



Neutral Citation Number: [2022] EWHC 2773 (Ch)

Claim No: IL-2018-000182

**IN THE HIGH COURT OF JUSTICE**  
**BUSINESS AND PROPERTY COURTS OF ENGLAND AND WALES**  
**INTELLECTUAL PROPERTY LIST (ChD)**

Rolls Building  
Fetter Lane  
London, EC4A 1NL

8 November 2022

**Before :**

**MRS JUSTICE BACON**

-----  
**Between :**

(1) WEISS TECHNIK UK LIMITED  
(2) WEISS TECHNIK GMBH  
(3) WEISS TECHNIK FRANCE S.A.S.

**Claimants**

- and -

(1) MR CHRISTOPHER DAVIES  
(2) SJJ SYSTEM SERVICES LIMITED  
(3) MR STEPHEN JONES  
(4) MRS CATHERYN WHITFIELD  
(5) MR BEN ORAM

**Defendants**

-----  
**Robert Howe KC and Sam Carter** (instructed by **Mishcon de Reya LLP**) for the **Claimants**  
The **Defendants** appeared in person

Hearing dates: 7–8, 11–13, 19–20 July 2022  
-----

**Approved Judgment**

This judgment was handed down remotely at 2pm on 8 November 2022 by circulation to the parties or their representatives by email and by release to the National Archives.

<b>Introduction.....</b>	<b>3</b>
<b>The parties .....</b>	<b>4</b>
<b>Witnesses.....</b>	<b>5</b>
Claimants' evidence .....	5
Defendants' evidence .....	6
<b>The Weiss confidential and copyright materials.....</b>	<b>7</b>
<b>Procedural history .....</b>	<b>8</b>
<b>Issues for the trial.....</b>	<b>10</b>
<b>Background factual matters.....</b>	<b>11</b>
Defendants' employment contracts with DEL/Weiss .....	11
General comments as to the way in which SJJ obtained Weiss material .....	18
<b>Breach of confidence.....</b>	<b>23</b>
Legal principles .....	23
Breach of contractual/equitable obligations .....	27
Procuring or inducing breaches of contract.....	39
<b>Copyright claims .....</b>	<b>41</b>
Legal principles .....	41
Breaches of copyright.....	42
<b>Database rights.....</b>	<b>45</b>
Legal principles .....	45
Breaches of database rights .....	46
<b>Other issues.....</b>	<b>48</b>
Unlawful means conspiracy .....	49
Loss and damage .....	49
Competition law .....	50
<b>Conclusions.....</b>	<b>50</b>

**MRS JUSTICE BACON:**

**INTRODUCTION**

1. This is a claim for breach of confidence, copyright infringement, database right infringement, breach of contract, inducing/procuring breaches of contract, and conspiracy to cause loss by unlawful means. It is brought by three companies within the Weiss Technik group (which I will refer to individually as **Weiss UK**, **Weiss Germany** and **Weiss France**, and collectively as **Weiss**) against four former employees (**the individual defendants**) and the company SJJ System Services Limited (**SJJ**), which was set up by one of those employees, Mr Jones, when he left Weiss.
2. The claim is, essentially, that Mr Jones established SJJ by taking large swathes of confidential Weiss information and software, which he used to compete with Weiss. The claimants say that the other defendants, i.e. Mr Davies, Mrs Whitfield and Mr Oram, then continued to provide Mr Jones and SJJ with confidential information from Weiss either at Mr Jones' request or voluntarily, before they left Weiss at various different times to work for SJJ. They then (the claimants say) continued to use Weiss's confidential information after they had joined SJJ.
3. By the time of the trial, the thrust of the defendants' defences was that the relevant materials obtained from Weiss were not understood by the defendants to be confidential, and that any use of Weiss materials by the defendants after leaving the employment of Weiss was legitimate. While the defendants all admitted providing SJJ with some of the Weiss materials found on SJJ's system, Ms Whitfield, Mr Davies and Mr Oram all maintained denials in respect of other materials alleged to have been provided by them. All of the defendants denied any conspiracy to cause loss by unlawful means.
4. Following orders made in May and October 2021, the present trial is a trial of liability only, with liability in respect of (some of) the claims for breach of confidence and copyright infringement to be determined on the basis of samples of documents found on SJJ's systems. As described further below, determination of the claims based on the sample framework originally ordered would have been wholly unfeasible in the trial window. The claimants have therefore, for the purposes of this trial, pursued only a very small subset of the sample claims, limited to documents said to have been obtained or used in breach of confidence.
5. Weiss was represented at the hearing by Mr Howe KC and Mr Carter. Mr Oram has acted as a litigant in person throughout the proceedings. Mr Davies and Mrs Whitfield had legal representation until 4 February 2021 and 7 June 2021 respectively, and Mr Jones and SJJ were represented by solicitors and both leading and junior counsel until 31 March 2022. Since those dates, however, the defendants have been litigants in person. All of the defendants appeared in person at the hearing (with Mr Jones representing both himself and his company SJJ), and made written and oral submissions as well as cross-examining the claimants' witnesses.
6. The first two days of the hearing were conducted remotely, as I had contracted Covid. This included the cross-examination of Mr Walther, Mr Ruppert, Mr Lefort and the start of the cross-examination of Mr Youll. The hearing resumed in person on Day 3 and continued in person to the end of the trial, save that Mr Goebel was cross-examined

remotely from the US on the afternoon of Day 3 (interposed during the cross-examination of Mr Youll, given the time difference). All of the defendants were cross-examined in person over the course of Days 4–5 of the trial.

## THE PARTIES

7. The Weiss Technik group is a division of the Schunk group of companies, which is a multinational technology and engineering group with its headquarters in Germany. Weiss Technik has particular expertise in, among others, environmental simulation technology. This includes the manufacture, sale and maintenance of environmental test chambers (ETCs), which is the focus of the business of the claimant companies. There are around 5,500 ETCs in the UK, which are used by the life sciences sector and industrial clients to maintain and monitor specific environments. The temperature, humidity, and lighting within the chamber can be closely monitored and altered by the user. The Weiss ETCs are operated using proprietary (and password-restricted) control software, although some aspects of the maintenance of the ETCs can be carried out without using that software or needing the passwords.
8. All three claimant companies are the successors to companies that operated under various different names. For the purposes of this trial, the main relevant point to note is that Weiss UK is the successor to two companies: a UK subsidiary of the Schunk group (known first as Schunk Environmental Holdings, and later as Weiss Gallenkamp) which had premises in Loughborough, and Design Environmental Limited (**DEL**) which operated out of premises in Ebbw Vale. Schunk bought DEL in 1998, but DEL continued to operate as a distinct entity from its premises in Ebbw Vale until the business was merged into the Weiss Gallenkamp business to form Weiss UK in 2013. Following the merger, the Weiss UK business continued to operate from both the Loughborough and Ebbw Vale sites until the closure of the Ebbw Vale site in 2018.
9. Weiss Germany is the immediate parent company of Weiss UK, and is the successor company to Vötsch Industrietechnik GmbH. Weiss France is another company in the Weiss Technik group. Weiss Germany and Weiss France are included in the claim because of their ownership of rights in some of the materials the subject of this claim, including some of the software packages.
10. All four of the individual defendants worked at the Ebbw Vale site of DEL, and became employees of Weiss UK in 2013 with the consolidation of the businesses, before leaving to found (in Mr Jones' case) or join (in the case of the other defendants) SJJ.
11. Starting with SJJ itself, the company was incorporated by Mr Jones on 1 September 2015, shortly before Mr Jones gave notice of his resignation from Weiss. SJJ does not manufacture its own ETCs, but maintains and repairs ETCs throughout the UK, in direct competition with the service division of Weiss UK.
12. Mr Davies worked at DEL and then Weiss UK from February 2008 until 25 July 2018, starting as a trainee electrical design engineer and ending up as a senior technical support engineer. He has effectively continued in that role at SJJ, which he joined in September 2018.

13. Mr Jones worked at DEL and then Weiss UK from January 1990 until 11 December 2015 (with the last month of that on medical leave following an operation), having given notice of his resignation on 21 September 2015. From 2011–2015 he held the position of service manager, initially for DEL and then (following the merger) for the whole of the Weiss UK business. On his departure from Weiss UK he set up and became the managing director of SJJ.
14. Mrs Whitfield worked at DEL and then Weiss UK from September 1989 until 19 August 2016, having given notice of her resignation on 28 July 2016. She initially started at the company as an office junior, progressing to the role of service administrator which she held from 1998 onwards. She joined SJJ in September 2016 and continued in effectively the same role there.
15. Mr Oram worked at DEL and then Weiss UK from June 2009 until 7 November 2016, starting as a trainee electrical design engineer and ending up as a technical service support engineer. He then spent a short time working for another company before returning to Weiss UK in March 2017 as a systems and refrigeration design engineer. In December 2017 he left Weiss, and joined SJJ in January 2018 as a control system engineer.

## WITNESSES

### Claimants' evidence

16. The claimants relied on the evidence of four witnesses of fact: Malcolm Youll, Michael Walther, Wolfgang Ruppert and Sebastian Goebel. They also relied on an expert report from Pascal Lefort on issues of French law.
17. The sole purpose of the evidence of Mr Goebel and Mr Lefort was to address the ownership of one of the Weiss software packages in issue in these proceedings, in circumstances where the defendants in their pleaded case had put the claimants to proof on this issue. The defendants asked to cross-examine both Mr Goebel and Mr Lefort, but in the event did not challenge the content of their evidence, and in their closing submissions all of the defendants confirmed that they no longer disputed the claimants' ownership of or the subsistence of copyright in any of the Weiss software relevant to these proceedings. The sole questions put to Mr Goebel were on matters unrelated to his evidence which were in any event of no material significance. I therefore say no more about these two witnesses.
18. As for the other witnesses, Mr Youll was the claimants' principal witness. He was appointed as the interim managing director of Weiss UK in January 2018, and has remained in that role since then. He gave detailed evidence as to the defendants' employment with Weiss (including the terms of their employment contracts), the events leading up to the claim, Weiss's claims to confidentiality and copyright in its software and its "ServiceLife" customer database, and the key evidence of infringement relied upon by the claimants. Mr Youll's cross-examination by the defendants started on Day 2 of the trial, and continued until Day 4. He was a straightforward and patently honest witness, and I considered his evidence to be entirely reliable.
19. I should, however, note that on the morning of Day 4 it emerged that Mr Youll had earlier that morning made an enquiry with colleagues at Weiss about one of the matters raised

in the evidence. This was discovered by the claimants' solicitors very shortly before the start of court on that day, and Mr Howe immediately drew it to my attention at the start of the hearing. He explained that Mr Youll had forgotten that he remained in purdah while his cross-examination continued. Later that day, after his cross-examination had concluded, Mr Youll provided a witness statement with a frank explanation of what he had done, offering a sincere apology to the court and the defendants for his breach of the purdah rules. Mr Howe reiterated that apology at the start of the hearing on Day 5. The defendants did not seek to recall Mr Youll for further cross-examination, nor did they ask me to make any further order in that regard. I am satisfied that Mr Youll's breach of the purdah rules was a genuine mistake and I do not consider that it undermines the remainder of his evidence.

20. Mr Walther is the head of the software consulting team at Weiss Germany. He gave evidence as to the development and ownership of the claimants' proprietary software, some of which he had personally helped to build. He was cross-examined to a very limited extent by Mr Jones and Mr Oram. I considered him to be a straightforward and reliable witness.
21. Mr Ruppert is the global director of services at Weiss Germany. His evidence described the functionality of the claimants' proprietary software at issue in these proceedings. He was cross-examined by all of the defendants, but again only to a limited extent. I considered him to be a straightforward and reliable witness.

### **Defendants' evidence**

22. The defendants all provided witness statements and were cross-examined at the trial. They did not rely on evidence from any other witnesses of fact or experts.
23. Mr Davies admitted supplying Mr Jones/SJJ with passwords for the Contour software and Simpac controller while he was still employed by Weiss. However, on the important issue of how a large number of Weiss documents had come to be uploaded to SJJ's systems shortly after his departure in 2018, he denied any responsibility. As set out below, I consider that his evidence on that point was inconsistent and incomplete, and I am not persuaded by his account.
24. Mr Jones gave evidence on his own behalf and on behalf of SJJ. Much of his written evidence was very defensive, and his cross-examination started in similar vein. As his cross-examination progressed, however, he made significant concessions, admitting that he had taken and misused internal information from Weiss in order to take business from Weiss. He nevertheless continued to deny knowledge of how key materials had come to be saved onto SJJ's systems, and denied asking the other defendants to bring Weiss materials with them when they left Weiss to join SJJ. I do not consider his evidence in this regard to be plausible; rather, I consider that Mr Jones was being deliberately evasive in an attempt to protect the other defendants.
25. Mrs Whitfield was very defensive in her written evidence. Her oral evidence unfortunately did not improve matters: her answers to questions ranged from evasive to utterly implausible. I regretfully consider that she was an entirely unreliable witness and have not placed any weight on her evidence on disputed points of fact, save where corroborated by other more reliable evidence in the case, including contemporaneous documentation.

26. Mr Oram provided two witness statements, which were largely straightforward, as was some of his oral evidence. His credibility was tainted, however, by defensive and implausible answers to a number of questions concerning (in particular) assistance provided by him to Mr Jones/SJJ while he was still employed by Weiss. As a result I have treated his evidence with some caution.

## **THE WEISS CONFIDENTIAL AND COPYRIGHT MATERIALS**

27. Weiss ETCs are operated and maintained using various items of password-restricted software. Five software packages are relevant to these proceedings, as follows:
- i) Simpac (asserted as both copyright and confidential). This is the core software used to control Weiss ETCs. It is installed on a physical Simpac controller which is incorporated into the ETC sold to customers. Some level of control of Simpac is possible through the touch panel on the front of the ETC or through web access, but more sophisticated control and operation requires the use of other Weiss software such as Contour or Simpati, run on a separate computer.
  - ii) UpToDate3 (asserted as both copyright and confidential). This is one of the most important Weiss service tools. It is run by Weiss engineers on a computer separate to the ETC, and is used to install and update Simpac software on Simpac controllers as well as to modify more complex settings.
  - iii) Contour (asserted as both copyright and confidential). Again, this runs on a separate computer which integrates with the Simpac software. It enables Weiss engineers to conduct more sophisticated data gathering and analysis than could otherwise be achieved with Simpac alone.
  - iv) Simpati (asserted as confidential only). Again, this runs on a separate computer which integrates with the Simpac software. It is typically used to control multiple ETCs at once, and like Contour enables more sophisticated data gathering and analysis than could be achieved with Simpac alone.
  - v) Magic Simpac (asserted as confidential only). Again, this runs on a separate computer, and is used to locate and diagnose hardware or software faults on Weiss ETCs and/or Simpac controllers.
28. As noted above, the claimants' ownership of these software packages, and the subsistence of copyright in the Simpac, UpToDate3 and Contour packages, are no longer disputed by the defendants.
29. The claimants also assert breach of confidence and *sui generis* database rights in relation to extracts from Weiss's ServiceLife customer and supplier databases found in the possession of SJJ. ServiceLife is a piece of third-party software that provides small to medium-sized companies with a database for their customer and supplier details. It keeps track of (among other things) site equipment, maintenance history and service contracts. Weiss used this platform from around 2003 to 2019 for all its customer service contracts, using it to record each customer's service history, contract prices and renewal dates.

30. In addition to the software and database described above, the claimants rely on numerous miscellaneous documents found on SJJ's electronic file storage systems, in particular the SJJ Dropbox account, which the claimants say should not have been provided to SJJ, or retained by SJJ thereafter.

## **PROCEDURAL HISTORY**

31. Following the departure of Mr Jones from Weiss, Weiss became aware that he had set up SJJ as a direct competitor to Weiss and was starting to take a significant number of Weiss's service customers. Mr Youll was also informed by another employee that Mr Jones had taken a copy of the Weiss ServiceLife database with him, and was shown quotes from SJJ to a customer which reproduced the same spelling mistakes as those contained on Weiss's ServiceLife database. Mr Youll also discovered that various Weiss customers whose service contracts were about to expire had been visited by Mr Jones, seeking to persuade them to transfer their contracts to SJJ. In addition Mr Youll noted what he considered to be odd behaviour by Mr Davies shortly before he left Weiss in July 2018.
32. Mr Youll therefore started to become concerned that SJJ was using confidential Weiss information to compete with Weiss, and that SJJ had been assisted in this by Weiss employees.
33. That led Mr Youll to instruct a forensic IT consultant to image the laptops and other electronic devices which had been used by Mr Davies prior to his departure. That revealed that Mr Davies had, in the months before he left Weiss, downloaded Weiss proprietary software onto a USB using his laptop, accessed Dropbox via his laptop, and sent documents related to Weiss software to his personal email address.
34. In light of this evidence and Mr Youll's concerns described above, Weiss's solicitors initiated these proceedings with an urgent without notice application for a search, computer imaging and evidence preservation order against Mr Davies and SJJ.
35. The search and imaging order sought by the claimants was obtained and served on Mr Davies and SJJ on 1 October 2018. Following the imaging of Mr Davies' and SJJ's devices, many thousands of documents were found in SJJ's possession which were responsive to initial searches under the agreed search protocol. Those included copies of the claimants' core proprietary software packages, extracts from the Weiss ServiceLife database, and around 40,000 miscellaneous documents said to be Weiss confidential and/or copyright documents.
36. The claim form was issued in October 2018, initially against only Mr Davies and SJJ. Mr Jones was joined in the amended particulars of claim in December 2018. Mrs Whitfield and Mr Oram were then added in the re-amended particulars of claim in July 2020. The particulars of claim were further amended in 2022; references in this judgment to the particulars of claim are therefore to the re-re-re-amended particulars dated 15 June 2022.
37. As already noted, case management orders during 2021 directed a split trial as between liability and quantum. In addition, it was necessary to reduce the claims in relation to the 40,000 miscellaneous Weiss documents to a manageable scope.



38. To that end, the order of Deputy Master Rhys dated 15 September 2021 set out a detailed framework for the selection of the samples. In particular, the order provided for the parties to agree categories of alleged copyright documents and documents containing alleged confidential information, with one sample document for each category to be selected by each of the claimants and any defendant alleged to have infringed the claimants' rights in respect of that category of documents.
39. The order specified that if any document within a sample category was determined to fail on liability, that entire category of documents would fail on liability. If, however, each of the documents within a sample was determined to succeed on liability, the result would be that the entire category of documents was deemed to succeed on liability.
40. In accordance with that order, the parties initially agreed 44 categories of sample documents to be determined, giving a pool of around 3,500 documents, from which the parties selected individual sample documents for each category. The claimants' case on the samples was set out in five Schedules to the particulars of claim, grouping the samples into (i) confidential only categories as against Mr Jones and SJJ; (ii) copyright only categories as against Mr Jones and SJJ; (iii) copyright and/or confidential categories as against Mr Jones and SJJ; (iv) categories asserted against Mrs Whitfield; and (v) categories asserted against Mr Oram. The defendants' responses to those were set out in Schedules to their respective defences. The pleaded positions were then consolidated into a 69-page schedule that resembled a Scott Schedule.
41. By the start of the trial, however, it remained unclear how the parties' submissions on all of those categories of documents were to be accommodated within the two-week trial timetable. Following discussions with Mr Howe, the claimants agreed to reconsider the question of how to address the samples.
42. On the afternoon of Day 5 of the trial, after the evidence on both sides had concluded, Mr Howe proposed that the majority of the sample categories should be stood over (including all of the categories related to alleged breaches of copyright), with liberty to apply, and suggested that the claims arising from the samples should be confined at this stage to five categories of documents going to alleged breaches of confidence only, as follows:
  - i) Category 3 (asserted in relation to Mr Jones and SJJ): documents containing Weiss passwords;
  - ii) Category 21 (asserted in relation to Mr Jones and SJJ): documents containing Weiss ETC cooling load calculations;
  - iii) Category 35 (asserted in relation to Mr Jones and SJJ): Weiss order consolidation forms;
  - iv) Category 36 (asserted against Mrs Whitfield): email exchanges between Weiss and its customers;
  - v) Category 44 (asserted against Mr Oram): Weiss internal technical materials.
43. The defendants were content with these proposals and the trial therefore proceeded on that basis.

44. At the same time as proposing the reduction of the sample categories for the purposes of this trial, Mr Howe agreed that the multiple causes of action pleaded by the claimants could also be narrowed, leaving the issues set out below.

## **ISSUES FOR THE TRIAL**

45. The claimants' case is that Weiss's software and confidential information was taken by the individual defendants either during the course of their employment at Weiss, or when they left Weiss to join SJJ, and was subsequently uploaded by those defendants to the SJJ systems and used by SJJ and the other defendants to divert customers from Weiss to SJJ.
46. The claimants' pleaded case in that regard involves a large number of alleged infringing acts. As a result, however, of the narrowing of both the causes of action and the sample categories relied on by the claimants, the following issues now fall to be decided:
- i) Whether the defendants breached express/implied contractual duties of confidence (individual defendants) and/or equitable obligations of confidence (all defendants) by providing to Mr Jones/SJJ and/or using for the purposes of SJJ's business software and passwords for that software, the ServiceLife database, and the materials in sample categories 3, 21, 35, 36 and 44.
  - ii) Insofar as Mr Davies, Mrs Whitfield and Mr Oram did breach their contractual duties of confidence, whether those breaches were induced or procured by Mr Jones/SJJ.
  - iii) Whether the defendants infringed copyright in the Simpac, UpToDate3 and Contour software packages by (variously) copying them and providing them to Mr Jones/SJJ, storing them on the SJJ Dropbox, copying or downloading them from the SJJ Dropbox, and providing copies or making them available to other defendants and third parties.
  - iv) Whether Mr Jones/SJJ and Mrs Whitfield infringed Weiss's rights in the ServiceLife database by extracting (at least) a substantial part of its contents, storing those extracts on SJJ's systems, and sending marketing emails to email addresses extracts from the database.
  - v) Whether the defendants' conduct amounted to a conspiracy to cause loss by unlawful means.
  - vi) Whether Weiss has suffered more than merely nominal loss and damage.
47. The above set of issues nevertheless belies the complex nature of the claim, involving multiple defendants said to have carried out different (but overlapping) specific infringing acts, causes of action which overlap as to the acts of wrongdoing relied upon, and a miscellany of allegations which are not pleaded as allegations of wrongdoing but which are said to support the pleaded allegations. The claims have been set out in (variously) the particulars of claim and replies to the defences of each of the defendants, the consolidated Schedules for the sample categories, a lengthy opening skeleton argument from the claimants which was updated to include their closing submissions, a

29-page A3 table with a chronology of the alleged wrongdoing, and a note produced by Mr Howe and Mr Carter during the trial outlining the claimants' position on the reduced sample categories and the narrowed causes of action now relied upon.

48. Doing the best I can with the voluminous material before me, I have not attempted to set out a comprehensive assessment of each and every act of alleged wrongdoing, but have focused on the main evidence and arguments relating to issues (i) to (iv) above. For the reasons which I set out further below I do not consider it possible to determine issue (v) (unlawful means conspiracy) on the submissions currently before me; and for that and other reasons issue (vi) (loss and damage) also does not arise for determination, although I will make some brief comments on that for completeness.
49. Before addressing the issues above, I will address two background factual issues. The first is the terms of the individual defendants' employment contracts at Weiss. Secondly, I will make some general comments on (and where disputed make factual findings concerning) the way in which SJJ obtained information and documents from Weiss. These background issues will set the scene for the specific allegations of wrongdoing raised by the issues above.

## **BACKGROUND FACTUAL MATTERS**

### **Defendants' employment contracts with DEL/Weiss**

50. Each of the individual defendants disputed the extent to which obligations of confidentiality arose under their employment contracts at DEL and then (following the merger) Weiss UK, and the extent to which they understood their obligations under those contracts. It is therefore necessary to set out the employment terms for each of the defendants in some detail.

#### *Mr Davies*

51. Upon joining DEL Mr Davies signed a statement of terms and conditions of service. That was updated with a new set of terms and conditions and a revised Employee Handbook sent on 17 January 2012. The updated terms provided in clause 15:

**“Confidentiality** In the normal course of your employment with the Employer you may have access to and be entrusted with confidential information which is of substantial commercial value to the Employer and potentially to any other business operating in the same field. To protect the confidentiality of this information and the legitimate business interests of the Employer you agree not at any time, whether during or following your employment (unless expressly so authorised by the Employer in writing or as a necessary part of the performance of your duties, or as required by law), to disclose to any person or knowingly permit or enable any person to acquire or to make use of any such confidential information for any purpose in a manner which may cause loss or damage to the Employer.”

52. The end of the document also contained a confirmation that the company Employee Handbook had been received:

“I acknowledge receipt of my Statement of Terms and Conditions of Employment and a copy of the Employee Handbook. I confirm that I have read and understand the contents of both of these documents and accept that together they form my contract of employment.”

53. On 10 February 2012 a letter was sent to Mr Davies by the then HR manager noting that he had not signed the new terms and conditions, but had been working under those terms without complaint, and saying that in those circumstances the company assumed that he had accepted the new terms and conditions. He was asked to sign the letter to acknowledge receipt, which he did on the same day.
54. Following the merger of DEL and Weiss Gallenkamp in 2013, to form Weiss UK, Mr Davies was issued with a further update to his employment terms and conditions on 8 July 2013 (which did not change the substance of the provisions set out above). The updated terms also enclosed a copy of the latest Employee Handbook. The updated terms were again not acknowledged by Mr Davies, and a further letter was sent to him on 1 August 2013 stating (as with the 10 February 2012 letter) that due to his continued employment at the company it was assumed that he had accepted the new terms and conditions.
55. The version of the Employee Handbook at that time was the May 2013 version, which included the following terms:

#### **“COMPUTER POLICY**

**Software** ... Software issued by the Company for your use is licensed to the Company and is protected by copyright law. You must not make copies of, or distribute software that has been copied.

**Passwords** To access various software programs you may have been given a user name and password. These passwords are personal to you. Do not write them down where they may be seen by anyone else. ... You should not therefore allow anyone else to use your access rights and password.

**Email** ... Confidential information about or relating to the Company should not be transmitted via email unless done so in the course of business. ... You must not distribute sensitive commercial data concerning the Company to competitive sources. Doing so may result in disciplinary action leading to your dismissal without notice for gross misconduct.

**Inappropriate use** ... Examples of inappropriate use include, but are not limited to ... (e) Downloading or disseminating copyright materials. (f) Disclosing confidential information. ... (h) Copying or downloading software.

#### **PROPERTY AND EQUIPMENT**

**Return of Company property** Upon termination of your employment for whatever reason, you must return to your line manager all property belonging to the Company including but not limited to, Company vehicle, computer, equipment, tools, uniforms, keys, entry passes, records, documents, accounts,

letters, papers (including all copies, summaries and extracts) within your possession or control belonging to the affairs and business of the Company and its customer.”

56. On 1 September 2015 Mr Davies was issued with a new contract of employment, containing the following relevant provisions:

**“Confidentiality** During the course of your employment you will be party to information concerning the Company, its products and customers. Such information is to be regarded as strictly confidential. You may not disclose or discuss with any other person outside the Company information relating to its business including product information or matters relating to security. Any breach of this condition will render you liable to disciplinary action, which may result in dismissal.

... I have read, understood and am willing to abide by the terms and conditions laid down in the Employee Handbook and accept that they form an integral part of this Contract of Employment.”

57. The relevant Employee Handbook at this time was the May 2015 edition, which included the following terms:

**“Return of Company property** On the termination of your employment for whatever reason, you must return all Company property in your possession or for which you have responsibility. Failure to return all such items will result in the cost of the unreturned items being deducted from any monies outstanding to you. This is an express written term of your contract of employment.

**Conduct at work** The following list provides examples of the type of conduct that the Company would expect:

...

- To devote all your time and attention, whilst at work, to the Company and ensure that all its property including confidential information, records, equipment, information technology, etc, is kept safe and used correctly.

**Computer usage** Employees must keep their passwords confidential and must not disclose them to any other party. ... On the termination of employment ... employees must return all information that they have in a computer compatible format to a nominated member of staff. All information, programs and systems created by employees during the course of their employment with the Company will remain the property of the Company.

**Email** ... Employees must not use emails to distribute information that is confidential in nature, unless the permission of the customer and/or Management has been given in advance. Employees must not use emails to distribute anything that is copyright protected or to pursue or promote personal business interests.

**Employee Handbook receipt** This Handbook has been drawn up by the Company to provide you with information on employment policies and procedures. It is important for you to read the Handbook carefully as this, together with your Contract of Employment, sets out your main terms and conditions of employment.”

58. Following a query by Mr Davies, an amended contract of employment was sent to him for signing in January 2016. Mr Davies again did not sign the contract, leading to emails in similar terms to the letters of February 2012 and August 2013 recording that he had been working to the terms and conditions of the new contract of employment, which were therefore regarded as having been accepted.
59. On 14 June 2016 Mr Davies was sent a revised version of the Employee Handbook (with changes that did not affect the terms set out above). He signed to confirm receipt of this version of the Handbook.
60. It is well-established that a contract (including a contract of employment) can be accepted by conduct: see e.g. *Solelectron Scotland v Roper* [2004] IRLR 4, §30. During the course of his cross-examination Mr Davies conceded that he had accepted the 2015 contract by continuing to work at Weiss. I consider that the same applies to the previous versions of Mr Davies’ contract of employment. Accordingly, at all times material to these proceedings, Mr Davies was subject to a contract of employment. Those contracts incorporated the terms of the Employee Handbook. Both the contracts of employment and the various versions of the Employee Handbook contained terms relating to confidentiality. The Employee Handbook in force at the time when Mr Davies left the company also made clear that on termination of the employment he was required to return to Weiss all company property, including information in his possession in a computer compatible format.
61. I do not accept Mr Davies’ submission that his contractual terms did not identify the information classified as confidential. On the contrary, those terms contained express provisions referring to the confidentiality of (among other things) Weiss’s product and customer information, and passwords. The clear terms of the Employee Handbook also contradict Mr Davies’ submission that his contract contained no reference to the use of confidential information once he had left the employment of Weiss. Mr Davies either was, or should have been, well aware that he was not entitled to take Weiss company materials with him to SJJ, including not only hard copy materials but also material stored electronically.

*Mr Jones*

62. Mr Jones’ statement of employment particulars, signed by him on 28 November 2003, included the following clauses:

“Following the termination of your employment you shall not: ... 4. Use or disclose any confidential information relating to the business or financial affairs of the company to any individual, firm, company or other body so long as the information remains confidential.

...

Further terms and conditions relating to your employment can be found in the Employee Handbook. The content of the Employee Handbook is to be read in conjunction with this statement, which together form your contract of employment.”

63. Updated terms and conditions of employment and an updated version of the Employee Handbook were issued to Mr Jones in January 2012 (i.e. the same time that they were provided to Mr Davies). Mr Jones appears to have objected that the contract was not legally binding because the documentation (or some of it) related to Weiss Gallenkamp rather than his employer DEL.
64. Following the merger of DEL and Weiss Gallenkamp in 2013, to form Weiss UK, Mr Jones was issued with a further update to his employment terms and conditions on 8 July 2013. The updated terms also enclosed a copy of the latest Employee Handbook. The updated terms included the same provisions as set out at §§51–52 above; the relevant provisions of the then-current Employee Handbook are at §55 above.
65. Mr Jones signed and dated each page of the statement of terms and conditions, as well as the acknowledgement at the end. While he marked up a number of the clauses, for instance to correct the address of his place of employment, he accepted in cross-examination that he had not made any alterations to clause 15 or the employee acknowledgement.
66. A further contract of employment was provided to Mr Jones on 1 September 2015, with the terms (and, incorporated by reference, Employee Handbook terms) set out at §§56–57 above. That contract was not signed by Mr Jones. Instead, he handed in his letter of resignation on 21 September 2015. Weiss accepted that resignation by letter dated 8 October 2015, informing Mr Jones that his last day of work would be on 11 December 2015. That letter also drew Mr Jones’ attention to the Confidentiality clause in his last signed contract of employment (i.e. the version cited at §51 above) and the Return of Company Property clause in the May 2013 version of the Employee Handbook (cited at §55 above).
67. In these circumstances, notwithstanding Mr Jones’ protestations that his employment contract was “everything but a binding contract”, I find that Mr Jones was subject to a contract of employment at all material times. That included in particular the period between his resignation and his last day of work in 2015, when he was subject to the July 2013 contract and the terms of the Employee Handbook in the version at that time.
68. As Weiss’s letter dated 8 October 2015 made clear, the terms to which Mr Jones was subject included a confidentiality provision expressly applicable following termination of his employment, and a requirement to return all company property on his departure. Mr Jones accepted in cross-examination that he understood those provisions, and understood that he had to comply with them.
69. Mr Jones repeatedly questioned the confidentiality of materials he had received as part of his general training in his various roles at Weiss, including (for example) City & Guilds courses. These proceedings are not, however, concerned with the use of general training materials. They are concerned with the disclosure and use of Weiss-specific company materials, in particular (as regards Mr Jones) Weiss’s proprietary software (and materials related to the use of that, such as passwords), the ServiceLife database, and

other Weiss customer information. Mr Jones can have had no doubt that those materials were confidential both before and after he had left Weiss UK, under the terms of his contract and the relevant Employee Handbook.

*Mrs Whitfield*

70. As with Mr Davies and Mr Jones, Mrs Whitfield received new employment terms and conditions in January 2012. As with Mr Davies, a letter was sent to Mrs Whitfield by the company on 10 February 2012 noting that she had not signed the new terms and conditions, but had been working under those terms without complaint, such that the company assumed that she had accepted the new terms and conditions. That letter was signed by Mrs Whitfield on the same day, but with a markup indicating various “Issues to be discussed”. Those issues did not, however, relate to the confidentiality provision, or any of the terms of the Employee Handbook.
71. It appears that a further updated version of the contract was sent to Mrs Whitfield in 2013, which is presumed to have occurred in July 2013 at the same time that the new contract was sent to Mr Davies and Mr Jones. Mrs Whitfield then received a new contract of employment on 1 September 2015, with the provisions (and, incorporated by reference, the provisions of the Employee Handbook) set out at §§56–57 above. That contract was signed by Mrs Whitfield on 24 February 2016. The document marked up queries in relation the specified place of work and Mrs Whitfield’s job title. There is, however, no evidence either on the signed contract or otherwise indicating that Mrs Whitfield objected to any aspect of the confidentiality provisions, or anything in the Employee Handbook.
72. Mrs Whitfield claimed that she had signed the 2015 contract under duress and with issues left unresolved. There is, however, no evidence of duress beyond Mrs Whitfield’s bare assertion; and as noted above the version of that contract marked-up by Mrs Whitfield does not indicate any objection to the provisions relied upon by Weiss for the purposes of these proceedings. In any event, Mrs Whitfield accepted in cross-examination that the information that she had access to while working at Weiss was confidential, and that she had an obligation to keep it confidential.
73. Mrs Whitfield was therefore, in my judgment, bound by the relevant terms of the 2015 contract of employment and associated Employee Handbook, and before that the relevant terms of (at least) the 2012 version of the contract and Handbook.
74. Mrs Whitfield also claimed that she was unaware of any confidentiality obligations continuing beyond her employment. I have no hesitation in rejecting that contention. The relevant provisions were clearly stated in the contractual documents received by Mrs Whitfield. The 2012 terms and conditions (cited at §51 above) expressly referred to the employee’s confidentiality obligations subsisting beyond employment. While the 2015 contract did not do so in the same terms, the 2015 Employee Handbook specified explicitly that upon the termination of their employment employees were required to return to the company all information held by them in a computer compatible format.
75. Mrs Whitfield’s contractual confidentiality obligations were also emphasised in a letter sent to her by Weiss dated 5 September 2016, shortly after Mrs Whitfield had joined SJJ. The letter warned Mrs Whitfield about contacting Weiss customers using her new SJJ email address, highlighting the confidentiality clause of her 2015 contract. The letter continued:



“...any information regarding pricing structures and customers must be kept confidential and should not be disclosed to your new employer for your gain.

Secondly, the company considers its pricing structures to be a ‘trade secret’ and you are therefore subject to an implied duty not to misuse trade secrets post-employment. This means that you cannot reveal any information about our pricing structures to customers and/or your new employer. We consider revealing details about our pricing structure to be a misuse of information you gained whilst working for us.

Finally, may I also point out unlawfully obtaining or accessing personal data is a criminal offence under the Data Protection Act and this extends to taking client records that contain personal information to a new job without permission. This information belongs to Weiss Technik and absolutely must not be used by you in your new job. I therefore ask you to cease and desist contacting our company clients using information that you have gained by working for us.”

76. On 16 September 2016 Mr Jones sent a response to Weiss on behalf of Mrs Whitfield, assuring Weiss that Mrs Whitfield was “very much aware of her responsibilities regarding confidentiality and data protection, and the accusation that she may have breached this and committed a criminal offence is totally unfounded and unnecessary.” That indicates that Mrs Whitfield was not only aware of her continuing obligations but had discussed them with Mr Jones.

*Mr Oram*

77. As with the other individual defendants, Mr Oram received new employment terms and conditions in January 2012, and again in July 2013. In both cases, as in the case of Mr Davies, he did not sign the contracts, and therefore received letters recording that he had worked under the relevant terms without complaint, such that the company assumed that he had accepted the new terms and conditions.
78. Mr Oram was issued with a new employment contract on 1 September 2015, in identical terms to the contracts provided to the other individual defendants on that date. Emails sent in early 2016 record that an addendum to the contract was provided on 5 January 2016, and that although Mr Oram had not signed to confirm his acceptance he was taken to have accepted the terms and conditions by working under those terms since they were issued.
79. On Mr Oram’s resignation and then (after a short break) reemployment by Weiss in March 2017 in a different role, he signed a new employment contract containing the same relevant terms as in the 2015 contract (§56 above). The revisions to the Employee Handbook which had been made since 2015 did not change the provisions relevant to these proceedings, as cited at §57 above.
80. In those circumstances, I consider that Mr Oram was bound by the terms of the successive employment contracts received by him, whether by conduct or (in the case of his last contract) by his signing of the contract. The confidentiality terms in those contracts and the successive Employee Handbooks were, as I have already found, explicit. It was also clear from the 2015 version of the Employee Handbook that company information in any

computer compatible format had to be returned upon termination of the contract. Mr Oram either was, or should have been, well aware of his obligations in that regard.

### **General comments as to the way in which SJJ obtained Weiss material**

81. The evidence before me revealed a fairly clear picture as to how SJJ obtained large swathes of material from Weiss, from the time that SJJ was first incorporated in 2015 until proceedings were brought by Weiss in 2018.

#### *Initial establishment of SJJ*

82. Mr Jones said that SJJ started trading in January 2016. In fact the evidence shows that SJJ was issuing quotes and invoices as early as October 2015, while Mr Jones was still working his notice period at Weiss, and a marketing email sent on 15 August 2017 refers to “the successful launch of the company in September 2015”. During that early phase (for some of which Mr Jones was ostensibly on medical leave from Weiss) it is apparent that he was being actively assisted by Mrs Whitfield, who left Weiss less than a year later.
83. In a notable example of this, on 13 October 2015 Mrs Whitfield sent to her personal email account screenshots of pages on the ServiceLife database showing contact and other details of a customer of Weiss, CMCA. She then forwarded those screenshots from her personal account to Mr Jones’ SJJ email address. Mr Jones was by then in his notice period following his resignation from Weiss, and Mrs Whitfield said that she had provided the information at Mr Jones’ request.
84. When cross-examined, Mr Jones said that Mrs Whitfield could have done this for legitimate reasons in order to enable him to provide a quote to the customer from Weiss. That suggestion was patently untruthful. In the first place, if Mrs Whitfield was sending this to Mr Jones for the purposes of Weiss, she would have used his Weiss email address rather than his SJJ email address. Secondly, if that had been her purpose, there would have been no need for Mrs Whitfield to use her personal email account; she could and would simply have sent the relevant material from her own Weiss work email account. The fact that she used, instead, her personal email address strongly indicates that she was doing so in order to conceal the fact that she was sending confidential Weiss information to Mr Jones for the purposes of his competing business.
85. Thirdly, the evidence shows that Mr Jones used the information received to send the customer a competing quote from SJJ. That is apparent from an email sent from Mrs Whitfield to Mr Jones on 19 October 2015 (again from her personal address), saying that the same customer had then asked Weiss for a quote, “and he has also said received a competitive quote off you. Email only to me thou, what should I do?????”
86. It is, therefore, quite clear that Mrs Whitfield was sending Mr Jones confidential Weiss customer information in October 2015 for the specific purpose of helping Mr Jones to establish SJJ as a competing business.

#### *Subsequent materials obtained by Mr Jones/SJJ*

87. When Mr Jones eventually left Weiss in December 2015, he admitted that he took with him all of his “training materials” and large quantities of other materials on USB sticks,

including service manuals for the Weiss proprietary software packages. He also admitted that he took with him the Weiss ServiceLife database in printed format.

88. Thereafter, Mr Jones appears to have had two main ways of receiving Weiss information for use by SJJ.
89. First of all, Mr Jones continued to receive ad hoc information regularly from existing employees of Weiss, including documents sent via their personal email addresses. This practice appears to have commenced (as I have already noted) with Mrs Whitfield during Mr Jones' notice period in 2015, following his resignation from Weiss. After Mr Jones had left Weiss, Mrs Whitfield evidently remained in very close contact with him, and continued to send him Weiss information which she copied or forwarded from her work email to her personal email address, and forwarded on to Mr Jones from there.
90. When asked why she had used her personal email account to send Weiss information to Mr Jones' SJJ email address, Mrs Whitfield repeatedly obfuscated, claiming that she didn't know why she had done so, or that she had simply responded to emails sent from Mr Jones to her personal email address. Those responses were in my judgment wholly untruthful. The reason that Mrs Whitfield used her personal email address for this purpose was, quite obviously, to avoid detection in circumstances where she was well aware that what she was doing was wrong.
91. This was illustrated by a rather revealing exchange of emails on 30 June 2016, in which (as discussed further below in relation to sample category 36) Mrs Whitfield forwarded to Mr Jones (from her personal email account) an exchange of emails with a Weiss client, in which the client was seeking a quote for a service of ETC units. Mrs Whitfield suggested that Mr Jones should call the client to offer a competing quote, and they then discussed the possibility of Mrs Whitfield pricing the service high to encourage the customer to go with Mr Jones/SJJ. Mr Jones then warned Mrs Whitfield about sending emails to her personal address: "Be careful sending emails to your personal address they can be traced sometimes." Her response was: "I randomly do it by mistake as it automatically picks up my personal one if sending off the service ... So I can cover that if anyone says. Even others done it so I mix it up so there's no continuity ... I'm not that dull X". Mr Jones replied: "Never said you was dull you super girl. Just don't want you in trouble. Happy with all the info though".
92. Mrs Whitfield's attempts to describe this email exchange as legitimate, and her denials that she deliberately forwarded Weiss materials to her personal email account to send on to SJJ, were again palpably untruthful. The email exchange demonstrates clearly that Mrs Whitfield not only deliberately used her personal email address to send confidential Weiss information to Mr Jones, but sought to "randomly" include her personal address in work emails so as to cover her tracks.
93. By February 2016 Mr Oram was also using his personal email address in the same way to send Weiss materials to Mr Jones, at the request of the latter: see §132 below. As with Mrs Whitfield, Mr Oram denied using his personal email addresses to conceal the fact that he was sending Weiss information to Mr Jones. I consider those denials to have been, likewise, implausible and untruthful.
94. Mr Davies also provided information to Mr Jones before he left Weiss. He admitted that he had given Mr Jones passwords for the Weiss software on three occasions during the

summer of 2018 (by which time all of the other defendants had left Weiss). I consider it likely that Mr Davies provided passwords on other occasions also, not set out in his evidence.

95. The second main way in which Mr Jones received Weiss information was through the provision by the defendants of materials either on USB sticks or using some other means, either shortly before or shortly after their departure from Weiss. This was partly admitted by the defendants; but in my judgment the practice of doing so went very substantially beyond the admissions that were made.
96. Mr Oram admitted that when he left Weiss he had taken with him a USB stick with a number of folders relating to projects on which he was working during his final year at Weiss, including documents confidential to Weiss and the relevant customers, and that he had subsequently uploaded to the SJJ Dropbox at least some parts of those folders.
97. Mr Jones admitted that the other Weiss materials found on the SJJ Dropbox (which were vast in number) had “obviously come with a USB stick or a drive device of some kind”. At least some of those, he admitted, had been provided to SJJ on a memory stick supplied by Mrs Whitfield’s husband Mark, who had moved from Weiss to SJJ about a year after Mrs Whitfield’s move. It was difficult for him to avoid that admission, because the SJJ Dropbox folder structure included a set of folders under the path “Dropbox\Engineers\MW Stick\”. More generally, when cross-examined as to the source of extracts from the ServiceLife database found on SJJ’s systems, Mr Jones admitted that when the other defendants left Weiss they “may have had information on USB sticks that may have come with them”.
98. That admission was a strong indication, in my view, of the likely truth of the matter: that anyone moving from Weiss to SJJ brought with them a substantial quantity of Weiss material on USB sticks or other similar devices, which was then uploaded to SJJ’s Dropbox folder. The evidence clearly shows that Mr Oram and Mr Whitfield did so. As discussed further below, I consider it very likely that Mrs Whitfield brought with her (or transferred even before she left Weiss) substantial extracts from the ServiceLife database. As for Mr Davies, who was the last of the defendants to leave Weiss, he is alleged to have been the source of a large number of documents which were uploaded to SJJ’s systems on Sunday 29 July 2018, but he denied responsibility. I address this below.

*Documents uploaded to SJJ Dropbox on 29 July 2018*

99. A forensic review of the data obtained as a result of the search and imaging order revealed that of the approximately 40,000 documents responsive to Weiss search terms found on SJJ’s systems, 1905 documents stored on SJJ’s Dropbox folder were last accessed on 29 July 2018. The claimants’ case is that those must have been provided to SJJ by Mr Davies, who left Weiss a few days before that on 25 July 2018.
100. In particular, apart from the timing of the document upload relative to Mr Davies’ departure from Weiss, the investigation of Mr Davies’ laptop and other devices which initiated these proceedings revealed that Mr Davies had on 18 July 2018 stored Simpac software on a USB device and had also accessed Dropbox, which was prohibited for use by Weiss employees. Mr Youll also noted that Mr Davies had, in previous months, downloaded various other software files onto USBs, and had used up to 63 different USB

memory sticks that were not in Weiss's possession when he left, including one on his last day in the office (25 July 2018).

101. Mr Youll also said that on 18 July 2018 he had seen Mr Davies rummaging through large plastic tubs of IT equipment, and a few hours later had seen Mr Davies working in an office in the part of the Ebbw Vale building that had been closed down around six weeks previously as part of the closure of the site. Mr Youll noted that the lights in the office in question were off, and that Mr Davies was sitting at a desk working with his laptop and using multiple memory sticks. A short time later Mr Youll walked past the office again and Mr Davies was not there, so he went in and saw a number of memory sticks on the desk, as well as an identical USB stick still in the laptop with its light flashing. At the time, while Mr Youll thought that this was odd, he said that he had not wanted to challenge Mr Davies for fear of being perceived as confrontational. The following week, however, he discovered that Mr Davies was leaving Weiss to work for SJJ, and was concerned that Mr Davies had been using the empty office to download Weiss confidential material.
102. Mr Youll's description of this incident was first set out in his witness statement filed for the purposes of Weiss's application in September 2018 for a search and imaging order. It was repeated in his first witness statement for the trial, and he gave a consistent account of the incident when he was cross-examined by Mr Davies. His evidence was corroborated by a near-contemporaneous document, in the form of an email sent by Mr Youll to another Weiss employee on 25 July 2018: "Tony, last week I found in the back office (testing area) Chris doing something with his laptop and using memory sticks, does he have any memory sticks to hand over if he does please send them to me directly."
103. On the basis of that evidence, taken together with the evidence of the documents subsequently found on SJJ's Dropbox, the particulars of claim asserted that Mr Davies had stored Weiss material on USB sticks on 18 July 2018, which was then uploaded to SJJ's system on 29 July 2019. Mr Davies' defence denied the allegations, but offered no alternative explanation for the events of 18 July 2018; nor was this addressed in his witness statement for the trial, or his skeleton argument.
104. The first explanation from Mr Davies of his behaviour on 18 July 2018 therefore came in his cross-examination. He claimed that he couldn't remember whether he had been in the empty office on 18 July 2018, but said that he sometimes used that office after the closure of that part of the building, because there was an old desktop PC in the office belonging to a previous Weiss employee, which he used to create LogiCAD files for projects going on in the factory at the time. The reason for doing this was that, according to Mr Davies, he was having problems with doing so on his laptop. Mr Davies said that this was the only reason that he would have been in that office. He denied having used that office to transfer files from his laptop onto USB sticks, and said that he did not have access to SJJ's Dropbox until he started working at the company in September 2018.
105. In further submissions sent to the court following the circulation of my draft judgment Mr Davies said that he had sent this explanation to his former solicitors in his comments on the particulars of claim and Mr Youll's September 2018 witness statement, and he provided the court with the relevant correspondence between him and his solicitors.
106. Mr Davies' account does not, in my judgment, satisfactorily address Mr Youll's evidence on this point. It is unfortunate that his explanation of why he was using the empty office

was not included in his defence, and there is nothing before me to explain that omission. By the time Mr Davies came to draft his witness statement for the trial he was representing himself, and he may not have appreciated the importance of addressing this issue. It is, however, notable that (alone among the defendants) Mr Davies did not file any reply evidence once he saw Mr Youll's first witness statement for the trial, which set out at length Mr Youll's account of Mr Davies' conduct on 18 July 2018, and his belief that Mr Davies had been downloading Weiss confidential information onto USB sticks on that date which was then transferred to SJJ's Dropbox. If Mr Davies considered that he had a good answer to Mr Youll's evidence, it is rather odd that he chose not to address that in a reply witness statement.

107. In any event, even if Mr Davies did occasionally use the empty office for the purpose that he described, his explanation fails to account for the fact that Mr Youll said that he had seen Mr Davies using multiple USB sticks with a laptop. In cross-examination, Mr Davies accepted that it was possible that he had been seen by Mr Youll working on his laptop in the office in question. But that is inconsistent with his claim that the only reason he used that office was to carry out work on old desktop PC that had belonged to a former employee. Mr Davies also accepted that he might have been working with the lights off, as Mr Youll had said repeatedly, but he did not explain why he would have done so if he was using the empty office for a legitimate work purpose.
108. Moreover, while Mr Davies denied having access to SJJ's Dropbox on 29 July 2018, it would have been easy for someone else at SJJ to transfer the materials on that date from wherever they were previously stored to the SJJ Dropbox. The real question is therefore not who uploaded the documents to the SJJ Dropbox, but where the materials came from if not from Mr Davies, who had left Weiss only days before. By that time all of the other individual defendants were already at SJJ, so it is very unlikely that the documents derived from any of them. Nor has any defendant offered any explanation whatsoever of any other source from which the materials could have derived, if not from Mr Davies.
109. I therefore find that the most likely explanation for the presence of 1905 Weiss documents on SJJ's Dropbox, last accessed on 29 July 2018, is that they were provided in some form to SJJ by Mr Davies on his departure from Weiss. It seems very probable that Mr Davies was using the empty office on 18 July 2018 at least in part for that purpose, as observed by Mr Youll (whether or not on that occasion or other occasions he had also used the office in order to work on a desktop PC there).
110. I am not, however, able on the evidence before me to reach any conclusions as to the specific nature of the materials retained by Mr Davies and subsequently provided to SJJ, or the means by which Mr Davies copied the Weiss materials. The claimants have not identified what the relevant documents are said to have been, and it appears from an exchange that I had with Mr Howe during his closing submissions that there has not in fact been any analysis of the contents of the 1905 files last accessed on 29 July 2018. The only specific allegation is that Mr Davies stored a version of the Simpac software on a USB device, which Mr Youll suggested was retained by Mr Davies on his departure. In fact the forensic IT report produced in evidence for the initial search and imaging application shows that the USB device on which that software was stored on 18 July 2018 was one of the devices which Weiss retained, and which was provided to its forensic consultants to be imaged as part of Weiss's initial investigation following Mr Davies' departure. The forensic report does not, therefore, suggest that Mr Davies used that particular USB to take the Simpac software to SJJ.

111. Mr Davies may, however, have used other USB devices. He may also have used a Dropbox account to store Weiss files. The forensic IT analysis shows that on the morning of 18 July 2018 Mr Davies accessed a Dropbox account via his laptop. Mr Youll's evidence (again, first set out in his September 2018 witness statement, and repeated in his witness evidence for the trial) was that Weiss does not use or permit use of Dropbox for company purposes, and he commented that he did not know of any legitimate business reason why Mr Davies was accessing Dropbox on that day (and on previous occasions during 2017). Mr Davies did not either in his witness statement or in his oral evidence offer any coherent explanation of why he was using Dropbox on that day.
112. Ultimately, however, I do not need to reach any definitive conclusion as to how Mr Davies transferred Weiss materials to SJJ. For present purposes it suffices to record that I am satisfied that Mr Davies was the source for the documents uploaded to Weiss on 29 July 2018, and that it seems probable that at least part of Mr Davies' activity in that regard took place on 18 July 2018.

## **BREACH OF CONFIDENCE**

### **Legal principles**

113. It is well-established that an obligation of confidentiality may arise either under the express or implied terms of a contract, or as an equitable obligation. In the present case the claimants say that:
- i) The four individual defendants breached their express and/or implied contractual duties of confidentiality, by communicating confidential information to SJJ variously before and after they had left the employment of Weiss, and by using that information for the purposes of SJJ's business.
  - ii) All five defendants breached their equitable duties of confidentiality, by using Weiss's confidential information in SJJ's business, to the detriment of Weiss.
114. The individual defendants' express contractual confidentiality obligations are discussed above. Those made clear that information concerning Weiss, its products and its customers was regarded as strictly confidential. The Employee Handbook also made clear that all Weiss property was to be returned to the company on termination of the employment contract. In the May 2013 version applicable to Mr Jones when he left Weiss, that included company documents and papers belonging to the affairs and business of the company. In the May 2015 version applicable to the other three individual defendants, who left Weiss on later dates, the Employee Handbook expressly required the return of all company information held in a computer compatible format.
115. The seminal case of *Faccenda Chicken v Fowler* [1987] Ch 117 confirms that confidentiality obligations will also typically be implied in an employment relationship where necessary, in circumstances summarised at pp. 135–138:
- “(2) In the absence of any express term, the obligations of the employee in respect of the use and disclosure of information are the subject of implied terms.

(3) While the employee remains in the employment of the employer the obligations are included in the implied term which imposes a duty of good faith or fidelity on the employee. For the purposes of the present appeal it is not necessary to consider the precise limits of this implied term, but it may be noted: (a) that the extent of the duty of good faith will vary according to the nature of the contract (see *Vokes Ltd v Heather*, 62 R.P.C. 135); (b) that the duty of good faith will be broken if an employee makes or copies a list of the customers of the employer for use after his employment ends or deliberately memorises such a list, even though, except in special circumstances, there is no general restriction on an ex-employee canvassing or doing business with customers of his former employer ...

(4) The implied term which imposes an obligation on the employee as to his conduct after the determination of the employment is more restricted in its scope than that which imposes a general duty of good faith. It is clear that the obligation not to use or disclose information may cover secret processes of manufacture such as chemical formulae ..., or designs or special methods of construction ... and other information which is of a sufficiently high degree of confidentiality as to amount to a trade secret. The obligation does not extend, however, to cover all information which is given to or acquired by the employee while in his employment, and in particular may not cover information which is only “confidential” in the sense that an unauthorised disclosure of such information to a third party while the employment subsisted would be a clear breach of the duty of good faith ...

(5) In order to determine whether any particular item of information falls within the implied term so as to prevent its use or disclosure by an employee after his employment has ceased, it is necessary to consider all the circumstances of the case. We are satisfied that the following matters are among those to which attention must be paid:

(a) The nature of the employment. Thus employment in a capacity where ‘confidential’ material is habitually handled may impose a high obligation of confidentiality because the employee can be expected to realise its sensitive nature to a greater extent than if he were employed in a capacity where such material reaches him only occasionally or incidentally.

(b) The nature of the information itself. In our judgment the information will only be protected if it can properly be classed as a trade secret or as material which, while not properly to be described as a trade secret, is in all the circumstances of such a highly confidential nature as to require the same protection as a trade secret *eo nomine* ...

(c) Whether the employer impressed on the employee the confidentiality of the information. Thus, though an employer cannot prevent the use or disclosure merely by telling the employee that certain information is confidential, the attitude of the employer towards the information provides evidence which may assist in determining whether or not the information can properly be regarded as a trade secret ...



(d) Whether the relevant information can be easily isolated from other information which the employee is free to use or disclose. In *Printers & Finishers Ltd v Holloway* [1965] R.P.C. 239, Cross J. considered the protection which might be afforded to information which had been memorised by an ex-employee. He put on one side the memorising of a formula or a list of customers or what had been said (obviously in confidence) at a particular meeting, and continued, at p. 256:

‘The employee might well not realise that the feature or expedient in question was in fact peculiar to his late employer’s process and factory; but even if he did, such knowledge is not readily separable from his general knowledge of the flock printing process and his acquired skill in manipulating a flock printing plant, and I do not think that any man of average intelligence and honesty would think that there was anything improper in his putting his memory of particular features of his late employer’s plant at the disposal of his new employer.’

For our part we would not regard the separability of the information in question as being conclusive, but the fact that the alleged “confidential” information is part of a package and that the remainder of the package is not confidential is likely to throw light on whether the information in question is really a trade secret.”

116. As for equitable confidentiality obligations, the classic statement is that of Megarry J in *Coco v AN Clark (Engineers)* [1968] FSR 415, p. 419:

“In my judgment, three elements are normally required if, apart from contract, a case of breach of confidence is to succeed. First, the information itself ... must ‘have the necessary quality of confidence about it’. Secondly, that information must have been imparted in circumstances importing an obligation of confidence. Thirdly, there must be an unauthorised use of that information to the detriment of the party communicating it.”

117. The first of those conditions was pithily described by HHJ Waksman QC in *McGill v The Sports and Entertainment Media Group* [2014] EWHC 3000 (QB) at §148 as encompassing “information which is not generally available to others and which the possessor does not wish to be generally available”.
118. The second of the *Coco v AN Clark* conditions will apply where the receiver of the confidential information knows or should know that the information is confidential. That may be the case not only where confidential information has been disclosed in breach of an obligation of confidence, but also where confidential information innocently comes into the hands of the receiver, who should nevertheless know that it is confidential: Lord Goff in *AG v Observer (the Spycatcher case)* [1990] 1 AC 109, p. 281D–F.
119. The principle was expressed by the Supreme Court in *Vestergaard v Bestnet* [2013] UKSC 31, [2013] RPC 33 as follows:

“The classic case of breach of confidence involves the claimant’s confidential information, such as a trade secret, being used inconsistently with its

confidential nature by a defendant, who received it in circumstances where she had agreed, or ought to have appreciated, that it was confidential”.

120. As to the third requirement for a detriment arising from the use of the confidential information, use can be established in a wide variety of ways, including not only examining the material and making copies of it, but also deliberately setting out to obtain material known to be confidential. In *Tchenguiz v Imerman* [2010] EWCA Civ 908, [2011] 2 WLR 592, Lord Neuberger MR said that:

“68. If confidence applies to a defendant who adventitiously, but without authorisation, obtains information in respect of which he must have appreciated that the claimant had an expectation of privacy, it must, a fortiori, extend to a defendant who intentionally, and without authorisation, takes steps to obtain such information. It would seem to us to follow that intentionally obtaining such information, secretly and knowing that the claimant reasonably expects it to be private, is itself a breach of confidence.  
...

69. In our view, it would be a breach of confidence for a defendant, without the authority of the claimant, to examine, or to make, retain, or supply copies to a third party of, a document whose contents are, and were (or ought to have been) appreciated by the defendant to be, confidential to the claimant. It is of the essence of the claimant’s right to confidentiality that he can choose whether, and, if so, to whom and in what circumstances and on what terms, to reveal the information which has the protection of the confidence. It seems to us, as a matter of principle, that, again in the absence of any defence on the particular facts, a claimant who establishes a right of confidence in certain information contained in a document should be able to restrain any threat by an unauthorised defendant to look at, copy, distribute any copies of, or to communicate, or utilise the contents of the document (or any copy), and also be able to enforce the return (or destruction) of any such document or copy. Without the court having the power to grant such relief, the information will, through the unauthorised act of the defendant, either lose its confidential character, or will at least be at risk of doing so. The claimant should not be at risk, through the unauthorised act of the defendant, of having the confidentiality of the information lost, or even potentially lost.”

121. The remaining question is whether such use must give rise to a detriment to the claimant in order for a breach of confidence to be established. Megarry J in *Coco v AN Clark* left open the question of whether this is required in all cases, as did Lord Goff in the *Spycatcher* case. Lord Keith, however, said in that case that:

“as a general rule, it is in the public interest that confidences should be respected, and the encouragement of such respect may in itself constitute a sufficient ground for recognising and enforcing the obligation of confidence even where the confider can point to no specific detriment to himself ... So I would think it a sufficient detriment to the confider that information given in confidence is to be disclosed to persons whom he would prefer not to know of it, even though the disclosure to him would not be harmful to him in any positive way.”

122. The passage from *Tchengui* set out above is consistent with the approach of Lord Keith. *Toulson & Phipps on Confidentiality* (4<sup>th</sup> ed, 2020), §§5-021–022 draws a distinction between private and public confidences, suggesting that in the case of the former:

“the confider may have an interest in the information being kept confidential, regardless of whether disclosure would be positively harmful to it, for reasons which may be perfectly understandable (and which would be understood by any reasonable person in the position of the confidant). If so, for the reasons suggested by Lord Keith in the *Spycatcher* case, that should be sufficient to found a cause of action; and the question whether unauthorised disclosure in such circumstances is considered to involve ‘detriment’ is an exercise in semantics.”

123. On the basis of these authorities, if the defendants have deliberately and surreptitiously obtained, copied and stored the claimants’ confidential information for the purposes of a competing business, in circumstances where the defendants knew or should have known the information to be confidential, that is sufficient to establish a breach of confidence as an equitable claim. It is not necessary to show that the defendants have specifically used the material in their business, or that the claimants have suffered loss and damage as a result.
124. In light of those general principles, I will first address the allegations of breach of confidentiality obligations (whether express/implied contractual duties, or equitable obligations) in each of the various relevant categories of documents and other materials. I will then consider the claims of procuring or inducing breach of contract.

### **Breach of contractual/equitable obligations**

#### *Weiss software and passwords*

125. As described above, five software packages are relevant to these proceedings: Simpac, UpToDate3, Contour, Simpati and Magic Simpac. All five are asserted as being confidential, and in my judgment there is no doubt that they were. UpToDate3 and Magic Simpac are internal-only software packages which (on the evidence before me) Weiss has never provided to third parties outside the Weiss group. Simpac, Contour and Simpati are provided to Weiss customers, but on licence terms which include provisions prohibiting the customers from passing the software on to third parties.
126. All five software packages are password-protected, as described in the evidence of Mr Youll and Mr Ruppert:
- i) Simpac has four different levels of password access, with the service password updated every six months since 2009. All service-level functionality requires the service password. UpToDate 3 is required to get the Simpac package onto or off the Simpac controller on an ETC, such that possession of an ETC with Simpac embedded on it will not itself allow extraction of the software.
  - ii) UpToDate 3 is entirely password-protected, with different levels of password protection. The service-level password is required to perform an effective service of an ETC with a Simpac controller.

- iii) Contour functionality is protected by a USB licence key or dongle. In addition, service-level functionality is protected with passwords that are updated daily and monthly. While Contour can be operated in demo or simulation mode without a password or dongle, that does not allow use on an actual ETC.
  - iv) Simpati requires a one-off licence key, in addition to which there are various levels of password protection including passwords for service-level access to extended functionality.
  - v) Magic Simpac is entirely password-protected, with the passwords updated every six months.
127. Various of the defendants contended that the passwords for the Weiss software were not confidential, on the basis that they were (or at least some of them were) written on whiteboards in the Weiss offices. To the extent that this did occur, that would indicate that the passwords were not confidential within Weiss itself. But that does not undermine the confidentiality of the passwords as against third parties outside Weiss, and Mr Davies accepted in cross-examination that the passwords were not displayed in a publicly accessible area. The express contractual confidentiality obligations clearly prohibited communication of the passwords to third party competitors such as SJJ.
128. There is also no doubt whatsoever that the express (and, in so far as necessary, implied) contractual confidentiality obligations of the four individual defendants prohibited them from providing copies of the software or the passwords for that software to SJJ both during and after their employment at Weiss. The software was Weiss's proprietary software, developed for the purposes of the Weiss business and for use on Weiss ETCs; it therefore had the character of a trade secret, as did the passwords, and the individual defendants must have known that their obligations of confidentiality prohibited them from providing to SJJ either the software itself or any passwords for the software, at any time, whether before or after they had left Weiss. Likewise, I consider that the defendants must have known that they were not themselves entitled to use the Weiss passwords after they had left Weiss.
129. All five software packages came at various times into the hands of Mr Jones and were stored on the SJJ Dropbox, as Mr Jones admitted. The explanation given by Mr Jones was that they were all acquired legitimately from customers and from the purchase of ETCs on which copies of the software were stored. I do not accept that explanation. While it is possible that Contour and Simpati could have been obtained from customers, an email from Mr Jones to Mr Oram on 27 February 2018 indicates that they both knew that third party use of these packages without a licence was not permitted by Weiss: "I stumbled upon a Contour package complete with Dongle today at DSTL which has found its way into my van, we can use this for another customer."
130. In any event, UpToDate 3 and Magic Simpac are internal-only software packages, which are not stored on third party devices, and Simpac cannot be extracted from an ETC without UpToDate 3. It is in my view highly likely, therefore, that at least some of the software packages stored on the SJJ Dropbox were copied from the Weiss systems by one or more of the defendants prior to their departure from Weiss, and were then uploaded to the SJJ Dropbox.

131. I am not, however, on the evidence before me able to reach any definitive conclusion as to which of the individual defendants was responsible for providing any particular software package(s). The only specific allegation in that regard advanced by Weiss is that some of the software was provided by Mr Davies in the materials uploaded to the SJJ Dropbox on 29 July 2018. As discussed above, the forensic IT report and other related evidence does not enable me to identify any specific documents or files that were in the set of documents for which Mr Davies was the source.
132. The evidence before me does, however, show that on at least one occasion in February 2016 Mr Oram sent Mr Jones a set of Contour driver files and parameter configurations, while Mr Oram was still employed at Weiss. Mr Jones accepted that Mr Oram had done so at his request, and that both he and Mr Oram knew that what he was doing was wrong. Mr Oram claimed that he didn't know at the time that Mr Jones was a competitor of Weiss. That claim was utterly implausible – Mr Oram could not conceivably have failed to understand that Mr Jones had set up his own business in direct competition with Weiss. That was, indeed, precisely the reason that Mr Jones needed the material which he had requested from Mr Oram.
133. Irrespective of the means by which the Weiss software was acquired, it could not be effectively used by SJJ to service Weiss ETCs without the relevant passwords. That is why Mr Jones asked the other individual defendants (and other Weiss employees) for the current passwords for the software. That point is illustrated by two email exchanges in February 2016 in which Mr Jones noted that he would need the current Contour passwords:
- i) On 1 February 2016 Mr Jones responded to a customer support query concerning the Contour software, noting that “I have requested the passwords for Feb but unfortunately the guy at Weiss UK who receives this info from France is on Paternity leave ... Some one is looking into it for me.”
  - ii) A few days later on 4 February 2016 Mr Jones emailed the same customer saying that “I could look at the Contour issue I did speak to Chris briefly and it looks like it has been deactivated in Contour. I would need this month's password and one of you at the other end of the phone in front of the chamber ... I will see what I can find out.”
134. Similarly, around a month later on 9 March 2016, Mr Jones emailed Mr Oram (on Mr Oram's personal account) offering him “pocket money” in exchange for information, including passwords, needed to fix two Vötsch ETC chambers, commenting “I can pay in \$ dollars ready for holidays”. Mr Oram denied providing any information in response to this request; the email is, however, again indicative of Mr Jones' *modus operandi* during this period. When asked whether Mr Jones had paid Mr Oram for information on any other occasions, Mr Jones denied doing so, but admitted that he had offered Mr Oram meals out or drinks “once or twice”.
135. It appears that passwords were provided by a mixture of use of personal email accounts, online messaging systems and by telephone. Where such passwords were provided, it can be inferred that they were then used by Mr Jones/SJJ. The provision of the passwords by the defendants while they were still employed by Weiss was, as they must have known, a clear breach of their contractual confidentiality obligations, as was the continued use of Weiss passwords by the defendants once they were employed by SJJ.

136. In particular:

- i) On 7 December 2015 Mr Davies sent an email to various Weiss employees with the new UpToDate3 password to be used from 1 January 2016. The addressees included Mr Jones, who was at the time still employed by Weiss, although he was at the time on medical leave. That was not in itself a breach of confidence, in circumstances where Mr Davies was providing the password to an internal Weiss group. On 10 December, however, the day before Mr Jones' last day of employment, the email was forwarded from Mr Jones' Weiss email account to his personal email account. Mr Jones denied having done so, as did the other defendants. Given the timing, however, it is in my view overwhelmingly probable that it was indeed forwarded by Mr Jones himself to his personal email account, to enable him to make use of the password after he had left Weiss.
- ii) On 1 March 2016 Mrs Whitfield sent Mr Jones, from her personal email account, a screenshot of the daily and monthly Contour passwords for March 2016.
- iii) On 25 April 2018 Mr Davies provided an SJJ employee (not party to these proceedings) with the Contour password for that month, via an online messaging system. He also admitted providing Mr Jones with Simpac passwords on two other occasions by telephone, in June and July 2018. In his witness statement, he maintained that this was not a breach of confidentiality. When cross-examined, however, he admitted that this was wrong and he should not have provided the passwords to Mr Jones.
- iv) On 11 July 2018 Mr Oram, who was by then employed by SJJ, sent an email to various other SJJ employees (including Mr Jones and Mrs Whitfield) a link to a Dropbox folder containing Weiss software passwords, and referring to a technique used for backdating PCs to enable old passwords to be used:

“Please find a copy of some previous/current passwords for both Contour and UptoDate software packages stored in the following directory:

Dropbox\Engineers – Documents\Passwords\

As with Contour, we know we can backdate the PC to activate the passwords we know for that time period.”

Mr Oram said that he had obtained the passwords from Mr Jones, and believed that Mr Jones had in turn obtained them from Mr Davies. In so far as the passwords provided were from the period from the start of January 2018 onwards, it is likely that they were indeed provided by Mr Davies, given that Mr Davies admits providing passwords on three occasions in 2018; all of the other individual defendants had by then left Weiss; and no other source of the 2018 passwords has been suggested in the evidence before me.

137. It is also notable that where necessary Mr Jones obtained from the other defendants details of how to use the Weiss software. In particular, on 22 April 2016 Mr Oram forwarded to Mr Jones (via his personal email address) a guidance document with instructions on how to reset maintenance counters on ETCs with a Simpac controller,

with the comment “Please find invoice to follow!”. Mr Jones’ response was “You can have cash or electronic transfer or Pie and a pint in spoons ;-)”

138. Mr Oram accepted in cross-examination that the document in question was internal Weiss information, created by Mr Oram as part of his duties for Weiss. While he claimed that he had no reason to believe that it was confidential, on the basis that he had created the document, the context of the email exchange and the fact that Mr Oram sent the document using his personal email address indicates that Mr Oram knew perfectly well that this was an internal Weiss document, confidential to Weiss’s business, that he should not have been forwarding to Mr Jones.
139. On the basis of the facts set out above, therefore, all four of the individual defendants breached their contractual duties of confidentiality by providing to Mr Jones/SJJ materials related to the Weiss software packages (Mr Oram), and/or passwords to those software packages (Mr Jones, Mrs Whitfield and Mr Davies), and/or using those passwords once employed by SJJ (Mr Jones and Mr Oram).
140. As regards SJJ, the same facts establish a clear breach of its equitable obligations, in its use of Weiss software and passwords. The evidence indicates that SJJ used at least some of the Weiss software and related materials that the company managed to obtain – e.g. the 27 February 2018 email from Mr Jones cited at §129 above, noting that the Contour package that had “found its way into my van” could be used for another customer. In an earlier email exchange on 14 February 2017 a customer asked whether Mr Jones had available the software required for a particular ETC, and Mr Jones replied to Mrs Whitfield asking “Does he have a copy of the Contour disc, we have one so that’s not an issue”. As recorded above, it can also be inferred that the passwords provided to SJJ were used for the purposes of SJJ’s business. That is corroborated by the fact that passwords were shared internally, e.g. the 11 July 2018 email from Mr Oram at §136.iv) above.
141. There is no doubt that Mr Jones, SJJ’s director, knew that both the software and the passwords for that software were confidential to Weiss and that SJJ was not entitled to use any of those materials, however those materials came into SJJ’s possession.
142. All of the defendants therefore breached their contractual duties of confidentiality (in the case of the individual defendants) or their equitable obligations of confidentiality (in the case of SJJ) in the provision and/or use of Weiss software, passwords to Weiss software and/or instructions for the use of the software.

#### *ServiceLife database*

143. Mr Jones said that he took the Weiss ServiceLife database in printed format when he left Weiss. He also admitted that further extracts from the ServiceLife database had subsequently “turned up” on SJJ’s system, as he put it, including in particular lengthy extracts apparently downloaded on 16 June 2016 (with details of both customers and suppliers) and 1 August 2016 (customers only). In addition to these, the documents found on the SJJ Dropbox included a ServiceLife report dated 3 March 2017 containing a service visit schedule for Mr Whitfield for the period 6–9 March 2017.
144. When asked in cross-examination who had supplied those extracts from the database, Mr Jones’ initial answer was to “hazard a guess” that when the other defendants left Weiss they “may have had information on USB sticks that may have come with them”. When

specifically asked for the source of the June 2016 database extracts, he initially refused (repeatedly) to answer, before finally accepting that it “might” have been Mrs Whitfield, but claiming that he did not know for sure. Mrs Whitfield, for her part, denied providing any ServiceLife extracts to Mr Jones, save for the 16 June 2016 supplier list which (as discussed below) she claimed to have sent to Mr Jones for the first time in January 2018, when she was working at SJJ.

145. I do not consider those answers to be credible. If Mr Jones genuinely did not know who had supplied the database extracts to SJJ, he would have had no difficulty in saying so. His strenuous attempts to avoid answering the questions can only be explained by the fact that he knew perfectly well who had done so. The overwhelming likelihood is that the extracts from the ServiceLife database dated 16 June and 1 August 2016, found in SJJ’s possession, were provided by Mrs Whitfield. She was the senior administrator in Weiss’s service department, and therefore used the ServiceLife database continually during her daily work there. Mrs Whitfield had also been covertly assisting Mr Jones with the SJJ business from the time of its establishment, and as I have already noted this included the provision (in October 2015) of screenshots of pages on the ServiceLife database showing details of a customer of Weiss. Mrs Whitfield was also, by the summer of 2016, about to leave Weiss herself to join SJJ, whereas Mr Oram and Mr Davies did not join SJJ until 2018.
146. I also note that on 16 January 2018 Mrs Whitfield emailed a detailed Weiss supplier list (taken from the ServiceLife database) to Mr Jones, with the comment “I attach list you may recognise ...”. The list was dated 16 June 2016. Mrs Whitfield claimed that she had “inadvertently” retained this on her departure from Weiss UK, and had not provided this to Mr Jones before January 2018. That claim is wholly implausible. There is no credible reason why Mrs Whitfield would have retained a Weiss supplier list for over a year after she left Weiss to join SJJ, only to produce it in January 2018. The far more likely explanation is that all of the customer and supplier lists dated June and August 2016, which were found on SJJ’s systems, were supplied by Mrs Whitfield either while she was still at Weiss, or when she went to SJJ.
147. As for the 3 March 2017 ServiceLife report with Mr Whitfield’s visiting schedule, I do not make any specific finding as to who provided that to SJJ, save to note that the only plausible sources for this are either Mr Whitfield, who remained at Weiss UK until July 2017 before leaving to join SJJ, or Mrs Whitfield.
148. The evidence before me shows that Mr Jones started to use information taken from the ServiceLife database to provide competing quotes to Weiss customers from SJJ during his notice period at Weiss in the autumn of 2015, and continued to do so once he had left Weiss. I have already set out, at §§83–85 above, an example of Mr Jones obtaining details of Weiss’s customer CMCA from Mrs Whitfield, and using that to provide the customer with a competing quote. In addition:
  - i) On 15 October 2015 Mr Jones emailed a quote to Gary Spencer at Reeves Wireline Technologies, who was listed as a Weiss customer on the ServiceLife database.
  - ii) On 18 January 2017 Mrs Whitfield sent to Mr Jones details of Weiss’s service schedule and pricing for the customer Bergstrom. This indicates that Mrs Whitfield may well have had access to details from the ServiceLife database which went beyond the June and August 2016 extracts that were found on SJJ’s system. Mrs



Whitfield's explanation was that the relevant information had come from the customer. There is, however, no explanation of how the customer had been contacted by SJJ, if not by using the details on the ServiceLife database. There is, moreover, no contemporaneous support for her claim that the customer had supplied the information as to their service schedule and pricing (for example in the form of an email exchange between Mrs Whitfield and the customer), and I have already found Mrs Whitfield's evidence to be so thoroughly unreliable that I do not accept her explanation without further corroboration. I therefore consider it most likely that Mrs Whitfield obtained the details for the customer from the ServiceLife database.

149. More generally, Mr Jones admitted using the ServiceLife database to contact customers for SJJ's business. SJJ was also using customer details obtained from the ServiceLife database to send out marketing materials to prospective customers. The evidence before me includes five direct marketing emails sent by Mrs Whitfield on behalf of SJJ, on 6 April 2017, 15 August 2017 and three emails on 3 September 2018. Between them, the emails were sent to a total of 1,308 prospective clients, 89% of which were on the Weiss ServiceLife database. The content of the emails left no doubt that their purpose was to encourage the customers to switch from their existing service provider to SJJ. Mr Jones admitted that SJJ had used the Weiss database to compile and send these marketing emails.
150. In my judgment, therefore, the evidence establishes that Mr Jones and Mrs Whitfield breached their contractual duties of confidentiality, in taking and then using the ServiceLife database for the purposes of SJJ's business, and indeed specifically with the purpose of diverting customers from Weiss to SJJ.
151. Those defendants must have known that they were breaching their contractual confidentiality obligations by taking and using this material, which was the core Weiss information concerning its customers. Mrs Whitfield maintained, in her written and oral evidence, that she did not know that it was wrong to send Weiss customer details to Mr Jones for the purposes of the SJJ business, claiming that she did so in order to assist clients where Weiss could not provide the services required. I consider those assertions to be wholly implausible and I unhesitatingly reject them. The chain of emails in October 2015 discussed at §§83–85 above quite clearly shows that Mrs Whitfield's intention was to help Mr Jones to divert business from Weiss to SJJ, even before the expiry of Mr Jones' notice period at Weiss. Her intentions thereafter are also revealed by the emails on 30 June 2016, cited at §91 above.
152. The evidence set out above also establishes that SJJ breached its equitable obligations of confidentiality by storing and using extracts from the ServiceLife database, which Mr Jones knew to be confidential and knew to have been obtained from Weiss, in breach of his and Mrs Whitfield's contractual confidentiality obligations.
153. Mr Jones and Mrs Whitfield therefore breached their contractual duties of confidentiality, and SJJ breached its equitable obligations of confidentiality, by taking and/or using Weiss's ServiceLife database for the purposes of SJJ's business.

*Sample category 3: passwords*

154. Sample category 3 relates to Mr Jones and SJJ and contains three sample documents (from a total population of seven). The first is a list of daily and monthly Contour passwords for March 2016, which had been sent to him by Mrs Whitfield as described at §136.ii) above. The second document contains an IP address, username and password for a Vötsch intranet page which apparently related to “Schematics/software”. The third document is similar to the first, and contains daily and monthly Contour passwords for June 2016. The claimants’ case is that irrespective of the source of the passwords, the presence on SJJ’s systems of all three documents is a breach of Mr Jones/SJJ’s equitable obligations of confidentiality.
155. Mr Jones and SJJ admit that the password lists (first and third documents) were confidential to Weiss, but claim that they didn’t need to use the information because it was possible to backdate machines to access them with earlier passwords. As for the second document, Mr Jones and SJJ say that they do not know what this was and did not use it.
156. Those contentions do not, in my judgment, provide a defence to Weiss’s confidentiality claim. As already discussed, it is not necessary to show that confidential material was specifically used by SJJ for the purposes its business. It is sufficient that Mr Jones and SJJ deliberately and surreptitiously obtained, retained and stored documents that were, or ought to have been, appreciated by the defendants to be confidential to Weiss. That is clearly the case for all three documents in this sample category. I accept that the Vötsch passwords may have come to Mr Jones and SJJ together with a set of other Weiss documents obtained in the way that I have described above, and Mr Jones may not have looked at all the materials that were then stored on SJJ’s Dropbox. That should not, in my judgment, make a difference to the analysis. I accept Mr Howe’s submission that if someone sets out to acquire, and does indeed obtain, a quantity of information which they know or ought to know contains confidential information, then the act of acquiring that information (and the subsequent retention and storage of that information) is a breach of confidence whether or not they then proceed to examine each piece of the information thus obtained.
157. In any event and for completeness, in relation to Mr Jones’ submission that the Contour passwords were not needed by him or SJJ, I note that there is unambiguous evidence that during the course of 2016 Mr Jones did require Weiss software passwords in order to service Weiss ETCs (see §133 above); and Contour/Simpac passwords continued to be provided by Mr Davies on at least three occasions in 2018. That belies the suggestion that current passwords were superfluous because of the possibility of backdating the machines.
158. I therefore consider the claim of breach of confidence to be proven in relation to sample category 3.

*Sample category 21: cooling load calculations*

159. Sample category 21 again relates to Mr Jones and SJJ and contains three sample documents (from a total population of 82). All three are calculation documents, originally in Excel spreadsheet format, relating to the cooling load (part of the calibration of an ETC). The first is a complete set of calculations relating to a specific customer; the

second document is similar but only partially completed; the third document is a similar template calculation document without specific figures added. Again, the claimants' case is that the presence on SJJ's systems of all three documents is a breach of Mr Jones/SJJ's equitable obligations of confidentiality.

160. Mr Jones' submissions on this sample category were twofold. First, while he accepted that the documents were confidential in so far as they contained customer information, he denied that the template calculations were in themselves confidential. Secondly, he said that none of the three documents were of any benefit to SJJ's business since SJJ does not design, manufacture or sell new equipment.
161. I do not accept those contentions. The documents are all plainly confidential. Whether or not they are populated with customer-specific information, Mr Ruppert's (unchallenged) evidence was that these are internal documents created by a Weiss Germany employee, which contain Weiss know-how as to the calculation of cooling loads for the calibration of ETCs. Mr Jones at the very least ought to have known that the documents were confidential to Weiss. While he asserted that the calculations were standard form calculations which could be carried out by anyone with appropriate qualifications, there was no evidence of that other than Mr Jones' assertions, and Mr Jones notably did not make any specific assertions as to the specific formulae in the Excel spreadsheets.
162. Obtaining, retention and storage of the documents was therefore a breach of Mr Jones and SJJ's obligations of confidentiality, irrespective of whether or not SJJ intended to use the documents in its business. Accordingly, I consider the claim of breach of confidence to be proven in relation to sample category 21.

*Sample category 35: order consolidation forms*

163. Sample category 35 again relates to Mr Jones and SJJ and contains three sample documents (from a total population of six). All three are order consolidation forms which summarise the details of orders by Weiss customers. They provide extensive information not only of the customer's specific technical requirements, but also the agreed warranty terms and payment terms, as well as attaching the relevant customer emails by which the order was agreed. Those emails contain further detailed information such as breakdowns of hourly rates for repairs and special discounts agreed. Again, the claimants' case is that the presence on SJJ's systems of all three documents is a breach of Mr Jones and SJJ's equitable obligations of confidentiality.
164. Mr Jones and SJJ's defence is that (as with category 21) the information contained in the documents was irrelevant, since SJJ does not design, manufacture or sell new equipment; and that some of the information in the attached emails appears to come from publicly available sources such as legislation.
165. Again, I do not accept these contentions. The documents are all plainly confidential, containing very detailed customer-specific information including pricing and payment terms. Mr Jones either knew or ought to have known that the documents were confidential to Weiss. Obtaining, retention and storage of the documents was therefore a breach of Mr Jones and SJJ's obligations of confidentiality, irrespective of whether or not SJJ intended to use the documents in its business.

166. I therefore consider the claim of breach of confidence to be proven in relation to sample category 35.

*Sample category 36: external emails*

167. Sample category 36 relates to Mrs Whitfield and contains two sample documents (from a total population of three). The claimants' case is that both constituted breaches of confidence by Mrs Whitfield. The first document shows a chain of emails between a Weiss customer, Weatherford, and Weiss, discussing the renewal terms for Weiss's annual service agreement, which Mrs Whitfield forwarded to Mr Jones.
168. The chain started with an email on 13 January 2016 from Kym Lewis, another service administrator at Weiss, noting the imminent expiry of the service agreement and attaching a renewal quotation. It appears that Mrs Whitfield was aware of this quotation, because on the same day, in a separate email in evidence before me (but not part of the email chain in the sample document) she forwarded the quote from her personal email address to Mr Jones.
169. In subsequent emails which were then copied to Mrs Whitfield, the customer asked for a revised quotation, which was sent (again by Kym Lewis) on 19 January 2016. On 10 February 2016 the customer responded that it had received another lower quote for the service contract, and asked if Weiss was able to match that. Mrs Whitfield forwarded that email to Mr Jones, with the comment "Just seen this FYI X".
170. In cross-examination, both Mrs Whitfield and Mr Jones accepted that the competing quote had come from Mr Jones. Mrs Whitfield also accepted that the email of 10 February 2016 was a confidential communication, which she had received as an employee of Weiss, and that it was improper for her to have forwarded this to Mr Jones. Mr Jones likewise conceded that the reason why Mrs Whitfield had forwarded him the initial quote (on 13 January 2016) was to enable him to undercut Weiss, and that both he and she knew that this was improper. He then made the following admission:

"Q. You see, the situation is, Mr Jones, that this client is an example of how you have taken business from Weiss, isn't it, by stealing and misusing their internal information?

A. Yes."

171. Those admissions were, in my judgment, properly made. There is no conceivable doubt that a quotation by Weiss for the renewal of its service agreement with an existing customer is a highly confidential document which should never have been sent to Mr Jones, and Mrs Whitfield must have known that doing so was a breach of her contractual duties of confidentiality.
172. The second document in the sample category is an email chain on 30 June 2016 to which I have already referred (§§91–92 above), in which Mrs Whitfield forwarded to Mr Jones a request from a Weiss client, Gooch, to quote for a service job. The conversation between them is illuminating of the way in which Mrs Whitfield willingly assisted and encouraged Mr Jones in his attempts to divert business from Weiss:

- i) On 29 June 2016 a Weiss customer asked Weiss for a quotation to calibrate two pieces of equipment not on the existing Weiss service contract. The request was forwarded to Mrs Whitfield to address.
  - ii) 30 June 2016 Mrs Whitfield had an exchange of emails with the customer as to the type of equipment and levels of calibration required, in which she copied in her personal email address.
  - iii) She then forwarded the entire exchange of emails to Mr Jones, in the evening, from her personal email address, with the comment “May be you just need to call these to quote ... off the cuff? Coincidentally ...”
  - iv) Mr Jones replied, “I would have no problem calibrating these two ovens. Maybe if you price it high he might contact me. I did have good correspondence with him before he placed the contract with Weiss.”
  - v) Mrs Whitfield responded indicating the price she might quote: “Hi not sure if our kit can calibrate that system so probably have £800 for two levels plus £750 call out and I could add another £550 to cover next day ... High enough?”
  - vi) Mr Jones replied “The price is right” followed by a laughing emoji. He then continued with the warning about Mrs Whitfield’s personal emails which I have discussed above, with the subsequent reply from Mrs Whitfield.
  - vii) The email exchange ended with Mrs Whitfield commenting “CCTV with parts going in my car ... But that could be for Mark. fcuk um as Bas would say”, interspersed with similar emojis.
173. Mr Jones admitted, in cross-examination, that this was improper conduct on the part of Mrs Whitfield, and that he knew that she should not be sending him emails containing information about Weiss UK’s dealings with its customers.
174. By contrast Mrs Whitfield (consistent with many of her other responses) denied that it was wrong, and claimed that she had sent Mr Jones the customer request in order to benefit the customer and enable the work to be done. I have no hesitation in rejecting that explanation. The entire tenor of Mrs Whitfield’s comments in this email chain (including the section in which she discussed her use of her personal email address) make absolutely clear that she was well aware that she was improperly providing Mr Jones with highly confidential Weiss information, and that she regarded Weiss (and her obligations to the company) with little more than contempt. This email exchange is a clear and obvious breach of Mrs Whitfield’s contractual duties of confidence.
175. I therefore consider the claim of breach of confidence to be proven in relation to sample category 36.

*Sample category 44: internal technical materials*

176. Sample category 44 relates to Mr Oram and contains two sample technical documents (from a total population of five) sent by Mr Oram to another SJJ employee. Both are said by the claimants to constitute breaches of confidence by Mr Oram.

177. The first document is a service and configuration manual containing technical information and drawings relating to Simcon 32 controllers for ETCs (which are an older type of controller used by Weiss before the introduction of Simpac controllers). It was emailed by Mr Oram to an employee of SJJ on 6 August 2018, with a cover note explaining that the document contained a drawing of a cable that Mr Oram required, and asking for that cable to be made.
178. In his written closing submissions Mr Oram submitted that the document was available on the SJJ Dropbox when he joined the company, and that it had been provided to numerous engineers at Weiss, who were not told that the document was confidential or that it should be returned to Weiss on their departure. He also said that the cable in question was in fact never made by SJJ.
179. The second document is a presentation delivered at a Weiss service meeting on 28 June 2015, containing technical information regarding the Contour software. It was emailed by Mr Oram to the same SJJ employee on 11 July 2018.
180. Mr Oram said, again for the first time in his closing submissions, that the document was available on the SJJ Dropbox when he joined the company. He said that he believed that the information in the presentation was not confidential, since it had been written by him and had been provided to numerous engineers at Weiss, and he had himself provided that document or similar documents to customers and engineers during his employment at Weiss, to assist them in installing and using Contour. He also said that he could have rewritten the document from scratch if necessary.
181. Mr Howe noted that these explanations had not previously been set out in Mr Oram's evidence. Nor was any of this pleaded in Mr Oram's response to the relevant Schedule to the particulars of claim. I do, however, have to bear in mind that Mr Oram has acted as a litigant in person throughout these proceedings, and (as I have already noted) the claimants did not confirm their position as to the samples to be addressed until quite late in the trial, after the evidence had been concluded. I also note that Mr Howe could have, but did not, put any questions to Mr Oram in cross-examination as to his position on the documents in sample category 44. I do not, therefore, consider that I should disregard the submissions made by Mr Oram in his closing submissions.
182. Those explanations do not, however, provide a defence to the breaches of confidence alleged in relation to these sample documents. Regarding the service and configuration manual, which is the first sample document, it is marked on the front page "**!! For internal use only !!**", in a prominent box. Even if provided to multiple Weiss engineers, there could have been no doubt that it was an internal Weiss technical document which was confidential to Weiss, and Mr Oram must have known that.
183. Accordingly, even if it was already present on SJJ's servers when he joined the company (as to which there is no concrete evidence either way), it was a breach of Mr Oram's equitable obligations of confidence for him to forward a copy of the document to another SJJ employee, whatever use was in fact subsequently made of the material.
184. As to the internal presentation, which is the second sample document, that is not marked as being for internal use only, but there is in my judgment no doubt that it was confidential to Weiss. It may be that some of the information is material that, of itself, would not be described as highly confidential, such as the operating system required for

particular versions of the Contour software, or the directory into which Contour is installed on an operating system. Much of the presentation, however, contains highly technical information including technical diagrams, detailed configuration instructions and driver debugging instructions including code changes. All of this was Weiss's proprietary information, relating to its proprietary software. Even if Mr Oram did write the presentation, he did so as part of his duties for Weiss, and there is no evidence that the presentation was publicly available outside Weiss. I consider that Mr Oram either knew or at least should have known that it was confidential to Weiss.

185. Again, therefore, regardless of whether it was already present on SJJ's servers when Mr Oram joined the company (as to which, as with the first sample document, there is no evidence either way), it was a breach of Mr Oram's equitable obligations of confidence for him to forward a copy of the document to another SJJ employee.
186. I therefore consider the claim of breach of confidence to be proven in relation to sample category 44.

### **Procuring or inducing breaches of contract**

187. The remaining issue in relation to the claims for breaches of confidence is the extent to which the breaches of contractual duties of confidentiality by Mr Davies, Mrs Whitfield and Mr Oram were procured by Mr Jones.
188. The ingredients of the tort of inducing or procuring a breach of contract were summarised by Morgan J in *Aerostar Maintenance International v Wilson* [2010] EWHC 2032 (Ch) at §163 (recently cited by Bryan J in *Lakatamia Shipping v Nobu* [2021] EWHC 1907 (Comm), §125) as follows:

“first, there must be a contract, second, there must be a breach of that contract, thirdly, the conduct of the relevant defendant must have been such as to procure or induce that breach, fourthly, the relevant defendant must have known of the existence of the relevant term in the contract or turned a blind eye to the existence of such a term and, fifthly, the relevant defendant must have actually realised that the conduct, which was being induced or procured, would result in a breach of the term.”

189. As Morgan J noted in that summary, the requirement of knowledge of the contractual term is satisfied by blind-eye knowledge, where the defendant is “knowingly, or recklessly, indifferent” to whether the conduct procured is a breach of contract or not: Lord Denning in *Emerald Construction v Lowthian* [1966] 1 WLR 691, pp 700–701, cited with approval in *OBG v Allan* [2007] UKHL 21, [2008] 1 AC 1, §§40–41.
190. I have already found that Mr Davies, Mrs Whitfield and Mr Oram breached their contractual confidentiality obligations by providing (between them) software, passwords to the software, instructions for the use of the software and other technical documents, extracts from the ServiceLife database, and details of Weiss negotiations with customers for service contracts.
191. There is no doubt whatsoever that those breaches of contract were procured or induced by Mr Jones. The evidence before me is replete with examples of Mr Jones asking for confidential Weiss material to be provided to him: see e.g. the emails cited at §§133 and

134 above. In respect of other materials, even if they do not contain an express request from Mr Jones, it is evident from the context and/or the evidence of the other defendants that they were sent to Mr Jones in response to requests from him: see e.g. §§83, 136.ii) and iii), 137 and 146 above.

192. In cross-examination, Mr Jones repeatedly admitted that he had sought and obtained passwords and other Weiss materials (such as the Contour driver files sent by Mr Oram, discussed at §132 above) from Weiss employees. He denied, however, that he had asked the other defendants to bring material with them when they left Weiss, suggesting that documents had simply turned up on SJJ's system without his knowledge. An example was the following exchange in cross-examination:

“Q. ... is it really your evidence that you can't offer any explanation to the court how this and hundreds of other documents from Weiss that are clearly sensitive, commercially sensitive, have ended up in your company's possession? Is that really your evidence? You have no idea?

A. I have no idea. They've obviously come on board, but I've no idea how they're on there. They've obviously come with a USB stick or a drive device of some kind.

Q. Because you asked them to, didn't you, Mr Jones?

A. No, no.”

193. I do not accept Mr Jones' evidence on this point. As the owner and director of SJJ, he must have known how his company had come into possession of Weiss documents such as its pricing discussions with customers. The only explanation can have been that – as Mr Jones himself suggested – those documents were provided to SJJ by someone who was either at Weiss or had been at Weiss; and it is implausible to suggest that any Weiss employee or ex-employee would have done that if they had not been asked to do so by Mr Jones.
194. It is evident from my findings above that the other defendants were willing participants. Indeed, the documents from sample category 36 discussed at §§167–174 show that Mrs Whitfield proactively forwarded to Mr Jones details of Weiss's negotiations with customers, in order to assist him to win business for SJJ. Mr Jones accepted, however, that he encouraged Mrs Whitfield to do so. In relation to the email exchange on 30 June 2016, cited at §172 above:

“Q. ... She's alerting you to a potential business opportunity.

A. Yes.

Q. Which she had no business doing, did she? You knew what she was doing was wrong?

A. Yes.

Q. ... So what you're encouraging her to do is to overprice the Weiss offer or quote so that it increases the chance of you getting the business?

A. Yes.

Q. That's what you're asking her to do, isn't it?

A. There's history behind that, but, yes, in the light of that sentence, yes.

Q. And you knew that was wrong as well, didn't you?

A. Yes.

...



Q. ... what I've just shown you here is ... an example of you and Mrs Whitfield deliberately trying to divert business from Weiss to your company in a way that's completely improper?

A. Yes."

195. Mr Jones, on his own admission, knew that it was wrong for the other defendants to provide him with this sort of material. He was well aware, from the terms of his own contract and the letter sent to him on 8 October 2015 following his resignation, that he himself was subject to confidentiality obligations, and he must at that time have either known that the other individual defendants were subject to the same contractual conditions or, at the very least, was recklessly indifferent to that.
196. By September 2016, moreover, there is no doubt that Mr Jones had actual knowledge of at least Mrs Whitfield's contractual confidentiality obligations, since he had seen the letter sent to Mrs Whitfield by Weiss on 5 September 2016, which cited the confidentiality clause in her contract (set out at §56 above). Mr Jones must either have known that Mr Davies and Mr Oram were subject to the same contractual terms, or (again) at the very least was recklessly indifferent in that regard.
197. There is also, in my judgment, no doubt that Mr Jones knew that the conduct that he was inducing or procuring was in breach of those terms. Indeed in relation to some of the conduct he effectively admitted as such. One example is the exchange above. Another example is his answers to questions about the passwords provided by Mr Davies in June and July 2018:

"Q. ... you asked Mr Davies for the password more than once, didn't you?

A. For the Simpac, yes.

Q. According to Mr Davies you asked him in late June 2018 by text message; is that right?

A. Yes.

Q. And you also asked him in July 2018?

A. Yes.

Q. And again, those are both examples, aren't they, of you asking Weiss employees to do things which you knew were wrong?

A. Yes."

198. Considering the evidence as a whole, therefore, I consider that the breaches by Mr Davies, Mrs Whitfield and Mr Oram of their contractual confidentiality obligations were induced or procured by Mr Jones and SJJ.

## **COPYRIGHT CLAIMS**

### **Legal principles**

199. The Copyright, Designs and Patents Act 1988 (the **CDPA**) protects copyright in, among other things, original literary works, which are defined in s. 3(1)(b) of the CDPA to include computer programs.
200. Under the CDPA, infringing acts include copying the work by reproducing the work in any form, including storing the work in any medium by electronic means (s. 17(2)),

issuing copies to the public, by putting into circulation copies not previously put into circulation by or with the consent of the copyright owner (s. 18), communicating the work to the public (s. 20), possessing infringing copies in the course of business, knowing or believing the material to be an infringing copy of the work (s. 23).

201. There is a considerable body of case-law as to the interpretation of these provisions. I will address it, in so far as relevant, when dealing with the specific alleged infringing acts below.

### **Breaches of copyright**

202. Following the narrowing of the issues for the trial, the copyright claims are now limited to claims that the defendants infringed copyright in three of the Weiss software packages, namely Simpac, UpToDate3 and Contour, as follows:

- i) Mr Davies is said to have infringed copyright in the software by (a) providing copies of it to and/or otherwise making Contour available to Mr Jones and SJJ in around June/July 2018, and (b) subsequently copying or downloading the software from the SJJ Dropbox in around September 2018 when he joined SJJ.
- ii) Mr Jones and SJJ are said to have infringed copyright by (a) storing the software on the SJJ Dropbox, (b) copying the software to some or all of the other individual defendants and other SJJ employees, when the software was downloaded by them from the SJJ Dropbox, (c) possessing copies of the software in the course of business, knowing that they were infringing copies, and (d) providing copies of Contour to third parties and/or clients of SJJ.
- iii) Mrs Whitfield is said to have infringed copyright in the software by copying the programs from and/or storing them on the SJJ Dropbox, after she joined the company in September 2016.
- iv) Mr Oram is said to have infringed copyright in the software by copying or downloading it from the SJJ Dropbox, after he joined the company in January 2018.

203. The claimants' position as to the subsistence of copyright in the Simpac, UpToDate3 and Contour software packages, and the ownership by Weiss of the copyright in those software packages, is set out in particulars of claim and the evidence of the claimants' witnesses. As I have already noted by the time of the defendants' closing submissions the defendants no longer disputed the subsistence of copyright in or the claimants' ownership of the copyright in any of these three software packages. (The claimants do not, at least in these proceedings, assert title to copyright in the other two software packages relevant to these proceedings, Simpaci and Magic Simpaci.)

204. The only remaining issue, therefore, is whether the defendants' conduct infringed copyright in that software.

### *Mr Davies*

205. It follows from my findings above that I do not consider it to have been established, on the evidence before me, that Mr Davies provided copies of Contour or the other software to Mr Jones/SJJ in or around June/July 2018. I have found that Mr Davies was, most

probably, the source of the 1905 Weiss documents on SJJ's Dropbox which were last accessed on 29 July 2018. As I have explained above, however, the material before me does not identify the nature of those materials. Nor does the other evidence before me (such as the forensic IT report on the documents found on Mr Davies' devices retained by Weiss) allow me to conclude that Mr Davies provided software to Mr Jones on or around those dates.

206. Mr Davies has, however, admitted that he downloaded UpToDate3 and Contour (as well as Magic Simpac) from the SJJ Dropbox onto his company laptop when he started work at SJJ. That was, in principle, an infringement within the meaning of s. 17(2) CDPA. Mr Davies said that the download happened automatically by virtue of the synchronisation function in Dropbox. A primary infringement of copyright is, however, a tort of strict liability, for which ignorance is not a defence. In any event Mr Davies accepted that he was aware of what was on his laptop after the synchronisation had occurred. He was therefore aware that the Weiss software had been downloaded and also knew how it had been downloaded.
207. In those circumstances, I find that Mr Davies infringed the claimants' copyright in the UpToDate3 and Contour software by downloading it in around September 2018.

*Mr Jones and SJJ*

208. There is no dispute that the copyright software was stored on the SJJ Dropbox. That was again, therefore, an infringement under s. 17(2) CDPA, irrespective of Mr Jones' knowledge of how it got there (although as set out above I have rejected the suggestion that Mr Jones was not aware how his company had come into possession of Weiss's confidential materials, including the software). I do not, therefore, need to make any findings as to whether copyright was also infringed within the meaning of s. 23 CDPA in relation to the same conduct.
209. As regards Mr Jones and SJJ's involvement in the downloading of copies of the software to Mr Davies' SJJ laptop, the evidence does not reveal exactly how that occurred save for Mr Davies' account that it resulted from the synchronisation of files within Dropbox. That is not in itself sufficient for me to reach any conclusion as to Mr Jones and SJJ's liability for that. Nor, in any event, does the evidence establish that the software was copied to the computers or other devices used by Mrs Whitfield and Mr Oram. The claimants' case on that is based solely on the inference that if the software was copied to Mr Davies' laptop because of the synchronisation feature of Dropbox, the same must also have occurred in relation to the computers used by Mrs Whitfield and Mr Oram. Whether or not that did, however, occur would have depended on the Dropbox synchronisation settings on the relevant computers used by those defendants. I do not, however, have any evidence on that point; nor is there any evidence showing that those defendants did indeed have the copyright software stored on their devices.
210. The final allegation of copyright infringement in respect of Mr Jones/SJJ is that copies of Contour are said to have been provided to third parties and/or clients of SJJ, on three occasions.
211. First, on around 14 February 2017, Mr Jones and SJJ are said to have supplied a copy of Contour to a client NTU. The evidence relied upon is the email exchange cited at §141 above. That does not, however, establish that the software was supplied to NTU; the

email simply asks whether the client had a copy of the software and indicated that if not one could be supplied. The claimants' case in this regard is, therefore, based entirely on inference, and I do not accept that the evidence in this regard is sufficient to establish infringement.

212. Secondly, on around 2 June 2017, Mr Jones and SJJ are said to have supplied a copy of Contour to another client Helical Technology. Again, however, the evidence does not establish that the software was supplied. The email in question (sent by Mr Jones on that date) simply provides a quotation to supply and install Contour software, and comments that "I might be able to get my hands on a Demo version". Again, the claimants' case is based entirely on inference, and I do not accept that the evidence establishes an infringement.
213. Thirdly, Mr Jones and SJJ admit supplying a demo version of Contour to a software developer TBG Solutions in May 2018, with a view to developing an alternative product. By contrast with the other two allegations, there is no dispute that the supply took place (and is evidenced in the contemporaneous exchange of emails between Mr Jones and TBG). Nor is it said that the demo version of the product fell outside the claimants' copyright rights in the software.
214. Mr Howe's explanation of the basis on which this constituted an infringement of copyright was, however, rather opaque. He suggested that it amounted to a communication to the public within the meaning of s. 20 CDPA. However *Copinger and Skone James on Copyright* (18<sup>th</sup> ed, 2021) summarises the case-law on the interpretation of this provision at §7-237(3) as including the point that the words "the public" means "an indeterminate number of potential recipients and implies a fairly large number of persons. It excludes groups which are too small or insignificant." Mr Howe did not explain how the provision of a version of Contour to a single developer could satisfy that test.
215. Mr Howe also appeared to suggest that the conduct could fall within s. 18 CDPA, as an act of issuing copies to the public. That requires, however, an act of "putting into circulation" copies of the relevant work, which according to *Copinger* at §7-147 "suggests a release of a copy onto the market such that it may be passed on to other members of the public". Again, he did not explain in either his written or his oral submissions how this resulted from providing the software to a single developer.
216. Mr Howe's final suggestion was that the provision of the software to TBG involved an act of copying within the meaning of s. 17 CDPA. I accept that submission, on the basis that the admitted supply of Contour to TBG must have required the copying of the software for provision to the developer in some form.
217. I therefore find that Mr Jones and SJJ infringed the claimants' copyright in the Simpac, UpToDate3 and Contour by storing the software on the SJJ Dropbox, and by copying Contour in order to supply it to the software developer TBG. The claims of infringement by copying the software to the other defendants and clients of SJJ are not, in my judgment, established on the evidence before me.

*Mrs Whitfield and Mr Oram*

218. The allegations that Mrs Whitfield and Mr Oram downloaded the copyright software are, as I have already found, not established.
219. The remaining allegation is that Mrs Whitfield infringed the claimants' copyright in the software on the basis that she was the named administrator of the SJJ Dropbox. That allegation was, however, not developed by Mr Howe in his submissions, and the claimants' case in this regard remains entirely vague. I therefore do not make any findings on this point.
220. The claims of copyright infringement are therefore, in my judgment, not established as against Mrs Whitfield and Mr Oram.

## **DATABASE RIGHTS**

### **Legal principles**

221. The Copyright and Rights in Databases Regulations 1997 implemented, in the UK, Directive 96/9/EC on the legal protection of databases [1996] OJ 77/20. The Regulations provides, in Regulation 13(1), that a database right subsists if there has been a substantial investment in obtaining, verifying or presenting the contents of the database. A database is defined in s. 3A of the CDPA (as inserted by Regulation 6 of the 1997 Regulations) as a collection of independent works, data or other materials, which are arranged in a systematic or methodical way, and are individually accessible by electronic or other means.
222. In Case C-203/02 *British Horseracing Board v William Hill* EU:C:2004:695, §31, the CJEU said that the concept of an investment in obtaining the contents of a database must be understood to refer to:
- “... the resources used to seek out existing independent materials and collect them in the database, and not to the resources used for the creation as such of independent materials. The purpose of the protection by the *sui generis* right provided for by the directive is to promote the establishment of storage and processing systems for existing information and not the creation of materials capable of being collected subsequently in a database.”
223. The *sui generis* database right therefore protects the collection and processing of data in a database, rather than the creation of the data in the first place. As the CJEU went on to explain, the same person can both create the original data and rely on the database right in respect of the processing of those data, provided that there is an independent substantial investment in the latter:
- “35. ... the fact that the creation of a database is linked to the exercise of a principal activity in which the person creating the database is also the creator of the materials contained in the database does not, as such, preclude that person from claiming the protection of the *sui generis* right, provided that he establishes that the obtaining of those materials, their verification or their

presentation ... required substantial investment in quantitative or qualitative terms, which was independent of the resources used to create those materials.

36. Thus, although the search for data and the verification of their accuracy at the time a database is created do not require the maker of that database to use particular resources because the data are those he created and are available to him, the fact remains that the collection of those data, their systematic or methodical arrangement in the database, the organisation of their individual accessibility and the verification of their accuracy throughout the operation of the database may require substantial investment in quantitative or qualitative terms ...”

224. Under Regulation 16 a person infringes the database right in a database if, without the consent of the owner of the right, they extract or reutilise all or a substantial part of the contents of the database. “Extraction” is defined in Regulation 12(1) as the permanent or temporary transfer of any of the contents of the database to another medium by any means or in any form.
225. The concept of extraction from a database was considered by the CJEU in Case C-304/07 *Directmedia Publishing v Albert-Ludwigs-Universität Freiburg* EU:C:2008:552, from which the following principles in particular can be derived:
- i) The decisive criterion is the existence of an act of “transfer” of all or part of the contents of the database to another medium, whether of the same nature as the medium of the database or a different nature (§36).
  - ii) It is immaterial whether the transfer is effected through a technical process (e.g. electronic means) or by manual means (§37).
  - iii) It is also immaterial that the contents of the database are rearranged or adapted during the process of transfer (§§39–40).
226. As the Court of Appeal confirmed in *Football Dataco v Sportradar* [2013] EWCA Civ 27, §73, there can be an act of extraction of data where those data are uploaded onto and stored on a computer, even if the user of the computer has not read or accessed the relevant data.

### **Breaches of database rights**

227. The claimants rely on database rights in the Weiss ServiceLife database, as against Mr Jones, SJJ and Mrs Whitfield. Specifically:
- i) Mr Jones and SJJ are said to have infringed the claimants’ database rights by (a) taking an extract of the ServiceLife database from Weiss and providing it to SJJ/storing it on SJJ’s Dropbox; (b) storing on SJJ’s Dropbox extracts of the ServiceLife database dated 16 June 2016, 1 August 2016 and October 2017, as well as a Service Schedule dated 3 March 2017; and (c) sending direct marketing emails in April 2017, August 2017 and September 2018 to email addresses extracted from the ServiceLife database.

- ii) Mrs Whitfield is said to have infringed the claimants' database rights by (a) taking and providing to Mr Jones/SJJ extracts of the ServiceLife database 16 June 2016 and 1 August 2016; and (b) sending (on behalf of SJJ) the direct marketing emails in April 2017, August 2017 and September 2018.
228. Mr Jones, SJJ and Mrs Whitfield deny that the claimants have protectable rights in the ServiceLife database, on the grounds that they had not demonstrated substantial investment in the "obtaining, verification and presentation" of the data. Rather, it is said, the data in the database were already in Weiss UK's possession through the conduct of its business, and the database itself was generated by use of the ServiceLife software.
229. As for the claims regarding extraction and use of the content of the database, insofar as database rights subsist in that database, Mr Jones admitted receiving extracts from the ServiceLife database but denied that this was an infringement of the claimants' database rights. He claimed that SJJ's customer list had been built up over years of trading based on Mr Jones' acquired knowledge of Weiss's customers, together with direct contacts from those customers to SJJ.
230. Mrs Whitfield denied providing any part of the database to Mr Jones/SJJ, or using the database for the purposes of SJJ, save for the supplier list which she forwarded to Mr Jones on 16 January 2018, for which her explanation was as described at §146 above. She also claimed that the direct marketing emails sent out by her were based on the information on SJJ's system, the source of which was unknown to her.

*Subsistence of database rights*

231. The arguments regarding the subsistence of database rights, while pleaded in the defences of Mr Jones/SJJ and Mrs Whitfield, were not addressed by those defendants at the trial and are, in my judgment, misguided. The fact that the customer data on the database had been generated through the conduct of Weiss UK's business does not prevent a database right arising in relation to the collection, organisation and presentation of those data within the ServiceLife database, as the CJEU made clear in §§35–36 of *British Horseracing Board*, cited above.
232. What is relevant is the investment in the processing of the data within the database. As to that, Mr Youll's unchallenged evidence was that between 2003–2019 the ServiceLife database was the main tool used daily by the service administration department to collect, organise and verify both customer data and supplier data. The customer data included customer name and contact information, site details, maintenance history, service contracts including renewal dates and pricing, and future contract proposals. The supplier data included name and contact information, payment terms and correspondence. The data collected in the software were arranged in a systematic and methodical way, and were used to generate reports such as service schedules, as well as invoices. Mr Youll estimated that around 90% of the service administrators' time was spent on obtaining, updating, appending and verifying the data recorded on the database.
233. While Mr Youll also put forward an estimate of the cost of that investment, based on the time spent by the Weiss UK service administration team, I do not need to decide that point; it suffices to say that the investment by Weiss UK in the collection, organisation and verification of the data within the database was on any view a substantial investment that was independent of the resources used to create the original data. The fact that the

database used third party ServiceLife software is immaterial – the relevant investment for these purposes was the investment in the collection, organisation and verification of the data within the database, which gives rise to a protectable right under Regulation 13.

*Taking and storing of extracts of ServiceLife database*

234. The claim against Mr Jones and SJJ in respect of the taking and storing of extracts of the ServiceLife database on SJJ's systems is unanswerable. Mr Jones has admitted that he took extracts from the database with him when he left Weiss, and that further extracts were stored on SJJ's systems thereafter, namely extracts dated 16 June 2016 (both customers and suppliers) and 1 August 2016 (customers only), and the 3 March 2017 report setting out a visit schedule for Mark Whitfield.
235. The taking of such extracts and/or storage of those documents unquestionably amounted to "extraction" within the meaning of Regulation 16, on the part of Mr Jones/SJJ. I have already found that Mrs Whitfield was, in all probability, the source of (at least) the database extracts dated 16 June and 1 August 2016. She therefore breached Weiss UK's database rights when she extracted those reports from the ServiceLife database and saved them on some medium (whatever it was) in order to provide them to Mr Jones/SJJ.
236. As for the list of customers dated October 2017, Mr Jones' evidence at trial was that this was not a direct extract from the ServiceLife database, but was rather a list of SJJ's customers. He accepted, however (reluctantly, and after considerable prevarication), that this had been compiled at least in substantial part by using the ServiceLife database to contact customers, whose details were then put into SJJ's own database if they became SJJ customers. That was therefore likewise an act of extraction of a substantial part of the database, amounting to an infringement under Regulation 16 by Mr Jones and SJJ, even if the resulting "SJJ" customer list rearranged or adapted the information obtained from Weiss UK's database.
237. Mr Jones' admissions also, incidentally, discredit his pleaded claim that the SJJ customer list was built using Mr Jones' own contacts and on the basis of direct contacts from customers to SJJ.

*Direct marketing emails*

238. Mr Jones admitted in cross-examination that SJJ had used the Weiss database of customers to compile and send the five direct marketing emails in 2017 and 2018. It is common ground that Mrs Whitfield sent those emails. The extraction of substantial customer details for the purposes of those marketing emails therefore amounted to a further infringement of the claimants' database rights by SJJ.
239. The allegation in the particulars of claim regarding the marketing emails is, however, confined to an allegation against SJJ. The particulars of claim do not allege wrongful conduct by either Mr Jones or Mrs Whitfield in that regard. I do not, therefore, need to decide whether the marketing emails were also an infringement by those two defendants.

**OTHER ISSUES**

240. There are three remaining issues which, for different reasons, I do not need to determine.



## **Unlawful means conspiracy**

241. The first of those issues is the claimants' case on conspiracy to cause loss by unlawful means. The claimants' case in that regard is that from around September 2015 Mr Jones and SJJ conspired with intent to injure Weiss by using the information on the ServiceLife database to identify customers and their requirements, so as to compete with Weiss, and then to use infringing copies of Weiss's proprietary software, as well as confidential passwords and other confidential information so as to offer service contracts to those customers. The unlawful means relied on by the claimants are the breaches of contractual and equitable confidentiality obligations, breaches of copyright and breaches of database rights set out above. The other defendants are said to have become party to the conspiracy from dates between October 2015 and July 2018.
242. The claimants' pleaded case on conspiracy is extremely cursory, and was not fully developed at the trial. Mr Howe's submissions on the law were confined to a citation (in his skeleton argument) of a summary of the elements of the tort; as for the facts, his submissions amounted to little more than the identification of certain elements of the conduct of the various defendants. I also note that the submissions at trial – such as they were – were not entirely consistent with the pleaded case in the particulars of claim.
243. I do not consider that this is a satisfactory basis for me to determine this issue, particularly in circumstances where the defendants are now all acting in person. If, following my judgment on the other issues in this case set out above, the claimants wish to pursue this aspect of their claim, it will need to be addressed separately with further submissions on both the law and the evidence.

## **Loss and damage**

244. The second outstanding issue is the question of loss and damage. As I have already noted, the issue of the quantum of the claimants' loss is not before me in this trial. Nevertheless, the question of whether the claimants have suffered more than merely nominal loss and damage could arise as a threshold liability issue in two ways.
245. First, it is common ground that the causation of loss is a constituent element of the tort of conspiracy to cause loss by unlawful means. Having regard to my comments above regarding the claimants' conspiracy claim, however, I do not need to address that now.
246. Secondly, there is a question as to whether it is necessary to show detriment in order to establish an equitable cause of action for breach of confidence. On the basis of my conclusions at §123 above, this does not arise as a separate issue in a case of this nature.
247. If that is wrong, and specific detriment to the claimants does have to be shown, the evidence before me amply establishes such a detriment through the use by SJJ of Weiss's software, passwords, instructions for the use of the software, the ServiceLife database and customer information forwarded to him by (in particular) Mrs Whitfield, in order to compete with Weiss UK by seeking to secure service contracts from Weiss UK's customers.
248. As I have set out above, SJJ's business was from the outset based on diverting customers from Weiss UK using Weiss's customer information. Mr Jones accepted that he had done so, both in general terms and in relation to specific customers:

- i) Mr Jones accepted that information about an enquiry from a Weiss UK customer, Weatherford, which was forwarded to him by Mrs Whitfield in February 2016, was an “example of how [he had] taken business from Weiss ... by stealing and misusing their internal information”: see §§167–170 above.
  - ii) Mr Jones accepted that information about a similar enquiry from a Weiss UK customer, Bergstrom, which was forwarded to him by Mrs Whitfield in May 2016, was used by him “to go and see if [he] could get the business”, and was “another example of [Mr Jones] being able to curry business and favour from a customer of Weiss by using inside information taken from Weiss”.
  - iii) In yet another similar example, involving Weiss UK’s customer Gooch, Mr Jones accepted that this was an example of him “deliberately trying to divert business from Weiss to SJJ”: see §§167–174 and §194 above.
249. Mr Jones also accepted that he had used extracts from the ServiceLife database to contact customers of Weiss UK, many of which then became SJJ customers (see §236 above); that SJJ had used the ServiceLife database to compile and send direct marketing emails in 2017 and 2018 (see §238 above). I have also found that Mr Jones made use of Weiss’s password information to conduct SJJ’s business.
250. All of that establishes detriment to the claimants, irrespective of the precise quantum of loss and damage that can be established as having been caused by the defendants’ conduct.
251. The same cannot, however, be said of the second document in sample category 3, or the documents in categories 21 and 35, asserted against Mr Jones and SJJ, in relation to which there is no evidence that the documents were used in any way for the purposes of SJJ’s business.

### **Competition law**

252. Finally and for completeness regarding the issues in the case, I note that Mr Jones also raised an issue of competition law for the first time in his witness evidence. It was not pleaded, despite the fact that Mr Jones and SJJ had legal representation until March 2022. In any event the objection raised (concerning an offer of free renewal of a particular Weiss UK service contract) does not articulate how the conduct in question is said to have infringed competition law, or how that has any bearing on the issues raised by the claim. There is therefore no basis on which I can properly address it here and I say no more about it.

### **CONCLUSIONS**

253. My conclusions are that:

- i) All of the defendants breached their contractual or (as relevant) equitable obligations of confidentiality in the provision and/or use of Weiss software, passwords to Weiss software and/or instructions for use of the software.

- ii) Mr Jones, SJJ and Mrs Whitfield breached their contractual or (as relevant) equitable obligations of confidentiality, by taking and/or using the ServiceLife database for the purposes of SJJ's business.
- iii) The claims for breach of confidence in relation to sample categories 3, 21 and 35 (Mr Jones and SJJ), category 36 (Mrs Whitfield) and category 44 (Mr Oram) are established.
- iv) The breaches by Mr Davies, Mrs Whitfield and Mr Oram of their contractual obligations were induced or procured by Mr Jones and SJJ.
- v) Mr Davies infringed the claimants' copyright in the UpToDate3 and Contour software by downloading it in around September 2018.
- vi) Mr Jones and SJJ infringed the claimants' copyright in the Simpac, UpToDate 3 and Contour software by storing it on the SJJ Dropbox, and by copying the Contour software to a third party software developer.
- vii) The claims of copyright infringement in relation to the Simpac, UpToDate 3 and Contour software are not established as against Mrs Whitfield and Mr Oram.
- viii) Mr Jones and SJJ infringed the claimants' database rights by taking extracts of the ServiceLife database when he left Weiss and storing them on SJJ's systems, storing on SJJ's systems subsequent extracts from the database, and transferring extracts from the database into SJJ's own customer list.
- ix) Mrs Whitfield infringed the claimants' database rights by taking and providing to Mr Jones/SJJ extracts of the ServiceLife database.
- x) SJJ also infringed the claimants' database rights by sending direct marketing emails to email addresses extracted from the database. I do not make any findings as to whether that also constituted an infringement by Mr Jones or Mrs Whitfield.
- xi) I have not made any findings as to unlawful means conspiracy.
- xii) Insofar as (contrary to my primary conclusions) it is necessary to show detriment in relation to breach of equitable obligations of confidence, there is evidence of detriment to Weiss from the use by SJJ of Weiss's software, passwords, instructions for the use of software, ServiceLife database and customer information. That is not, however, the case for the second document in sample category 3, and the documents in sample categories 21 and 35.