THE HIGH COURT

COMMERCIAL

[2017 No. 6193 P.]

[2017 No. 170 COM.]

BETWEEN

ANN NOLAN, ELIZABETH NOLAN, JOAN NOLAN, RICHARD NOLAN, PATRICIA NOLAN, SALLY NOLAN and QUEST CAPITAL TRUSTEES LIMITED

PLAINTIFFS

AND

DILDAR LIMITED, CIARAN DESMOND AND COLM S. McGUIRE AND DERVAL M. O'HALLORAN, FORMERLY TRADING UNDER THE STYLE AND TITLE OF McGUIRE DESMOND SOLICITORS, A FIRM, JOHN MILLETT, PINNACLE PENSIONER TRUSTEES LIMITED, DILDAR LIMITED and JOHN MILLETT INDEPENDENT FINANCIAL ADVISORS LIMITED

AND BY ORDER

DILLON KENNY AND DARREN KENNY

AND BY FURTHER ORDER

PAUL KENNY

DEFENDANTS

AND BY ORDER

STEPHEN DECLAN MURPHY, EDEL MURPHY, KEVIN JOSEPH McMAHON, JOHN LYNCH, EFG BANK AG, BNP PARIBAS WEALTH MANAGEMENT, UNITED OVERSEAS BANK LIMITED and ALLIED FINANCE TRUST AG

THIRD PARTIES

JUDGMENT of Mr. Justice David Barniville delivered on the 27th day of November, 2020

Introduction

1. This judgment deals with another interlocutory application in this long running and complex case. The application the subject of this judgment was brought by the plaintiffs who were dissatisfied with the discovery made by the fifth, sixth and eighth defendants (the "Millett defendants") on foot of an order for discovery made by the High Court (Twomey J.) on 22nd February, 2019. The Millett defendants maintained that their computer systems were subjected to a cyber attack in the form of a ransomware attack which affected their ability to make the discovery required by that order.

2. In their application, the plaintiffs initially sought various wide-ranging orders permitting inspection and search facilities in respect of computer servers, mail servers, information technology devices and email addresses, together with an explanation on affidavit as to the whereabouts of electronically stored information, the appointment of an independent expert nominated by the court to carry out such an inspection and various other orders. The plaintiffs refined their application somewhat at the hearing in light of the affidavits exchanged between the parties.

3. The plaintiffs' application raises an issue as to what the court can or should do in circumstances where a party which is the subject of an obligation to make discovery on foot of an agreement or order for discovery finds itself unable properly to do so, in circumstances where its computer systems have been subjected to a cyber attack such as the ransomware attack allegedly suffered by the Millett defendants in this case.

4. For reasons set out in this judgment, I have concluded that, notwithstanding the clear deficiencies in the discovery originally made by the Millett defendants on foot of the order,

those defendants have adequately addressed the plaintiffs' complaints, have provided a satisfactory explanation on affidavit and have addressed the deficiencies in their discovery. I have concluded that no useful purpose would be served by granting the modified form of relief sought by the plaintiffs on the hearing of the application and that it would be unfair to the Millett defendants, contrary to the interests of justice and disproportionate to grant the modified relief sought by the plaintiffs. While the plaintiffs were perfectly entitled to bring their application in light of the unsatisfactory affidavit of discovery sworn by Mr. Millett on behalf of the Millett defendants, the deficiencies were (save in one respect) adequately addressed in the affidavits sworn in response to the plaintiffs' application by Mr. Millett and by Eamon Gallagher, the information technology expert engaged by the Millett defendants. I have concluded that, in light of the various affidavits sworn on behalf of the Millett defendants in response to the plaintiffs' application, the deficiencies in their discovery have been adequately addressed and that it would not be fair, appropriate or proportionate to accede to the plaintiffs' application for an order permitting the inspection and search of the Millett defendant's IT systems by an independent expert. I have, however, concluded that Mr. Millett should swear a further affidavit to confirm that a laptop was searched for responsive documentation at the time the discovery was made by the Millett defendants in late May, 2019.

Brief Description of the Proceedings

5. I have previously delivered a number of reserved judgments in interlocutory applications made in this case: [2020] IEHC 243 and [2020] IEHC 244. It is unnecessary to repeat the detailed description of the proceedings contained in the longer of those two judgments. It is sufficient to provide a brief summary in order to put in context the issues which have arisen on this application.

6. The plaintiffs have brought these proceedings in their capacity as trustees of a pension fund set up for the benefit of members of the Nolan family, the Oaklands Property Trust. The plaintiffs claim that a sum of in excess of €6.96 million, representing a portion of that pension fund, was lost due to the alleged fraud and other wrongdoing on the part of their solicitor, Ciaran Desmond (the second defendant), and their pensions and financial advisor, John Millett and companies operated by him as part of his business (the fifth, sixth and eighth defendants) (the "Millett defendants"). The plaintiffs claim that, without their knowledge or consent, Mr. Desmond and the Millett defendants permitted the plaintiffs' funds, which were in a bank account with EFG Bank in Zurich in the name of a Panamanian company, Clear Vision Solutions SA ("CVSSA"), to be pledged as collateral in order to obtain finance to purchase investment products to be issued by a number of the third parties in Singapore. By reason of a series of events, the plaintiffs claim that the bulk of their monies were misappropriated and lost to them.

7. The plaintiffs also claim that in September, 2013, without their knowledge or consent, Mr. Desmond and the Millett defendants used approximately €2.828 million of the plaintiffs' funds in the CVSSA account with EFG Bank to substantially finance the purchase, by an Isle of Man company, Dildar Limited ("Dildar IOM"), the first defendant, of development lands in Cork which were formerly owned by Nemo Rangers GAA Club (the "Nemo lands") which were purchased by Dildar IOM in September, 2013 for €3.07 million.

8. The plaintiffs claim damages and other reliefs against Mr. Desmond and the Millett defendants arising out of the alleged misappropriation of their funds. They also claim beneficial ownership of Dildar IOM and of the Nemo lands, which they claim were purchased substantially with their funds. Detailed allegations are made by the plaintiffs against Mr. Desmond and the Millett defendants. It is unnecessary to recite those allegations in this judgment. Mr. Desmond and the Millett defendants deny the claims against them.

They deny that the Nemo lands were purchased with the plaintiffs' funds and both plead that the funds used to purchase those lands, which were in an account in the name of CVSSA in EFG Bank, were monies belonging to another family (the Kennys) and did not come from the plaintiffs' monies. The plaintiffs dispute this. Several third parties were joined to the proceedings on the application of Mr. Desmond. Various members of the Kenny family were also joined as defendants.

The Discovery Process Involving the Millett Defendants

9. The plaintiffs sought discovery from the Millett defendants in July, 2018. In their discovery request dated 20th July, 2018, it was stated that, to the extent that any of the categories of documents sought contained electronically stored information, the plaintiffs requested that such documents be produced in searchable form and that the plaintiffs be provided with inspection and searching facilities. There was no agreement between the plaintiffs and the Millett defendants in relation to the plaintiffs' discovery request and a motion for discovery was issued in September, 2018. The Millett defendants agreed to make certain voluntary discovery and the scope of that discovery was ultimately agreed between the parties and reflected in the terms of the order made by the High Court (Twomey J.) on 22nd February, 2019.

10. The order required that discovery be made within twelve weeks of the making of the order. Mr. Millett swore an affidavit of discovery on behalf of the Millett defendants on 31st May, 2019. At para. 12 of his affidavit, Mr. Millett stated that the Millett defendants did not have in their possession, power or procurement, the documents set forth in the second schedule to the affidavit. Paragraph 2 of the second schedule referred to:-

> *"Documentation which in the ordinary course of business of the fifth, sixth and eighth defendants have possibly been lost, destroyed, or mislaid or which has not been*

retained or may have been overwritten prior to the commencement of these proceedings."

11. Mr. Millett further stated at para. 12 of his affidavit of discovery that the Millett defendants were not aware of any other documents which were in their possession, power or procurement. He concluded the paragraph by stating:-

"For the sake of completeness, the fifth, sixth and eighth named defendants [have] *not been able to conduct a search in relation to documents which were not retained by them, and/or were destroyed or were overwritten in the ordinary course of business, or were lost or mislaid prior to the commencement of these proceedings."*

12. The plaintiffs have focused for the purposes of the present application on one of the categories of documents which the Millett defendants were required by the order to discover, namely, category 3. Category 3 referred to documents relevant to the relationship between Mr. Desmond and Mr. Millett. Under category 3 of the order, the Millett defendants were required to make discovery of:-

"All documents, communications and correspondence exchanged between the second and fifth defendants in relation to the plaintiffs and their pension affairs and investments. For the avoidance of doubt, this category includes all mobile phone and email records from the relevant period."

13. Mr. Millett listed five documents under category 3 in the first part of the first schedule to his affidavit of discovery. The first document was described as follows:-

"Cyber attack report, Auth: Eamon Gallagher"

Apart from the reference to that report, there was no reference in Mr. Millett's affidavit of discovery to any alleged cyber attack experienced by the Millett defendants and no explanation of how that attack affected their ability to make the discovery ordered by the

court. There was no reference to the cyber attack in the letter enclosing Mr. Millett's affidavit of discovery and the discovery documents themselves.

14. The plaintiffs reviewed the discovery received from the Millett defendants and cross-referenced that discovery with the discovery received from Mr. Desmond. It became clear that the discovery made by the Millett defendants was much less extensive than the discovery received from Mr. Desmond and that significant communications between Mr. Desmond and Mr. Millett had not been discovered by Mr. Millett in his affidavit of discovery. While the plaintiffs complain in the present application that the report of Mr. Gallagher, referred to at item 1 under Category 3 in Mr. Millett's affidavit of discovery, was not provided with the other documents referred to in the affidavit, Mr. Millett believed that the report had been provided and claimed only to have become aware that it had not been when the plaintiffs brought the present application in late May, 2020. I do not accept that that belief was correct, as the correspondence to which I will shortly turn discloses that the plaintiffs' solicitors were seeking a copy of that report in correspondence sent in February, 2020, to which the Millett defendants' solicitors did not respond prior to the plaintiffs' application being issued in late May, 2020. However, I cannot help but feel that when the Millett defendants' discovery documents were provided with Mr. Millett's affidavit of discovery in May/June, 2019, the plaintiffs ought to have adverted to the fact that Mr. Gallagher's report was apparently not with those discovery documents. It is hard to accept that the plaintiffs could reasonably have understood that an exchange of emails between Mr. Millett and Mr. Gallagher from November 2016 concerning the ransomware attack amounted to Mr. Gallagher's report as referred to in the affidavit of discovery, as was subsequently claimed by the plaintiffs. The plaintiffs ought immediately to have sought clarification of the position from the Millett defendants and ought immediately to have requested a copy of Mr. Gallagher's report when it emerged that it was not contained in the discovery documents provided by the Millett

defendants as they claim. However, once it became clear to the Millett defendants (as it must have done on receipt of the plaintiffs' solicitors' letter of 10th February, 2020) that the plaintiffs did not have Mr. Gallagher's report, the Millett defendants ought immediately to have provided it. They did not and the plaintiffs' motion was ultimately issued in late May, 2020.

Correspondence Before Plaintiffs' Application

15. Following receipt and consideration of the Millett defendants' discovery documents, the plaintiffs' solicitors wrote to the Millett defendants' solicitors setting out their issues in relation to the discovery made by those defendants. There followed an exchange of correspondence between the parties.

16. The first letter in the sequence is a letter from the plaintiffs' solicitors dated 20th September, 2019. In that letter, the plaintiffs complained about the absence of documents falling within the scope of category 3 in particular (although, not limited to that category). The plaintiffs complained about the dearth of email correspondence between Mr. Millett and Mr. Desmond and the absence of telephone records and text messages in respect of communications between them, in circumstances where the plaintiffs were aware of their existence (through the discovery made by Mr. Desmond). The letter noted that Mr. Millett claimed that his devices were subject to a cyber attack which resulted in the loss or compromise of certain documents, although, it is unclear what information had been provided to the plaintiffs in relation to the cyber attack by that stage. It was noted that that issue had not been canvassed in correspondence during the discovery process. Reference was also made to a *"litigation hold"* which the Millett defendants had been requested to place on their documents (the relevance of the so-called *"litigation hold"* was disputed in the course of this application and it is, in my view, a red herring). The letter set out several queries which the

plaintiffs had in relation to the alleged cyber attack in the form of some 29 questions. The letter also noted that the plaintiffs did not accept that all emails and telephone records in respect of communications between Mr. Millett and Mr. Desmond were irretrievable and contended that those remained within the Millett defendants' power or procurement. The Millett defendants were requested to provide a supplemental affidavit of discovery. In the event that further documents were not in existence, the plaintiffs requested that a specific averment be made to that effect. It was noted that Mr. Millett's affidavit of discovery contained no averment in relation to the alleged cyber attack or in relation to the loss, corruption or absence of documents as a result of that alleged attack. The letter also stated that the plaintiffs would require inspection and searching facilities in respect of the Millett defendants' electronic documents and requested confirmation that such inspection would be facilitated.

17. There was no reply to that letter from the Millett defendants' solicitors and further letters were sent by the plaintiffs' solicitors on 15th October, 2019 and 14th November, 2019. The Millett defendants' solicitors finally replied on 21st November, 2019, pointing out that they had to seek assistance from Mr. Gallagher who they noted had provided the necessary IT services to the Millett defendants following the cyber attack. A substantive response was eventually sent on behalf of the Millett defendants on 2nd December, 2019. Some of the issues addressed in that letter are no longer relevant in light of the more confined and modified nature of the application pursued by the plaintiffs at the hearing, so it is unnecessary to deal at length with the letter. It is noted, however, that the response stated that the Millett defendants did not have access to either the handsets or to the telephone records and text messages in respect of communications between Mr. Millett and Mr. Desmond, that the devices used during the relevant time period were no longer in the Millett defendants' possession, that no backup of the devices was retained after the cyber attack and that all data

was permanently deleted as part of the *"sanitation process engaged in to restore the systems"*. The letter further stated that the eighth defendant replaced all of its IT hardware in February, 2017. The letter gave further information in relation to the cyber attack which occurred on the evening of 1st November, 2016, some eight months prior to the commencement of the proceedings. The letter then responded to the 29 questions raised in the plaintiffs' solicitors' September, 2019 letter. The letter concluded by stating that an affidavit was being prepared which would contain an averment confirming that the Millett defendants did not have access to any of the documentation on their server at the time of the cyber attack in November, 2016. That affidavit was not provided to the plaintiffs before the plaintiffs' motion was issued in late May, 2020. No explanation was provided for the failure to provide that affidavit.

18. The plaintiffs' solicitors replied on 10th February, 2020. They raised certain further queries arising from the Millett defendants' response. They requested a copy of Mr. Gallagher's report and noted that they had only seen an email from Mr. Gallagher to Mr. Millett in the discovery documents. They requested an affidavit from Mr. Gallagher verifying his report. They referred to a letter sent by the plaintiffs' former solicitors to Mr. Millett in March, 2015, which they maintained put the Millett defendants on notice of proceedings. The relevance of that "*litigation hold*" type letter was disputed in the course of this application and it does not seem to me ultimately to have any relevance to the issues I have to decide. If the Millett defendants' systems were subjected to a cyber attack as they allude, it would have made no difference whether documents stored on those systems were, or ought to have been, subject to a "*litigation hold*" or not.

19. The plaintiffs' solicitors' letter of 10th February, 2020 repeated the request for inspection of the Millett defendants' documents and devices and requested that access be provided to the plaintiffs' IT expert for the purpose of that inspection. The letter concluded

by noting that the supplemental affidavit of discovery referred to in the Millett defendants' solicitors' letter of 2nd December, 2019 was awaited. That letter attached copies of text messages between Mr. Millett and Mr. Desmond (which appeared to have been obtained by the plaintiffs from Mr. Desmond's discovery).

20. The correspondence ended there. No supplemental affidavit of discovery was provided and the plaintiffs issued the motion now before the court on 27th May, 2020.

Plaintiffs' Application as Issued

21. The plaintiffs issued their motion on 27th May, 2020. They initially sought a range of orders as follows:-

(1) An order pursuant to O. 31, r. 12 and/or O. 50, r. 4 and/or O. 63A, r. 5 RSC for inspection and search facilities by an independent expert of the Millett defendants' information technology devices and systems for the purposes of carrying out searches for data and emails alleged to have been damaged or destroyed in a cyber attack alleged to have occurred in or about November, 2016 as described in the affidavit sworn by Bernard McEvoy on 27th May, 2020 grounding the plaintiffs' application, including:-

(a) computer servers and mail servers at the Millett defendants' offices;

(b) information technology devices that were in use during the relevant period;

(c) all the Millett defendants' email addresses to include **[redacted]** and **[redacted]** and any other email addresses in existence; and

(d) a detailed explanation on affidavit as to:

(i) when the Millett defendants last had in their possession any electronically stored information or devices (including mobile

devices) on which discoverable electronically stored information is or was once located,

(ii) how such electronically stored information or devices (including mobile devices) came to no longer be in their possession,

(iii) the current whereabouts or what has become of such electronically stored information or devices (including mobile devices).

(2) In default of agreement between the parties, an order providing for the appointment of an independent expert nominated by the court to carry out such inspection;

(3) An order pursuant to the inherent jurisdiction of the court and/or O. 31, r. 12 RSC compelling the Millett defendants to make full and proper discovery by means of swearing a further supplemental affidavit setting out comprehensively:-

(a) the circumstances in which such data was lost or destroyed;

(b) the devices affected by any cyber attack;

(c) any reports generated in relation to the provenance and/or impact of such cyber attack; and

(d) the nature of the discoverable data relevant to this litigation which was destroyed.

(4) In the alternative, an order striking out the defence of the Millett defendants for failure to make proper discovery as required under the order of 22nd February, 2019.

The Evidence on the Plaintiffs' Application

22. The plaintiffs' application was grounded on an affidavit sworn by Bernard McEvoy, their solicitor, on 27th May, 2020. Mr. McEvoy outlined the complaints and queries in relation to the discovery made by the Millett defendants which had previously been set out in the correspondence sent on behalf of the plaintiffs. It was apparent from Mr. McEvoy's affidavit that the plaintiffs' complaints in relation to the adequacy of the discovery made by the Millett defendants were very much focused on category 3 of the discovery which they were required to make under the order of 22nd February, 2019. It was confirmed on behalf of the plaintiffs at the hearing of the application that the plaintiffs' complaints and the relief sought on this application were solely directed to category 3 and not to any of the other categories directed to be made under that order. It will be recalled that category 3 was directed to communications between Mr. Desmond and Mr. Millett in relation to the plaintiffs and their pension affairs and investments and was expressly stated to include all mobile phone and email records.

23. Mr. McEvoy noted that the discovery made by the Millett defendants was markedly less than that made by Mr. Desmond in respect of documents coming within category 3. Mr. McEvoy queried the absence of any reference to a cyber attack in the correspondence exchanged between the parties in relation to discovery prior to the order being made in February, 2019 and the absence of any reference to such an attack in Mr. Millett's affidavit of discovery or in the cover letter which provided that affidavit and the documents discovered to the plaintiffs. Mr. McEvoy made reference to certain documents emanating from Mr. Millett (and obtained from Mr. Desmond's discovery) which the plaintiffs contended suggested a desire on the part of Mr. Millett *"to minimise the documentary record of his role in matters"* (para. 15 of Mr. McEvoy's first affidavit). Having referred to the correspondence exchanged between the parties and to the absence of a satisfactory response from the Millett defendants,

Mr. McEvoy contended an inspection of the Millett defendants' *"devices"* by an independent expert was necessary to determine the *"exact details"* surrounding the cyber attack and to confirm that no other documents falling within the relevant category were in existence. It was contended that the Millett defendants were unclear in their responses to the queries raised on behalf of the plaintiffs and that they had not set out their position on affidavit.

24. Several rounds of affidavits then followed. In response to the plaintiffs' application, two affidavits were sworn on behalf of the Millett defendants, one by Mr. Millett on 22nd July, 2020 and another by Mr. Gallagher on 14th July, 2020. Mr. Gallagher swore another affidavit on 7th October, 2020. Mr. Millett swore two further affidavits: one on 9th October, 2020 and another (provided in unsworn form but subject to an undertaking to file a sworn version as soon as practicable) which was provided on the date of the hearing and was in response to a late affidavit provided on behalf of the plaintiffs.

25. In his first affidavit, Mr. Gallagher, a software engineer with a company called IT.ie, explained that a cyber attack was reported to his firm by the eighth defendant on 2nd November, 2016 and that an investigation was carried out which disclosed that the eighth defendant's server was *"completely encrypted by ransomware"* and that it was *"beyond recovery"*. Mr. Gallagher's firm began the process of *"rebuilding the system with new hard drives to return the network to a safe and normal operational level"*. He explained that the server was *"completely rebuilt with new hard drives"* and that the eighth defendant's computers and laptops were *"formatted and rebuilt"*. He explained that an *"onsite recovery and remediation"* of the issue was attempted on 4th November, 2016 which was unsuccessful. An offsite *"rebuild"* of the system was required and was completed on 9th November, 2016. Mr. Gallagher stated that *"all the data of the company on the server and machines was lost"* and that the *"document management system was without a recovery point"*. He referred to a report which he prepared for the eighth defendant in connection with the ransomware event

and exhibited that report which he verified in his affidavit. Mr. Gallagher's report bears the date 1st November, 2017 on its cover page (although the event occurred one year previously in November, 2016). This may simply be a typographical error. The report is a one-page document. In the report, Mr. Gallagher explained the nature of the ransomware event. He described it as *"a catastrophic experience"* for the eighth defendant and that it led to the *"loss of all data"*. He described it as a *"highly unusual experience mainly because of the complete and utter destructive nature of the attack"*. There was no ransom request which was unusual. The attack was *"malicious"* and *"did not have a recovery option"*. He stated that *"the ransomware was so pervasive, we (IT.ie) could not even connect a USB drive to the sever without it being completely encrypted"* and that the *"operating system was still working but it appeared to almost have been completely rewritten"*. They were never able to find out the source of the attack and felt that there was inadequate firewall protection.

26. Mr. Gallagher described the corrective measures taken which included completely rebuilding the server with new hard drives and formatting and rebuilding from scratch all of the laptops and desktop PCs. As regards data, Mr. Gallagher stated in the report as follows:-

> *"All company data was lost. The document management system (DOCTOPIA) was also without a recovery point. JMIFA* [the eighth defendant] *had thought the vendor was backing up the data but no such agreement had been formally put in place. There had been an external drive (x2) backup rotation setup when the server was originally installed. The staff at JMIFA would swap these out on a weekly basis. Unfortunately, this was never checked and although the backup drives were often swapped out, it is unknown if they ever worked at all. They were not actively monitored or checked by JMIFA or IT.ie. Again, there had been no formal agreement to do so. Only an offsite cloud backup of the server would have been sufficient as even the hard drive connected to the server was encrypted."*

27. In his first affidavit, Mr. Millett addressed the scope of the reliefs sought by the plaintiffs. With respect to the plaintiffs' application for inspection and search facilities, Mr. Millett stated that the eighth defendant's *"main server"* was *"replaced"* and that *"every system terminal was sanitised"* on Mr. Gallagher's advice and that the *"hardware itself"* was replaced in February, 2017 as it had come to the end of its standard life. I am assuming that the reference to the *"main server"* being *"replaced"* is intended to be a reference to the complete rebuilding of the server with new hard drives referred to by Mr. Gallagher in his report. The reference to the *"system terminals"* which were sanitised, I am assuming is a reference is to the laptops and desktop computers which were formatted and rebuilt as also noted by Mr. Gallagher. I am also assuming that the reference to *"hardware"* being replaced in February, 2017, is a reference to the laptops and desktop computers which (apart from one laptop) were replaced at that time and which are shown on the invoice exhibited at "JM1". I did not understand from Mr. Millett's affidavit or from the invoice attached that the server itself was replaced in February, 2017. I could not see any reference to a server in the invoice exhibited.

28. The affidavits also consider issues in relation to Mr. Millett's mobile phone which was apparently destroyed in an accident at Mr. Millett's home in 2015. However, while that issue was addressed in the affidavits, it was not pursued by the plaintiffs at the hearing so it is unnecessary for me to say anything more about Mr. Millett's mobile phone.

29. Mr. Millett objected to the plaintiffs request for inspection and search facilities in respect of the Millett defendants' email addresses on the basis that those email addresses would include all communications between Mr. Millett/the eighth defendant and their client base and third parties, including regulatory bodies. He averred (at para. 8 of his first affidavit) that, as part of the discovery process, the eighth defendant conducted a search of its server and *"provided everything found relevant to discovery raised by the plaintiffs which was*

downloaded and furnished to them" with Mr. Millett's affidavit of discovery. He further averred that *"there is no further material relevant to these proceedings on the server"* of the Millett defendants.

30. At para. 9 of his affidavit, Mr. Millett again explained that the *"computer hardware"* which was in use at the time of the ransomware attack was replaced and last in the possession, power or procurement of the eighth defendant in or about 2017 as it had come to the end of its standard life. He did, however, state that there is one laptop still in the possession of the eighth defendant. That laptop had been *"completely sanitised"* in line with Mr. Gallagher's advice. The evidence of Mr. Millett and of Mr. Gallagher in relation to the server and in relation to the one remaining laptop from the time of the cyber attack in November, 2016 is particularly relevant in light of the more refined and modified application pursued by the plaintiffs at the hearing.

31. A second affidavit was sworn by Mr. McEvoy in response on 31st August, 2020. An affidavit was also sworn on behalf of the plaintiffs by Declan Timmons, an information security consultant with Ward Solutions Limited, on 30th August, 2020. In his second affidavit, Mr. McEvoy offered the opinion that the confidentiality concerns expressed by Mr. Millett could be addressed by appropriate undertakings and confidentiality rings. Having considered the affidavits of Mr. Millett and Mr. Gallagher, Mr. McEvoy contended that inspection of the Millett defendants' devices by Mr. Timmons of Ward Solutions limited (who he described as an "*independent expert*") was necessary to determine *"the exact details surrounding the cyber attack alleged"* by the Millett defendants and contended that the Millett defendants were continuing to provide unsatisfactory responses to the plaintiffs' queries.

32. In his affidavit, Mr. Timmons considered Mr. Gallagher's first report and concluded that, in his view, there was a *"significant lack of detail in respect of the ransomware attack*

and its aftermath". He expressed the view that there would be *"considerable benefit in using Ward Solutions' IT experts to facilitate a search and inspection of the relevant devices at this juncture and that there is a likelihood that further relevant documents will be uncovered, based on documents already in discovery that suggest, that iCloud storage facilities were employed by* [Mr. Millett]*"* (para. 4 of Mr. Timmons' affidavit). The latter averment concerning the suggestion that iCloud storage facilities were employed by Mr. Millett appears to be a reference to Mr. Timmons' view (by reference to Apple's website) that Mr. Millett may have had the use of an iCloud account on his mobile phone. That issue was not pursued at the hearing of the application and, for that reason, I do not propose to consider it further.

33. Mr. Timmons prepared a detailed report which he exhibited to his affidavit. He raised several queries in relation to the nature of the alleged cyber attack, the steps taken to investigate and deal with the consequences of that attack and the possibility that some data might be capable of being retrieved by means of a digital forensics investigation. I will return to the detail of Mr. Timmons' report when considering the refined and modified relief pursued by the plaintiffs at the hearing. It is sufficient to point out at this stage that Mr. Timmons had queries in relation to the nature of the cyber attack and what was done to address it and as to the possibility that further data might be capable of being retrieved.

34. Mr. Millett swore his second affidavit on 9th October, 2020. In that affidavit, Mr. Millett provided more detail in relation to the ransomware attack of which he became aware on the morning of 2nd November, 2016 (para. 8 of Mr. Millett's second affidavit). He outlined what was done following the discovery of the attack and the steps taken in an attempt to preserve and recover the data on the server. He stated that there was no backup in place. IT.ie, Mr. Gallagher's firm, were *"immediately contacted and engaged to recover and remediate the computer system"*. He stated that the *"primary concern at this point was*

recovery of the system's data" which did not prove possible *"as the ransomware had encrypted it"*. Mr. Millett stated that *"in the direct aftermath of the ransom attack, the main server at the offices of the eighth named defendant was replaced and every systems terminal was sanitised on the advice of Mr. Gallagher"*. Again, I am assuming that the reference to the *"main server"* being "*replaced*" is a reference to the work done by Mr. Gallagher following his engagement to remove the hard drives from the server and to rebuild the server with refurbished hard drives sourced by Mr. Gallagher's firm as described in his two reports. I do not understand from the evidence that the server was replaced in the same way as the devices were replaced in February, 2017. Mr. Millett explained that the *"hardware"* (which I understood to be items such as the laptops and desktop computers which were purchased in 2012) were replaced in 2017 and were discarded at a recycling point, with the exception of one laptop from the time of the attack which remains in the possession of the Millett defendants and which is one of the main targets of the plaintiffs' refined application. Mr. Millett repeated the concern that any inspection and search of the server for emails would involve access to confidential and sensitive material, including clients and communications with regulatory bodies and would involve access to material going far beyond the scope of the discovery ordered and the issues in the proceedings. He further maintained that the inspection and search facilities sought by the plaintiffs in their application would be pointless and fruitless in light of the consequences of the ransomware attack and the steps taken following that attack to replace and rebuild the server and to replace the devices (with the exception of the laptop).

35. In his second affidavit, sworn on 7th October, 2020, Mr. Gallagher referred to and exhibited a second report which he prepared in response to Mr. Timmons' report. In his second affidavit and in his second report, Mr. Gallagher pointed out that his firm had been engaged as a *"break-fix contractor"* and not as a provider of managed services to the eighth

defendant or to any of the Millett defendants. He felt that the level of detail concerning the cyber attack requested by Mr. Timmons in his report was more in the nature of detail and information which might be expected from a multinational organisation rather than a business the size of the eighth defendant. Apart from making those overarching points, Mr. Gallagher's second report sought to address each of the main observations and findings made by Mr. Timmons. It will be necessary to refer to some of these when addressing the relief pursued by the plaintiffs at the hearing. It is sufficient to note at this stage that Mr. Gallagher attempted to provide a detailed and comprehensive report to the queries raised by Mr. Timmons. I have no reason to believe that Mr. Gallagher did not do so in a reasonable and genuine attempt to assist the court and to respond to the queries raised by Mr. Timmons on behalf of the plaintiffs.

36. Mr. Gallagher attached to his second report some documents which included emails which he exchanged with Mr. Millett in early November, 2016 following the discovery of the ransomware attack. Mr. Millett had sent those emails to Mr. Gallagher from an iPad device. This prompted Mr. McEvoy to swear a third affidavit on 5th November, 2020. That affidavit was not provided for in the directions for the hearing made by the court on 5th October, 2020 and was provided a few days before the hearing date. The Millett defendants objected to the use of Mr. McEvoy's third affidavit. It was urged on their behalf that the court should exclude that affidavit but that if the court was disposed to allow the plaintiffs to rely on it, the Millett defendants should be entitled to put in a further affidavit from Mr. Millett in response (which had been prepared but not sworn in light of the objection raised to the admissibility of Mr. McEvoy's affidavit). I ruled that, although not provided for in the directions made by the court on 5th October, 2020, and although the parties had not mentioned the issue at the callover on 6th November, 2020, no injustice would be caused to the Millett defendants if I were to permit the plaintiffs to rely on Mr. McEvoy's affidavit, in circumstances where a

response had already been prepared. I allowed the plaintiffs to rely on the affidavit and the Millett defendants to rely on an unsworn affidavit of Mr. Millett, subject to the Millett defendants' solicitor's undertaking to have that affidavit sworn and filed as soon as practicable.

37. In his third affidavit, Mr. McEvoy referred to the two emails sent by Mr. Millett from his iPad which were attached to Mr. Gallagher's second report. He stated that the iPad had not been referred to previously in correspondence, in Mr. Millett's affidavit of discovery or in the affidavits sworn in connection with the plaintiffs' application and it was contended that Mr. Millett had failed to account for all devices on which discoverable data was stored. In addition to raising an issue in relation to Mr. Millett's iPad, Mr. McEvoy's affidavit also continued to raise issues in relation to Mr. Millett's mobile phone and in relation to the external hard drives which were in existence as backup (but which, it was said, did not actually backup any data) at the time of the ransomware attack. Although those two issues were raised in Mr. McEvoy's last affidavit, they were not ultimately pursued by the plaintiffs at the hearing.

38. In his final affidavit in response, Mr. Millett addressed the issues raised in relation to his iPad which he said had been used *"occasionally out of office for work related activities in the absence of other devices"* and was *"never connected to the companies (sic) servers"* so that *"no files could have been either linked or would have been retained on the device during* [the relevant] *period"*. Mr. Millett stated that the emails sent from the iPad were sent by him to Mr. Gallagher during the ransomware attack when the computer systems were down. He also confirmed that the iPad was *"checked to ensure that no relevant information relating to the plaintiff's discovery was contained on it"* and that the email account is *"exactly the same email account loaded onto the phone and laptop and contains only that information"*. He further stated that there were and never had been any other email addresses on the iPad.

Finally, he explained that he purchased the iPad on 17th December, 2013 and traded it in with Apple for a new iPad on 1st July, 2019. Finally, Mr. Millett also addressed the issues raised by Mr. McEvoy in relation to his mobile phone and in relation to the external hard drives which have not been pursued by the plaintiffs.

39. That is the affidavit evidence exchanged between the parties for the purpose of the plaintiffs' application.

Modification of the Plaintiffs' Application at the Hearing

40. At the outset of the hearing, the plaintiffs' counsel explained that, in light of the evidence provided by Mr. Gallagher on behalf of the Millett defendants, the plaintiffs had decided to confine their application to seeking inspection and search facilities by an independent IT expert in respect of:-

(1) the current servers (or server) operated by the Millett defendants; and

(2) the one laptop which remained from the time of the ransomware attack in November, 2016;

(3) Mr. Millett's iPad.

41. When faced with the averment by Mr. Millett in his final affidavit that the iPad had been traded in with Apple and replaced by a new device in July, 2019, the plaintiffs' counsel acknowledged that an inspection and search of that device would no longer be possible and instead, stated that what the plaintiffs were seeking was a further affidavit from Mr. Millett setting out more information concerning the iPad in use between 2013 and July, 2019, the searches which had been undertaken in respect of that iPad when discovery was made by the Millett defendants in May, 2019 and the reason why it was not referred to in Mr. Millett's affidavit of discovery.

42. Before considering the legal principles applicable to the plaintiffs' application and the submissions advanced by the parties on the orders pursued by the plaintiffs at the hearing, it is appropriate that I record that the plaintiffs were not seeking to strike out the defence of the Millett defendants for failure to comply with the order for discovery and were not seeking any relief in relation to the other technology systems or devices referred to in the affidavits, such as the external hard drives or Mr. Millett's mobile phone. It is also appropriate that I record that the plaintiffs confirmed at the hearing that the deficiencies in the discovery alleged against the Millett defendants were confined to the discovery made in respect of category 3 of the order of February, 2019.

Relevant Legal Principles

43. In their notice of motion, the plaintiffs relied in support of their application for an order permitting inspection and search facilities by an independent expert of the current servers, the laptop and Mr Millett's iPad on certain provisions of the Rules of the Superior Courts (the "RSC"), namely, O. 31, r. 12, O. 50, r. 4 and O. 63A, r. 5. However, in their written submissions, the plaintiffs did not explain how any of those provisions of the RSC applied or permitted the court to make the inspection and search order sought. Rather, the plaintiffs relied on the inherent jurisdiction of the court to direct further and better discovery and to make orders, including an order permitting an independent expert to carry out an inspection and search of information systems. In their oral submissions, the plaintiffs maintained that the court had the power to grant the orders sought under the provisions of the RSC referred to in the notice of motion and under the inherent jurisdiction of the court.

44. In their written submissions, the Millett defendants did not dispute the applicability of the provisions of the RSC referred to in the plaintiffs' notice of motion, although they did argue that the orders sought should not be granted under those provisions. In their oral

submissions, however, the Millett defendants argued that the relevant legal principles were those applicable to the court's inherent jurisdiction to direct further and better discovery. They relied in that respect on a judgment I delivered in *Victoria Hall Management Limited & ors v. Cox & ors* [2019] IEHC 639 (upheld on appeal by the Court of Appeal [2020] IECA 79) ("*Victoria Hall*").

45. I have considered the plaintiffs' application by reference to the court's inherent jurisdiction and the legal principles governing applications for further and better discovery which I will sketch out below. I do not believe that O. 31, r. 12 has any relevance to the plaintiffs' application. Order 31, rule 12 is directed to applications for discovery and not to an application where it is contended that the discovery made is inadequate or deficient in some respect. That is clear from the terms of O. 31, r. 12(1). While O. 31, r. 12(2) expressly deals with the situation where the discovery sought to be ordered includes electronically stored information, it is clear from the opening words of para. (2) that that provision applies to the hearing of an application for discovery under O. 31, r. 12(1). Order 31, rule 12(3) which does contain provisions allowing for inspection and searching of documents to be undertaken by an independent expert, again, only applies to an application for discovery of electronically stored information. It does not, directly at least, apply to an application made by one party who alleges that the other party has failed properly to comply with an agreement or order for discovery. The plaintiffs' application is not an application for discovery falling under O. 31, r. 12. Therefore, the provisions of O. 31, r. 12 do not apply.

46. Order 50, rule 4 provides that the court may make an order for the *"detention, preservation, or inspection of any property or thing, being the subject of such cause or matter, or as to which any question may arise therein"* and provides further for what an order under that provision may permit. The court can make an order under that provision for inspection of computer files and programmes: *SoftCo v. DHL Information Services (Europe)*

s.r.o. [2013] IEHC 623 (Ryan J.). However, the plaintiffs did not actually advance any submissions to the court as to the application of this rule to the particular circumstances of this case and I am doubtful as to whether the provision is applicable, in circumstances where the case being made is that the discovery made by one party is inadequate. That seems to me to be an issue more appropriately dealt with in the context of the principles applicable to applications for further and better discovery. However, it is unnecessary for me to reach any definite conclusion on the scope of the application of O. 50, r. 4 as that provision was not relied upon by the plaintiffs in its written or oral submissions to the court.

47. The third provision of the RSC referred to in the notice of motion is O. 63A, r. 5. That is the general provision which empowers the court, dealing with cases in the Commercial List, to *"give such directions and make such orders, including the fixing of time limits, for the conduct of proceedings entered in the Commercial List, as appears convenient for the determination of the proceedings in a manner which is just, expeditious and likely to minimise the costs of those proceedings"*. That rule encapsulates the three underlying imperatives for cases admitted to the Commercial List, as discussed by McKechnie J. in the Supreme Court in *Ryanair Limited v. Bravofly Limited* [2016] IESC 53. At para. 42 McKechnie J. described those imperatives as follows:-

> *"Firstly, that the parties should engage in a fair trial of the issues so identified; secondly, that such issues should be dealt with and disposed of with reasonable expedition; and, thirdly, that costs should be reduced so far as possible in such litigation…"* (per McKechnie J. at para. 42)

48. However, O. 63A, r. 5 in itself does not confer any power on the court to make an order such as the inspection and search order sought by the plaintiffs. Rather, orders which the court can make under its inherent jurisdiction or under specific provisions of the RSC should, in the case of cases admitted to the Commercial List, be consistent with the three

imperatives just referred to. Again, however, no submission was addressed by the plaintiffs to the effect that O. 63A, r. 5 actually empowers the court to make the inspection and search order sought. I do not believe that it does but I will refrain from expressing a concluded view on that issue here, as it is unnecessary for me to do so.

49. I accept the submission advanced by the Millett defendants that the court should approach the plaintiffs' application as it would an application for further and better discovery. Indeed, that was ultimately the point at which the plaintiffs' submissions ended up as they urged the court to exercise an inherent jurisdiction to grant the reliefs which they were seeking.

50. There is no specific provision in the RSC conferring power on the court to make an order for further and better discovery in circumstances where the discovery originally made is inadequate or deficient in some respect. There is a provision in the RSC which confers an express power on the court to vary the terms of an order or agreement for discovery where it is satisfied that further discovery is necessary or where the discovery originally ordered or agreed is unreasonable. That power is conferred by O. 31, r. 12(11) and was considered by the Court of Appeal in *Hireservices E and Hireservices I Limited v. An Post* [2020] IECA 120 ("*Hireservices* ") (see paras. 16 to 18 of the judgment of Murray J.). However, that provision does not confer an express power on the court to direct further and better discovery where the discovery originally made is inadequate or deficient. In such a case, the court does have the power under O. 31, r. 21 to dismiss an action or to strike out a defence. However, the court will only exercise that power in exceptional circumstances. While initially seeking such an order in their notice of motion, the plaintiffs sensibly did not pursue an application to strike out the Millett defendants' defence.

51. It is, however, well-established that the court has an inherent jurisdiction to direct further and better discovery where the discovery made on foot of an order or agreement for discovery is inadequate or deficient. I accept the submission advanced by the plaintiffs that the court's inherent jurisdiction in that regard is extensive and can include, in very exceptional cases, an order directing cross-examination of a deponent on an affidavit of discovery (*Duncan v. Governor of Portlaoise Prison* [1997] 1 IR 558). I also accept that the court will be flexible in fashioning remedies which are capable of dealing with technological advancements. In the Supreme Court in *Dome Telecom Limited v. Eircom Limited* [2008] 2 IR 726, ("*Dome Telecom "*) Geoghegan J. stated:-

> *"I would reject any idea that the right to discovery of documents should be exclusively based on an interpretation (literal or otherwise) of the relevant rule of court… In modern times, courts are not necessarily hidebound by interpretation of a particular rule of court. More general concepts of ensuring fair procedures and efficient case management are frequently overriding considerations. The Rules of Court are important and adherence to them is important but if an obvious problem of fair procedures or efficient case management arises in proceedings, the court, if there is no rule in existence precisely covering the situation, has an inherent power to fashion its own procedure and even if there was a rule applicable, the court is not necessarily hidebound by it. It is common knowledge that a vast amount of stored information in the business world which formerly would have been in a documentary form in the traditional sense is now computerised. As a matter of fairness and common sense the courts must adapt themselves to this situation and fashion appropriate analogous orders of discovery…"* (per Geoghegan J. at 735-736)

52. The Supreme Court in *Dome Telecom* was dealing with an application for discovery and not an application for further and better discovery on foot of an order already made but,

nonetheless, the principle is equally applicable to the court's inherent power to fashion an appropriate remedy to address particular issues to which discovery of electronically stored information may give rise. It should also be noted that in *Dome Telecom*, the Supreme Court confirmed the importance of ensuring that the order for discovery made was proportionate. The majority held that the particular order sought by the plaintiff in that case was not necessary or proportionate at that stage of the proceedings for various reasons. While Geoghegan J. dissented on the ultimate decision of the Supreme Court, his comments in terms of the court's wide powers to address the court's powers to deal with discovery issues thrown up by technological developments are in no way undermined by his dissent on the ultimate decision.

53. I accept that, in an appropriate case, the court does have an inherent power to order the inspection and search by an independent IT expert of computer systems, devices and data to ensure compliance with an order or agreement for discovery. In *Pat O'Leary v. Volkswagen Group Ireland Limited* [2015] IESC 35 ("*O'Leary*"), the Supreme Court upheld the decision of the High Court that it was not necessary in that case for the plaintiffs' IT expert to have access to the defendants' computer records and systems. The Court held that the plaintiff had established no grounds whatsoever for making any such order and that there was nothing in the evidence to suggest that the defendant had acted other than *bona fide* and to the best of its ability in seeking to comply with the order for discovery (per Laffoy J. at para. 65 of the judgment). The Court did not, expressly at least, rule out that in an appropriate case, such an order could be made. Such an order was made by the High Court (Keane J.) in *Gallagher v. Raidió Teilifís Éireann* [2017] IEHC 237 ("*Gallagher*") in the particular circumstances of that case.

54. Therefore, I accept that the court has an inherent jurisdiction to make an order of the type sought by the plaintiffs providing for an independent IT expert to inspect and search

computers, computer systems, data and devices in circumstances where it is satisfied that the discovery made continues to be inadequate and that insufficient steps have been taken to address the identified deficiencies. However, before the court can consider making such an order, it must be satisfied that it is necessary, appropriate and proportionate to do so. Before it can reach that conclusion, it seems to me that the court must be satisfied that the party seeking such an order has met the threshold for establishing an entitlement to further and better discovery. If it does, the question then arises as to the precise nature of the relief or remedy which should be granted to address the continued inadequacy or deficiency in the discovery made.

55. I set out the principles applicable to applications for further and better discovery in *Victoria Hall* (paras. 16 to 22). The Millett defendants rely on the principles summarised by me in that case. Although the plaintiffs did not originally rely on those principles in support of their application, they appeared to accept, as I believe they had to, that the court must first consider whether the plaintiffs had established an entitlement to an order for further and better discovery before going on to consider what order should be made to remedy the situation. Logically, therefore, the plaintiffs had to accept that they were first required to establish an entitlement to an order for further and better discovery. That entitlement must be assessed by reference to the principles applicable to applications for further and better discovery which were summarised by me in *Victoria Hall* and subsequently by Murray J. in the Court of Appeal in *Hireservices*.

56. The relevant principles were very clearly set out by the Supreme Court in *O'Leary*. In her judgment in the Supreme Court in *O'Leary*, Laffoy J. quoted with approval the following summary of the circumstances in which it is appropriate to make an order for further and better discovery which were set out by Kenny J. in *Sterling-Winthrop Group Limited v.*

Farbenfabriken Bayer AG [1967] IR 97 ("*Sterling-Winthrop*"). Those circumstances were summarised by Kenny J. as follows:-

> *"The Court will, however, order a further affidavit of documents when it is satisfied (a) from the pleadings, (b) from the affidavit of discovery already filed, (c) from the documents referred to in the affidavit of discovery, or (d) from an admission by the party who has made the affidavit of discovery that the party against whom the order is sought has other documents in his possession relating to the issues in the action which have not been disclosed by the first affidavit. The Court will also order a further affidavit when there are grounds, derived from the documents discovered, for suspecting that there are other relevant documents in the possession of the party who has made the affidavit or where there are reasonable grounds for believing that the person making the affidavit of discovery has misunderstood the issues in the case and has, in consequence, omitted documents from it."* (per Kenny J. at 100)

57. Kenny J. further stated:-

> *"The authorities which I have mentioned establish that the Court should not order a further affidavit of documents unless it has been shown that there are other relevant documents in the possession of the defendants or that the person making the affidavits has misunderstood the issues in the action or that his view that the documents are not relevant is wrong…"* (per Kenny J. at 105)

58. That summary of the position was approved by the Supreme Court in *Phelan v. Goodman* [2000] 2 IR 577 ("*Phelan*"). It was also approved by the Supreme Court in *O'Leary*. In *Phelan*, Murphy J. in the Supreme Court considered two situations which frequently arise on applications for further and better discovery. The first is where the deponent of the affidavit avers that the party ordered to make discovery has documents but they do not require to be discovered as they are irrelevant. The second is where the deponent

avers that the party required to make discovery has no documents. The position in the present case is more akin to the second situation referred to than the first. With regard to the second situation, Murphy J. stated in *Phelan*:-

> *"Difficulties obviously arise in directing the discovery of documents or a particular range or class of document which the deponent denies are in his possession. To order the first defendant to swear a further affidavit of discovery presumably would result in his repeating the statements made and sworn by him on several occasions, namely, that he has not and never had any documents in addition to those already discovered in his power or possession relating to the matters in issue in the present proceedings. In those circumstances the Court would have to be satisfied on the evidence before it that it was making a meaningful order."* (per Murphy J. at 584)

59. In *O'Leary*, Laffoy J. stated that the test for the court in determining whether further and better discovery should be directed and whether orders should be made to remedy the situation is:-

> *"…whether the evidence presented to the High Court was insufficient to satisfy the Court that relevant documents are or have been in the possession of the Defendant which should have, but have not, been discovered in its original affidavit of discovery or its supplemental affidavit of discovery."* (per Laffoy J. at para. 56)

60. As noted earlier, Murray J. in the Court of Appeal in *Hireservices* concisely summarised the relevant principles by reference to *Sterling-Winthrop, O'Leary* and *Victoria Hall*, as well as a number of other cases (see paras. 13 to 15 of the judgment of Murray J.).

61. It is clear from all of these cases, and was explicitly stated by Murray J. in *Hireservices*, that the burden of showing that there are documents which ought to have been, but were not, discovered rests on the moving party. That party failed to discharge the burden in *Hireservices*. The burden of demonstrating that the Millett defendants are likely to have

further documents or data from which discoverable material could be obtained and which has not been discovered rests on the plaintiffs as the moving party on the application. So too must the plaintiffs demonstrate that the order which the plaintiffs have asked the court to make will be a *"meaningful order"* (as required by Murphy J. in *Phelan*).

62. In addition to discharging this burden, the plaintiffs must also demonstrate that the relief which they seek is necessary, appropriate and proportionate in all of the circumstances. It is relevant in that context that some of the material (to use that term in its broadest sense) to which the plaintiffs seek access on foot of the inspection and search order sought by them undoubtedly includes material which would not fall under category 3 of the discovery ordered to be made (which is the only category relied on by the plaintiffs) and that some of the material is undoubtedly confidential and refers to third parties and regulatory bodies. This is particularly so in the case of material on the eighth defendants' server and also on the laptop. I must take this into account in assessing the necessity, appropriateness and proportionality of the inspection and search order sought by the plaintiffs. While the confidentiality of the material does not amount to a bar on the making of the order sought (and the Millett defendants did not so contend), the existence of confidential material is a factor which the court must take into account in the balance in determining whether the order should be made in the first place (see in a different context: *Hartside Limited v. Heineken Ireland Limited* [2010] IEHC 3; *National Education Welfare Board v. Ryan* [2008] 2 IR 816; and *Moorview Developments Limited v. First Active PLC* [2008] IEHC 211 (all High Court (Clarke J.)). I accept of course that if the order sought is made, steps can be taken to protect the confidentiality of the material disclosed by any inspection and search and that an appropriate "*confidentiality ring*" limiting access to the material obtained on foot of the order could be put in place (see, recently: *Goode Concrete v. CRH PLC & ors* [2020] IECA 56). The Millett defendants submitted that, if the court were disposed to make the orders sought

by the plaintiffs, they should be given an opportunity to address the court on the precise order to be made and on the measures which should be put in place to preserve and protect the confidentiality of some of the material involved.

63. Finally, in assessing the necessity, appropriateness and proportionality of the order sought by the plaintiffs, it seems to me that I must also take into account the fact that the plaintiffs have obtained discovery from Mr. Desmond of documents from Mr. Desmond's side referable to the communications between him and Mr. Millett. These are the counterparties to the documents sought from Mr. Millett under category 3 of the order. While I completely accept the plaintiffs' submission that the fact that discovery is obtained from one party to a series of communications does not undermine the importance or utility of obtaining discovery from the other party to those communications, I do believe that it is relevant to include in the balance in determining the necessity, appropriateness and proportionality of the relief sought to take account of the fact that the plaintiffs have obtained discovery of documents held by Mr. Desmond in respect of his communications with Mr. Millett. This is particularly where one of the objectives of the orders sought is to permit an independent IT expert to examine file remnants which might be retrieved on a digital forensic investigation and which might yield file remnants which were encrypted during the ransomware attack. In deciding whether an order which would provide for such an exercise to be carried out is proportionate, I do believe that I am entitled to take into account that the plaintiffs already have documents referable to the communications between Mr. Millett and Mr. Desmond from Mr. Desmond's discovery. This is by no means a decisive factor to take into account, but it is one of the factors which I must consider in the balance.

64. These are the principles which I will apply now in determining the relief which the plaintiffs pursued at the hearing before me on 10th November, 2020.

Discussion and Conclusions on Reliefs sought by Plaintiffs

65. Before turning to the specific orders pursued by the plaintiffs at the hearing on 10th November, 2020, it is necessary for me to set out my findings on a number of important issues.

66. First, I am satisfied that Mr. Millett's affidavit of discovery was seriously deficient in failing to make any reference to the cyber attack which affected the Millett defendants' IT infrastructure and systems in early November, 2016. In fairness, through their counsel, the Millett defendants accepted at the hearing of the plaintiffs' application that the affidavit of discovery was not satisfactory in that respect. It is surprising to say the least that no reference whatsoever to the cyber attack was contained in the affidavit of discovery or in the cover letter dated 31st May, 2019 under which the affidavit was furnished to the plaintiffs' solicitors with the discovery documents. Not only that, there was no reference by the Millett defendants to the cyber attack in (a) the correspondence which preceded the plaintiffs' motion for discovery dated 20th September, 2018, (b) the correspondence between the date the plaintiffs' motion for discovery was issued and the date of the order made by the High Court on 22nd February, 2019, (c) the correspondence between the date of that order and the date on which Mr. Millett's affidavit of discovery was sworn on 31st May, 2019, and (d) the correspondence following the provision of Mr. Millett's affidavit of discovery on 31st May, 2019 and the date on which the plaintiffs' solicitors first took issue with the discovery on 20th September, 2019. However, despite all of that, Mr. Millett did refer to Mr. Gallagher's report on the cyberware attack at item 1 of category 3 in the first part of the first schedule to the affidavit of discovery and it was the intention of the Millett defendants that the report be included in the discovery documents furnished to the plaintiffs with the affidavit of discovery at the end of May, 2019. The reference to Mr. Gallagher's report and the evidence concerning Mr. Millett's (apparently mistaken) understanding that the report had been furnished with the discovery

documents is inconsistent with any attempt to mislead the plaintiffs or to withhold relevant information concerning the attack. Indeed, there is no conceivable reason for the Millett defendants to hold back or conceal that information since they rely on it to explain the paucity of responsive documents under category 3. Despite this, however, I am satisfied that Mr. Millett's affidavit of discovery was seriously deficient and that, as a consequence, the discovery originally made by the Millett defendants in late May, 2019 was seriously deficient.

67. Second, on an application for further and better discovery, which the plaintiffs' application is, in effect, (however framed), it is wrong in principle to focus only on the affidavit of discovery and the discovery originally made by the party in default. It is necessary also to consider the response by the defaulting party to the complaints made about its discovery. In my view, on this application, the plaintiffs focused unduly on the original affidavit of discovery and did not fully take into account the responses made and the measures taken by the Millett defendants to address the serious deficiency in Mr. Millett's affidavit of discovery.

68. Having reviewed the correspondence between the parties following the plaintiffs' solicitors' letter of 20th September, 2019 raising issues in relation to the adequacy of the discovery made by the Millett defendants, I have concluded that the response of the Millett defendants was initially inadequate. It took more than two months for the Millett defendants' solicitors to respond substantively to the plaintiffs' complaints. The first such substantive response was in the Millett defendants' solicitors' letter of 2nd December, 2019. While I accept that that letter did require input from Mr. Gallagher, the IT expert retained by the Millett defendants, it is difficult to see how it took so long to reply to the queries and complaints made by the plaintiffs. The failure by the Millett defendants to respond to the further letters sent by the plaintiffs' solicitors on 10th February, 2020 raising further queries

arising from the letter of 2nd December, 2019 exemplified the unsatisfactory nature of the Millett defendants' response to the queries raised. Their failure to provide Mr. Gallagher's report, despite the request for the report contained in the letter of 10th February, 2020, was unsatisfactory and without justification. The Millett defendants' solicitors did not bother to reply to the letter of 10th February, 2020 or to the subsequent letter dated 5th March, 2020. Nor was the supplemental affidavit of discovery referred to in the December, 2019 letter ever provided. In those circumstances, the plaintiffs had no alternative but to issue their motion on 27th May, 2020. In my view, the plaintiffs were entirely justified in issuing the motion.

69. Third, regard must, however, be had to the responses then made to the Millett defendants to the issues raised by the plaintiffs. Mr. Millett swore three affidavits in response to the application. Two affidavits were sworn by Mr. Gallagher which exhibited the two reports which he prepared. One of those reports provided information concerning the ransomware attack itself and the measures taken by Mr. Gallagher at the time at the request of the Millett defendants. The second report provided a detailed and comprehensive response to the report of Mr. Timmons of Ward Solutions, being the person the plaintiffs wished to have appointed as the independent expert to carry out the inspection and search of the Millett defendants' IT systems and devices.

70. I am satisfied that the Millett defendants have responded to the complaints made and the queries raised by the plaintiffs in relation to the discovery issues arising in respect of category 3 of the order for discovery made and that they have done so in a reasonable, comprehensive and realistic manner. I accept that, save for one minor respect, the Millett defendants have done the best that they could in the circumstances in responding to the complaints made and queries raised by the plaintiffs and have, where appropriate, provided expert evidence in support of their position. This is an important consideration to bear in mind when addressing the reliefs which the plaintiffs pursued at the hearing.

71. Fourth, while the affidavits sworn by the plaintiffs in support of the application and the written and oral submissions advanced on their behalf sought to cast some doubt about the occurrence of the cyber attack in early November, 2016, it was ultimately confirmed on behalf of the plaintiffs at the hearing that the plaintiffs were not seeking to make the case that the cyber attack did not occur at all. It was clarified that the plaintiffs were making the case that one would have expected more information and greater detail concerning the attack to have been provided by the Millett defendants at the outset and that the plaintiffs were entitled to the inspection and search order sought in order to confirm the detail of what was being said by the Millett defendants about the attack. Nonetheless, the plaintiffs continued to refer to what their counsel described as *"curious features"* about the attack, noting, for example, that the ransomware attack was unusual in that no ransom demand was made.

72. I should record that, for the purpose of this application, I accept that the attack did occur in the manner explained on affidavit by Mr. Millett and by Mr. Gallagher. The plaintiffs did not seek to cross-examine Mr. Millett or Mr. Gallagher on their affidavits and, it seems to me, that I must, for the purpose of this application, accept their evidence that the attack did occur: see, for example, *Boliden Tara Mines Limited v. Cosgrove* [2010] IESC 62; *RAS Medical Limited trading as Park West Clinic v. Royal College of Surgeons in Ireland* [2019] IESC 4; *Cork Harbour Alliance for a Safe Environment v. An Bord Pleanála* [2019] IEHC 85; and *Perrigo Pharma International DAC v. McNamara & ors* [2020] IEHC 552. That is not to say that at the trial it would not be open to the plaintiffs to challenge the fact and extent of the ransomware attack in the proper way. However, having chosen not to seek to cross-examine Mr. Millett or Mr. Gallagher, it seems to me that the plaintiffs must accept, for the purposes of this application, that the attack did occur. However, it was of course open to the plaintiffs to challenge the claimed consequences and effects of the attack and to query the extent of the data which may or may not be retrievable following the attack.

73. Having made those findings and conclusions, I turn to the reliefs pursued by the plaintiffs at the hearing.

74. The plaintiffs sought an order providing for the inspection and search by Mr. Timmons of Ward Solutions (or some other IT expert appointed by the court) to search (a) the Millett defendants' current server or servers and (b) the one laptop which remains in the possession of the Millett defendants from the time of the cyber attack in early November, 2016 for data and emails falling within category 3 of the order for discovery alleged to have been damaged or destroyed in the attack. In light of the information contained in Mr. Millett's most recent affidavit (his third affidavit) concerning his iPad which was traded in in July, 2019 and is no longer in his possession, the plaintiffs have asked the court to direct Mr. Millett to swear a further affidavit setting out further information in relation to the iPad, to material which may have been contained on the iPad and to the circumstances in which the iPad was checked for the purposes of Mr. Millett's affidavit of discovery.

75. I will address the relief sought in relation to the current server or servers and the laptop first and will then consider the iPad.

(a) <u>The Current Server/Servers</u>

76. There is some confusion in the material before the court as to whether the plaintiffs seek access to the Millett defendants' current server (singular) or servers (plural). That confusion appears throughout the affidavits and the written submissions of both sides as well as in the oral submissions. My understanding of the correct position is derived from the reports of Mr. Gallagher and from Mr. Timmons' report. Those reports all refer to the server in the singular rather than the plural (see, for example, Mr. Gallagher's first report, paras. 2.6.7, 2.6.9 and 2.8 of Mr. Timmons' report and pp. 6, 7, 10, 11, 13 and 14 of Mr. Gallagher's second report; see also the letter from the Millett defendants' solicitors to the plaintiffs' solicitors dated 2nd December, 2019). I will proceed on that basis.

77. In his first affidavit and in his first report, Mr. Gallagher explained that the ransomware attacked and completely encrypted the server and that it was not possible even to connect a USB drive to the server without it also being completely encrypted. He explained that the server was beyond recovery and all data was lost. While it had been thought that the data was being backed up through two external drives which ought to have been rotated, it appears that was never done. The server was rebuilt by Mr. Gallagher's firm and new hard drives were installed. In his second report, he explained that they *"most likely used refurbished cleaned/tested drives during the rebuild of the server that we had in-house"* and that they would not have charged for those (p. 13 of Mr. Gallagher's second report). Earlier in that report (at p. 5), he had stated that they had used *"refurbished (fully tested) drives from our HQ"*. He explained that the hard drives removed from the server (apparently there were two) were replaced as the server was *"still actively encrypting anything connected to it"* (p. 13) and that the hard drives removed from the server were sent for recycling (pp. 13-14).

78. In his report, Mr. Timmons raised various queries concerning the server and the hard drives removed from the server as well as those used to rebuild the server. Mr. Gallagher sought to address those queries in his second report. I am satisfied that he did so in a reasonable manner and to the best of his ability.

79. As I indicated earlier, there was a suggestion at para. 7 of Mr. Millett's first affidavit and at para. 8 of his second affidavit that the *"main server"* was replaced following the ransomware attack, I have set out what I understand to have occurred by reference to Mr. Gallagher's report and have proceeded on the basis that the reference by Mr. Millett to the "*main server*" being *"replaced"* was intended to be synonymous to the rebuild which Mr. Gallagher's firm did following the attack, which involved the removal and replacement of the hard drives contained in the server. Mr. Millett has averred (at para. 8 of his first affidavit) that the eighth defendant conducted a search of the server as part of the discovery process and

that *"everything found relevant to discovery raised by the plaintiffs"* was *"downloaded and furnished to them by affidavit of discovery dated 31 May 2019"* and that *"there is no further material relevant to these proceedings on the server of the* [Millett defendants]*"*. While the relevant time period for the communications sought is not expressly stated in category 3, the communications to which reference was made in Mr. McEvoy's first affidavit span a period between 2013 and August, 2016, pre-dating the date of the cyber attack.

80. On the basis that my understanding of what occurred is as described by Mr. Gallagher in his two reports, and as the hard drives in the server at the time of the attack were removed and replaced by new hard drives, I do not see what useful purpose would be served by appointing Mr. Timmons or an independent IT expert to inspect and search the current server (or servers). Even if I am incorrect in my understanding and if the server was entirely replaced at some point after the ransomware attack, I would reach the same conclusion that no useful purpose would be served by making the order sought. That is particularly so in light of the express averments contained in para. 8 of Mr. Millett's first affidavit to which I have just referred. I am not satisfied that the plaintiffs have discharged the onus of demonstrating with reference to the server (or servers) that the order sought would be likely to yield relevant material falling under category 3 of the discovery ordered. I am not satisfied that the order sought with respect to the server (or servers) would be a *"meaningful order"* in the terms described by Murphy J. in the Supreme Court in *Phelan*. Nor am I satisfied on the evidence before the court that the order sought with respect to the server or servers would reveal documents or other relevant information or data which are or were in the possession of the Millett defendants which should have, but have not, been discovered in Mr. Millett's affidavit of discovery in light of the explanations contained in the affidavits sworn in response to the plaintiffs' application. Finally, I am not satisfied that, in light of that evidence, it is necessary,

appropriate or proportionate to make the order sought with respect to the server (or servers) in the circumstances.

(b) The Laptop

81. The position with regard to the laptop is somewhat similar. The evidence discloses that the Millett defendants have in their possession one laptop which was in existence at the time of the cyber attack in early November, 2016. This was disclosed at para. 9 of Mr. Millett's first affidavit where he stated:-

> *"There is one laptop still in the possession of the eighth named defendant, this machine was completely sanitised in light of the expert advice received and averred to above and averred to* [in] *the supplemental affidavit of Mr. Gallagher."*

82. Mr. Millett was referring to Mr. Gallagher's first affidavit and to his first report. In his first affidavit, Mr. Gallagher stated that *"…the client computers and laptops were formatted and rebuilt"* (para. 3 of his first affidavit). In his first report, Mr. Gallagher stated that *"all PCs, laptops and desktop PCs were formatted and rebuilt from scratch"*. Mr. Millett explained in his first affidavit that, with the exception of one of the laptops, the rest of the *"computer hardware"* in use at the time of the attack was replaced in February, 2017 and he exhibited an invoice for the replacement of that hardware. With regard to the one remaining laptop, Mr. Timmons made a number of observations which were in turn addressed by Mr. Gallagher in his second report.

83. At para. 2.6.4 of his report, Mr. Timmons stated:-

> *"The sanitation process of simply re-formatting the device hard drive does not permanently delete the data. It is possible to retrieve full or partially deleted files from a fully re-formatted hard disk. This is commonly achieved by taking a digital forensic image of the hard disk and using a product such as Encase Forensics to restore the deleted data. It may not be possible to restore some data as its location on*

the disk may have been overwritten by new data over a period of time when the disk was subsequently re-used."

84. In response, Mr. Gallagher stated (at para. 3 of his second report) that the recovery of files would be *"highly unlikely"* but that, even if files could be retrieved, *"the decryption of these files is simply not possible"*. He continued: *"without decryption keys there is no way to recover"*. He concluded that, in his opinion, *"this would be an expensive and entirely wasteful exercise"*. There was no response from Mr. Timmons to Mr. Gallagher's evidence that, even if files could be retrieved from the reformatted hard drive in the relevant device (in this case, the laptop), it would not be possible to *"decrypt"* (or render intelligible) those files.

85. In his response Mr. Timmons stated, with particular reference to the one remaining laptop, at para. 2.6.5:-

"The laptop remaining in the possession of John Millett may contain some relevant data or file remnants which might be retrieved during a digital forensic investigation. It may also yield file remnants which were encrypted during the ransomware attack and thereby support the fact that the event occurred, confirm that no ransom notes were evident and potentially assign a date and time to the event…"

86. I draw attention to the fairly speculative terminology used by Mr. Timmons in this paragraph: *"<u>may</u> contain some relevant data or file remnant…"*, *"which <u>might</u> be retrieved…"* and *"<u>may</u> also yield file remnants which were encrypted…"* (emphasis added). In his response, at p. 3 of his second report, Mr. Gallagher explained that the laptop had originally been encrypted (by its owner) using a particular software. In the course of the ransomware attack, the laptop was encrypted by the attack. It was then formatted, rebuilt and encrypted again by Mr. Gallagher's firm with a particular encryption software. Having already expressed the view (in response to the previous point made by Mr. Timmons) that it would be impossible to conduct a forensic recovery process, in circumstances where

decryption of the encrypted files was not possible without decryption keys, Mr. Gallagher went on to state that any recovery process would corroborate the fact that no ransom note had been left behind.

87. In light of this evidence, I am satisfied that it would not be appropriate to grant the inspection and search order sought by the plaintiffs in respect of this laptop. I do not believe that the plaintiffs have discharged the burden which rests on them to demonstrate that an inspection and search by an independent IT expert would be likely to yield material falling within category 3 of the order. The plaintiffs have not satisfied me that an order in the terms sought would be meaningful, as that term was used by Murphy J. in *Phelan*. Nor am I satisfied that the plaintiffs have discharged the burden of demonstrating that the order sought will yield relevant documents or materials which are or were in the possession of the Millett defendants which should have, but have not, been discovered by them. Mr. Timmons' evidence on this issue is extremely speculative and there does not appear to be any obvious answer to Mr. Gallagher's evidence to the effect that even if any of the deleted files could be retrieved, they could not be decrypted without decryption keys and it is not suggested that such keys are available.

88. In those circumstances, I do not believe that the plaintiffs have discharged the burden of establishing an entitlement to an order for inspection and search of the laptop by an independent IT expert. Nor would such an order, in the light of that evidence, be necessary, appropriate or proportionate.

89. I note, however, that Mr. Millett has not expressly averred in any of his affidavits that the laptop was actually checked for any responsive documents or material for the purposes of Mr. Millett's affidavit of discovery. The affidavits sworn by Mr. Millett do not contain an equivalent averment with respect to the laptop as was made in relation to the server (or servers). In those circumstances, for completeness, I believe that Mr. Millett should confirm

on affidavit whether or not the laptop was searched for the purpose of the discovery exercise. If it was, and assuming that it is the case, he should confirm that no documents coming within any of the categories of discovery ordered, including, but not limited to, category 3, were found. If it was not, he should explain why it was not. I will discuss with counsel on a date following the delivery of this judgment the time period within which that affidavit should be sworn. It should be noted, however, that I am refusing the inspection and search order sought by the plaintiffs in respect of the laptop.

(c) Mr. Millett's iPad

90. I have touched on the evidence relevant to Mr. Millett's iPad earlier. The plaintiffs first saw reference to an iPad in a couple of emails from Mr. Millett to Mr. Gallagher following the discovery of the ransomware attack in early November, 2016, which were attached to Mr Gallagher's second report which was provided to the plaintiffs in early October, 2020. Following receipt of those emails, Mr. McEvoy swore his third affidavit shortly prior to the hearing. At para. 4 of that affidavit, Mr. McEvoy referred to the emails and to the iPad from which they were sent and stated, *"this is another example of Mr. Millett failing to account for all devices on which discoverable data was stored"*.

91. Following my ruling that the plaintiffs were entitled to rely on Mr. McEvoy's affidavit, a further unsworn affidavit was provided by Mr. Millett with an undertaking that the affidavit would be sworn as soon as practicable. In that affidavit, Mr. Millett stated (at para. 5):-

> *"…I have a personal iPad which has been used occasionally out of work for work related activities in the absence of other devices. It was never connected to the company's servers, the application system used for documents was not supported on iPads until 2015 so no files could have been either linked to or would have been*

retained on the device during this period. The exhibited emails from the iPad are an exchange between myself and Mr. Gallagher during the ransomware attack, when the company's computer systems were down. The iPad was checked to ensure that no relevant information relating to the plaintiff's discovery was contained on it. The email account is exactly the same email account loaded onto the phone and laptop and contains only that information. There was no other email addresses on the iPad and never have been. I purchased the iPad in question for home use on 17 December 2013, this was traded in with Apple for a new iPad on 1 July 2019."

92. In light of Mr. Millett's averment that the iPad was no longer in his possession, having been traded in in July, 2019, the plaintiffs accepted that it was no longer possible for them to obtain an order providing for the inspection and search of that iPad by an independent IT expert. However, the plaintiffs sought an order directing Mr. Millett, on behalf of the Millett defendants, to swear a further affidavit in relation to the iPad, which it was submitted by the plaintiffs' counsel was a *"information-bearing item of great and considerable importance between 2016 and 2019"*, to include details as to when the iPad was checked for the purpose of discovery, who it was checked by, what the fruits of that check were and why it was not referred to in Mr. Millett's affidavit of discovery. It was contended on behalf of the plaintiffs that an affidavit in those terms should be provided on behalf of the Millett defendants on the basis that it was *"connected intimately to email addresses which are connected to machines which are no more"*.

93. The Millett defendants opposed the making of any order with respect to the iPad. They relied on what was stated by Mr. Millett at para. 5 of his last affidavit. In particular, they relied on Mr. Millett's averment that the iPad was never connected to the server or servers and that no files were linked to or retained on the iPad during the relevant period. They also relied on the averment that the iPad was checked as part of the discovery process

and that no information required to be discovered was found on it. In addition, they relied on the averment that the email account on the iPad was the same account which was loaded on the laptop and Mr. Millett's phone and contained the same information as were contained on those devices. The Millett defendants argued that in those circumstances, there was no requirement specifically to refer to the iPad in the affidavit of discovery.

94. Clearly, in light of the fact that the iPad has been disposed of, the plaintiffs cannot obtain an order for inspection and search of that device by an independent IT expert. The plaintiffs accepted this. Instead, they now seek further affidavit from Mr. Millett. I do not believe that they have made out any entitlement to an order directing that a further affidavit be provided by Mr. Millett to deal with the iPad. It seems to me that Mr. Millett has adequately explained the situation in relation to the iPad at para. 5 of his most recent affidavit. He has explained the absence of any connection between the iPad and the server or servers and the absence of any files being retained in the device during the relevant period. He has also explained the fact that the device was checked during the discovery process. I do not believe that Mr. Millett should be required to set out in greater detail or to identify specifically the person or persons who checked the iPad and the particular circumstances in which that check took place. Mr. Millett has sworn that it was checked and that no responsive documents were found. The plaintiffs may not go behind that averment at this stage. They have not sought to cross-examine Mr. Millett on his averment. While the affidavit was produced during the course of the hearing, it was not suggested that the hearing should be adjourned to enable Mr. Millett to be cross-examined. I do not in any way criticise the plaintiffs for adopting that approach which seems to me to have been perfectly reasonable and appropriate. However, not having sought to cross-examine Mr. Millett, it was not open to the plaintiffs to seek to further interrogate Mr. Millett or to require him to swear yet a further affidavit in relation to the iPad. If a further affidavit were directed, it is likely that it would

say little more than was stated in his last affidavit and an order directing a further affidavit would, therefore, not be *"meaningful"* in the sense used by Murphy J. in *Phelan*. I do not agree that Mr. Millett was required expressly to refer to the iPad in his affidavit of discovery in circumstances where he said that it was checked and that no responsive documents were found. While the plaintiffs criticised Mr. Millett for replacing his iPad in July, 2019, I do not accept that such criticism was merited in circumstances where Mr. Millett has sworn that the iPad was checked at the time of discovery and no responsive documents were found. By July, 2019, the iPad was more than six years old and, in the particular circumstances, I do not accept that Mr. Millett ought to have held onto the device or informed the plaintiffs that he was intending to replace it. For all these reasons, I do not believe that it is appropriate to direct the Millett defendants to swear a further affidavit dealing with the iPad.

Summary of Conclusions

95. In summary, I have decided that in light of the evidence before the court, the plaintiffs have failed to discharge the burden upon them of demonstrating that an order providing for the inspection and search by an independent IT expert of the Millett defendants' current server or servers or the one laptop which remains in their possession from the time of the ransomware attack in November, 2016 would be likely to reveal documents which are, or were, in the possession, power or procurement of the Millett defendants falling within category 3 of the order for discovery made in February, 2019. For the various reasons outlined, I do not believe that the plaintiffs have established their entitlement to an inspection and search order in respect of the server or servers or the laptop. Nor do I believe that such an order is necessary, appropriate or proportionate in all the circumstances. I have carefully considered all of the evidence in reaching that conclusion. I have found that the affidavit of discovery sworn by Mr. Millett was seriously deficient and that the plaintiffs were well

within their rights to issue their motion at the end of May, 2020. However, I am also satisfied that the Millett defendants have addressed those deficiencies in a reasonable and responsible manner in the various affidavits sworn by Mr. Millett and by Mr. Gallagher, the IT expert retained by the Millett defendants. I have in one respect concluded that a further affidavit should be sworn by the Millett defendants addressing the searches, if any, conducted of the laptop at the time discovery was made by Mr. Millett's affidavit of discovery. I will discuss with counsel the time period within which that affidavit should be provided.

96. As regards the plaintiffs' application that a further affidavit should be sworn on behalf of the Millett defendants with regard to Mr. Millett's iPad, I have concluded that the plaintiffs have not established an entitlement to an order directing such a further affidavit. I am satisfied that the final affidavit produced by Mr. Millett during the course of the hearing (in response to the third affidavit of Mr. McEvoy furnished shortly prior to the hearing) adequately deals with the position in relation to the iPad. I do not believe that any further order or direction is required with regard to that device.

97. In those circumstances and for the reasons set out in this judgment, I refuse the plaintiffs' application for an order providing for the inspection and search by an independent IT expert of the Millett defendants' current server or servers and of the one remaining laptop from the time of the ransomware attack. I also refuse the plaintiffs' application for an order directing the Millett defendants to provide a further affidavit in respect of Mr. Millett's iPad. However, I will direct that the Millett defendants provide an affidavit confirming the steps, if any, which were taken to check the laptop for responsive documents at the time Mr. Millett swore the affidavit of discovery in late May, 2019.

98. I will list the case for mention at 10.45 on 3rd December, 2020 to consider any further orders or directions which may be required.