assist with a proposed application for permission to appeal against the First Defendant's conviction.

83. Mr Vassall-Adams submitted that the purpose exception was ultimately a species of public interest defence and that an objective, rather than subjective, test should be applied. He may be right, but I consider that there may be something to be said for the proposition advanced by Mr de Wilde that all that matters is the actual purpose (even if based on a misunderstanding) of the party to whom documents have been disclosed in criminal proceedings. I say this because of the terms of subsection 17(2)(b) of the 1996 Act. Subsection 17(2) provides as follows:

> "The accused may use or disclose the object or information—
>
> (a) in connection with the proceedings for whose purposes he was given the object or allowed to inspect it,
>
> (b) with a view to the taking of further criminal proceedings (for instance, by way of appeal) with regard to the matter giving rise to the proceedings mentioned in paragraph (a), or
>
> (c) in connection with the proceedings first mentioned in paragraph (b)."

84. The subsection only applies to unused material, but the parties did not suggest any reason why used material should be treated differently from unused material in this respect. In the case of unused material, the words "with a view to" in subsection 17(2)(b) could be said to point towards the subjective intention of the accused, rather than an objective test. However, I do not find it necessary to decide the point.

85. That is because I consider that it is clear that the action which from 19 October 2021 the Defendants were threatening to take, namely using the Disclosed Data to contact individual cardholders and tell them that there had been a data breach, was not action which would have been done for the purpose of, or "with a view to", an application for permission to appeal.

86. In his sixth witness statement, the First Defendant gives two reasons why the Defendants made use of the Disclosed Data:

i) The first reason was that they wanted to confirm that the Disclosed Data contained actual, rather than tokenised, credit card numbers. That was said to

be the reason for sending sample credit card numbers to Mastercard and Visa.

ii) The second reason was that they believed that any investigation into the alleged data breach might turn up evidence which would help the First Defendant in his proposed appeal.

87. However, neither of these reasons apply to contacting individual cardholders. The Defendants had by 19 October 2021 dealt with the issue whether the card numbers were actual or tokenised by contacting Mastercard and Visa. Individual cardholders were not in a position to conduct any investigations and the Defendants understandably did not suggest that the cardholders would have had any evidence which the Defendants believed could assist in the First Defendant's proposed appeal.

88. The First Defendant did not identify in his sixth witness statement any reason why he believed that contacting individual cardholders would assist his proposed appeal. Instead, he said as follows in paraph 24 of that statement, by reference to the Defendants' emails of 19 October and 1 November 2021:

i) "I accept that I stated therein that we would contact the affected individuals directly, but I made it clear that we would not disclose any private data in doing so."

ii) "Whilst I acknowledge that we maintained our intention to contact individuals, in the event, we did not want to take any risk of acting improperly, and no individuals or businesses whose details appeared in the Confidential Information were ever contacted."

89. Whether or not the Defendants were intending to disclose any data to the cardholders, they were threatening to make use of the Disclosed Data, and in particular the card holder names and contact details, in order to contact those cardholders and tell them that there had been a data breach. The Defendants do not claim that what they were threatening to do would be done for the purposes of the First Defendant's proposed appeal. I note that, in paragraph 25 of his sixth witness statement, the First Defendant said that:

> "All of the acts referred to above were carried out with a view to clearing my name and appealing against my conviction."

90. That applied to the various emails which the Defendants actually sent, which the First Defendant described as "highly focused and confined to organisations which I had a legitimate interest in sending them to", but the First Defendant made no such claim in relation to the contact which the Defendants threatened to make with individual cardholders. In the circumstances, there is no realistic prospect of it being found at trial that the use which the Defendants were threatening to make of the Disclosed Data was authorised.

***(5)(d) "to the Detriment of the Party Communicating it"***

91. There was a dispute between the parties whether it was necessary for the Claimant to show that the Defendants' unauthorised use, or threatened use, of the Disclosed Data had caused, or would cause, detriment to the Claimant. This issue is considered in

paragraphs 5-013 to 5-022 of *Toulson and Phipps on Confidentiality*, 4th Edn., but I do not find it necessary to resolve the dispute, since it is clear that the Defendants' threatened action of contacting cardholders and telling them that there had been a data breach would be detrimental to the Claimant's reputation.

**(6) Remedy**

92. The Claimant does not seek any damages. It seeks an injunction prohibiting the Defendants from using, preserving, disseminating or disclosing the Disclosed Data and delivery up and permanent destruction and/or deletion of any documents containing any of the Disclosed Data.

93. An injunction is, of course, a discretionary remedy. As to that, Mr de Wilde submitted that:

    i) A court may refuse to grant relief if the relief claimed would cause injustice to a defendant who has acted in good faith.

    ii) The court would not make an order which was ineffectual or unnecessary. The Defendants no longer have the Disclosed Data, which has been delivered up or destroyed in response to Collins-Rice J's orders. The conduct complained of, including the threat to use the Disclosed Data to contact cardholders, is no longer continuing.

94. However, the documents disclosed since the hearing show that I cannot assume that the Defendants have complied fully with Collins Rice J's orders. More importantly, it was necessary for the Claimant to bring this action in order to stop the Defendants from carrying out their threat, a threat which they repeated even after being told that what they were threatening to do was illegal. In those circumstances, it is right that an injunction should be granted.

**(7) Conclusion**

95. For the reasons which I have given, I will give summary judgment for the Claimant in respect of the threatened misuse of the Disclosed Data and grant an injunction in the terms sought.