Neutral Citation Number: [2026] EWHC 470 (Comm)

Case No: CL-2025-000564

IN THE HIGH COURT OF JUSTICE
KING'S BENCH DIVISION
BUSINESS AND PROPERTY COURTS OF ENGLAND AND WALES
COMMERCIAL COURT

Royal Courts of Justice, Rolls Building
Fetter Lane, London, EC4A 1NL

Date: 03/03/2026

Before :

THE HONOURABLE MR JUSTICE SAINI

- -

Between :

INFINNI INNOVATIONS S.A.	**Claimant**
- and -	
(1) OFMS LIMITED **(2) OMLAB DIGITAL LIMITED** **(3) PAVLO KHARMANSKYI** **(4) DANYL ROMANOV**	**Defendants**

- -
- -

Tony Singla KC and **Chintan Chandrachud** (instructed by **Cooley (UK) LLP**) for the **Claimant**
Arnold Ayoo and **Kendya Goodman** (instructed by **Eldwick Law**) for the **Defendants**

Hearing dates: 27-28 January 2026 and 25 February 2026

- -

Approved Judgment

This judgment was handed down remotely at 4pm on 3 March 2026 by circulation to the parties or their representatives by e-mail and by release to the National Archives.

.....

Mr Justice Saini:

This judgment is in 9 main parts as follows:

I. Overview

1. This is a claim for an interim injunction to restrain an alleged breach of confidence in a novel context. The underlying dispute is between the providers of two competing Customer Relations Management ("CRM") platforms in a specialised and niche market serving online content creators. The principal relevant content creators for the purposes of this claim are those who sell their digital content to their "fans" using the *OnlyFans* platform (see further **Section II** below for a more detailed description of the way *OnlyFans* works). These content providers are sometimes called *OnlyFans* "models" or "performers" in the papers before me.

2. An understanding of how the *OnlyFans* business works (and the relationship between models and their fans and the "chats" or messaging between them) is central to following what is in issue in this dispute and in understanding, in particular, the nature of alleged confidential information (or data) which is the subject of the claim for interim relief.

3. Content creators, particularly those models who are more successful and popular with their fans on *OnlyFans*, typically subscribe to CRM platforms such as those operated by the Claimant and Defendants. They also typically retain agencies to act on their behalf. These agencies may represent many content creators, and become customers of the CRMs in their own right in that capacity. In this case, these agencies are the relevant clients/potential clients of the companies in dispute.

4. The Claimant is a technology company incorporated in Spain. Its CRM platform is called Infloww, and it appears to be the market leader. The First Defendant is a company incorporated in England and Wales and the Second Defendant is a company incorporated in Cyprus. Their CRM platform is called *OnlyMonster*, and it appears to be a relatively new entrant. The Defendants' evidence is that they operate this platform "*together*". The Third Defendant ("Mr Kharmanskyi ") is a Ukrainian national resident in the UAE. He says that he is the co-founder of *OnlyMonster* and is responsible "*for the overall strategy of the business, marketing and product development*". The Fourth Defendant ("Mr Romanov") is an individual resident in Ukraine, and is its Head of Sales and Business Development, and also Head of Customer Success at *OnlyMonster*. His evidence is that he is "*responsible for maintaining direct communication with both prospective and existing clients"*.

5. The Claimant's claim is based on an allegation that the Defendants are responsible for what it calls "*cyber-attacks*" in the form of infiltration, and "*data-scraping*" of the Claimant's servers. The Claimant says these servers held data confidential to it, and the attacks enabled mass extraction of two broad categories of confidential data which relate to its *OnlyFans* creators: (1) data provided by content creators and their fans which was compiled by Infloww- that is, fan notes, and scripts; and (2) data generated by the Claimant based on the activities of content creators and their customers - that is, analytics and reporting data. For ease of reference, I will define the first category as "Fan Notes and Scripts", and the second category as "Generated Data". I will provide fuller descriptions below.

6. The purpose of the alleged unlawful infiltration and data scraping of its servers is said by the Claimant to have been to lure away the agency clients of Infloww and to make them subscribers of the Defendants' competing CRM platform, *OnlyMonster*. It seeks interim relief restraining future infiltration and prohibiting use of the Fan Notes and Scripts and Generated Data.

7. For their part, the Defendants admit taking certain Fan Notes and Scripts (but not the Generated Data) from the Claimant's servers, and say that this was done lawfully. They say that the former agency clients of the Claimant authorised them to "migrate" such data as they have taken. The Defendants put in issue the ownership and confidentiality of the Fan Notes and Scripts, as data which the Claimant can protect.

8. It is the nature of the data which is said to have been misappropriated which gives rise to the novelty of this claim as a breach of confidence claim. In particular, as I have recorded, there is an issue as to whether Fan Notes and Scripts are confidential to the Claimant or in fact the content creators/agents. The position as regards the confidentiality of the Generated Data is more straightforward.

9. On 9 December 2025, following a without notice hearing ("the WN Hearing"), I granted the Claimant an interim injunction ("the original injunction", or "Order"), restraining the Defendants from accessing the Claimant's servers and restraining use of certain identified data (at that time, only the Fan Notes and Scripts). I also directed that the Defendants identify within 10 days of service of the Order, in the form of an affidavit, a number of matters including all the data they had accessed and the uses made of it ("the Affidavit Obligation"). I gave permission to the Claimant to serve the Claim Form and the Particulars of Claim on the Second, Third and Fourth Defendants out of the jurisdiction. I directed a Return Day for 18 December 2025 ("the December Hearing").

10. At the December Hearing, the Defendants applied to set aside the original injunction on three grounds: (i) lack of a "serious issue to be tried"; (ii) the balance of convenience, and (iii) an alleged breach by the Claimant of the duty of "fair presentation" at the WN Hearing. Following submissions at that hearing from Simon Colton KC and Samuel Grimley (then acting for the Defendants and instructed by Enyo Law) and Mr Singla KC for the Claimant (and subject to suspending compliance with the Affidavit Obligation) I continued the original injunction until a further hearing. I declined to hear substantive arguments on the discharge/continuation application on that day because the Defendants had served substantial evidence, and a detailed Skeleton Argument, only the day before the December Hearing. As I indicated briefly in the judgment I gave at that time, fairness demanded that the Claimant have the opportunity to respond to the Defendants' evidence (and legal arguments), including serious allegations of breach of the duty of fair

presentation. I made directions for exchange of evidence and a further hearing, with a two day time estimate.

11. That further hearing (the effective Return Day) was argued between 27-28 January 2026 ("the January Hearing"). The position taken by the Defendants before me at that hearing was not exactly the same as that adopted by Mr Colton KC at the December Hearing. The Solicitor and Counsel teams for the Defendants had changed. They continued to argue that there was a breach of the duty of fair presentation at the WN Hearing and that the original injunction should be discharged on that basis. However, Arnold Ayoo and Kendya Goodman, Counsel now instructed for the Defendants, conceded (for limited purposes only) that there was a "serious issue to be tried", for American Cyanamid v Ethicon Ltd [1975] AC 396 (HL) ("American Cyanamid") purposes. They also no longer advanced the submission that I could determine at this early stage that the conduct of which the Defendants are accused (the extraction and use of data) was justified and lawful because the data belonged to the Claimant's customers (that is, the agencies or the content creators) and those customers authorised its extraction. They accepted there was a serious issue to be tried in this regard but no more. They also no longer took any point about the need for fortification of the cross-undertaking in damages.

12. The Defendants offered an undertaking reflecting paragraph 1(a) of the original injunction (restraint of further future accessing of the Claimant's servers and systems), but argued the remainder be discharged. Mr Singla KC argued that the injunction should be continued until trial and highlighted that the Claimant had discovered even more extensive scraping which included a wholly new category of appropriated data (the Generated Data).

13. However, there was a development at the January Hearing which required further evidence and submissions. I raised during the submissions the point that (at least as it appeared to me) the parties were not in fact agreed as to the scope of the original injunction. In short, was the effect of the original injunction to restrain the Defendants from continuing and facilitating the access of the agencies (who had moved over to *OnlyMonster*) to the extracted data? The Defendants appeared to say *no* while the Claimant appeared to say *yes*.

14. On the morning of the second day of the hearing, 28 January 2026, and in order to crystallise the nature of this dispute, Mr Singla KC and his junior Mr Chandrachud produced an amended draft order in which wider and narrower versions of the injunction were presented. These were described as Option 1 and Option 2, respectively (see [106] below for the full text). Arguments were concluded on all other issues but I made directions for further evidence and submissions on this Option 1/2 issue given the Defendants appear not to have considered denial of agency access was in issue. I decided that Option 2 (that is access be permitted to agencies) be the regime in place pending a further hearing which took place on 25 February 2026.

15. The parties have exchanged a number of rounds of evidence, including recent evidence in relation to the effects of Option 1. I cannot determine matters which are the subject of factual dispute at this hearing, and what I set out below in my narrative in **Section III** are no more than provisional conclusions formed on the basis of the evidence and arguments at this early stage in the claim.

16. In many respects, however, the core facts asserted by the Claimant concerning what was accessed and the means by which the Defendants apparently achieved this, were not the subject of challenge in evidence. I would have expected more to be said on that matter by the Defendants. At the time I suspended compliance with the Affidavit Obligation at the December Hearing, I indicated to Mr Colton KC that it would assist the Judge at the Return Day if his clients were as frank as possible as to how the (apparently admitted) extraction of data from the Claimant's servers took place; and that absent such disclosure the Court might draw inferences against the Defendants. At the January Hearing they did not explain their actions (as regards how in technical terms they entered the Claimant's systems) and were content to accept what the Claimant says about mechanisms of entry (and the data taken). I was surprised by the Defendants' continuing lack of candour in this regard.

17. The Claimant commissioned Kroll to undertake investigative work in this regard and they have provided a number of reports (on the basis of which the Particulars of Claim have been amended on two occasions as the nature of the entry into servers and scraping have become clearer). Mr Singla KC was right to submit that the Claimant's detailed investigations and repeated amendments would have been unnecessary had the Defendants come clean about how they got into the Claimant's systems and what precisely they had taken (on the apparent instructions of agencies).

18. In broad terms, there are three main issues for determination: (1) was there a breach of the duty of fair presentation? (2) should the injunction continue at all, and if so in what form? and (3) should I direct compliance with the Affidavit Obligation? As regard issue I indicated at the end of the January Hearing that I had concluded there was not a breach of the duty of fair presentation and I would give my reasons in due course. I provide those reasons in **Section IV** below.

19. As regards issue (2), continuation of the injunction, it was common ground that I must proceed on the basis that at a Return Date, the issue is whether an injunction is appropriate afresh in the light of such further evidence as the parties have submitted: White Book 2025 (vol 1), ¶25.1.27. The burden lies on the Claimant, applying the usual principles in American Cyanamid**,** to show that an injunction, in the terms it seeks, should be continued/granted. In particular, the fact that an interim without notice order was made does not give rise to any presumptions in favour of a claimant's entitlement to hold on to an injunction at the Return Day. The Court starts with a "clean sheet" because an effective Return Day is the first time that both parties will have had their say.

20. I should record that following the December Hearing, the Defendants acknowledged service and the Second-Fourth Defendants have indicated that they do not intend to challenge the jurisdiction of the English Court.

II. The *OnlyFans* business model

21. In order to understand the nature of the dispute, and in particular, the alleged breach of confidence claim and arguments made about Options 1 and 2, it is necessary to provide a brief explanation of how the *OnlyFans* business model works, and the data generated within that platform. *OnlyFans* is a subscription-based social media platform where creators share exclusive content (photos, videos, live streams), and use built-in messaging tools to have conversations with "fans". While used by some others in the entertainment world, *OnlyFans* is predominantly known for adult content, and serves as a direct income

source for creators in the modern so-called "creator economy". Creators/models charge fans for their interaction/services in a number of different ways and *OnlyFans* generally takes 20% of the charges.

22. Creators set their own subscription price for fans, usually between about US$5.00 and US$50.00 per month. For pay-per-view content, creators charge a one-off fee for access to particular content and tips are sent by fans in amounts of their choosing. Creators are responsible for generating income on the platform by producing content that attracts and retains subscribers. *OnlyFans* does not itself create content. One can gain an idea of the scale of the enterprise from some figures in the evidence before me. In its most recent (2024) accounts, *OnlyFans* reported gross payments from fans of approximately US$ 7.22 billion (across hundreds of millions of registered users and several million creators worldwide) and pre-tax profits of US$ 683.6 million. Earnings for individual creators vary, but an article published by the Claimant in the evidence before me identifies a number of "middle ground" content creators who earn around US$ 3,000.00-5,000.00 per month, and higher earners making in the region of US$ 20,000.00 per month.

23. In order to keep fans engaged, successful content creators maintain personalised dialogues ("chats") with each fan. Messaging lies at the heart of the *OnlyFans* model and the evidence shows that the overwhelming majority of creator revenue is generated through this "direct messaging" and chats between fans and content creators**.** As I describe below, the messaging is not in fact (in the case of successful creators) undertaken by them but by "chatters" employed by agencies.

24. Agents are responsible for day-to-day activities such as communicating with fans, managing paid content, monitoring performance, and maintaining account security. Such agencies typically manage a large number of creator accounts at the same time, often into the hundreds. *OnlyFans* is however designed for individual creators, not for agencies. A person can only be logged into one *OnlyFans* account at a time, and an *OnlyFans* account is limited to only one creator. However, CRM platforms, such as *OnlyMonster* and Infloww, offer a function where multiple creator accounts can be logged in to *OnlyFans* at the same time, through the CRM interface. The agencies can consequently manage tens, even hundreds, of creators who in turn have thousands of fans.

25. Agencies have members of staff who work as "chatters". These are people employed by the agencies to interact with thousands of fans on behalf of the creators, in sometimes an intimate and personal way. The fan believes that these are one-to-one chats, and they are having a personal dialogue with the creator. Fans may well believe that they are chatting to a model in real time but in fact an agency-employed chatter will be interacting with the fan on the pretence that they are the model. That explains why having the right "script" as a badge of apparent authenticity and personal relationship with the fan is crucial. These chats take place through the CRMs because these platforms allow the agencies to be logged into multiple *OnlyFans* creator accounts at the same time, which they can then easily manage from an operational perspective. Therefore, whilst the fan is interacting and chatting on the *OnlyFans* account, the creators (through the chatters employed by the agency) are interacting on the CRM platforms.

Fan Notes and Scripts

26. I turn to how Fan Notes and Scripts are created and used. I will use some examples from the evidence of the Claimant and the Defendants, in order to explain what this data looks like.

27. **Fan Notes** are the details (essentially raw information) that agencies collect on fan interactions from the chats on *OnlyFans.* To take an example in the evidence before me of a screenshot from Infloww which shows a (pixellated) content creator/model and a discussion with a fan called 'Brian'. In the middle of the screen is the *OnlyFans* dialogue between the content creator and Brian. To the right-hand side, in the 'Fan notes' section, is information which the agency has recorded and logged about Brian, in the course of the dialogue – he is from the Bay Area, California; 40 years old; single; lives with parents; etc. Another example of Fan Notes record that 'Bruno' is a veteran of the Navy SEALS, a jiu jitsu black belt, and that he is from Brazil with Italian parents. Because fan relationships are ongoing, these entries necessarily evolve over time.

28. Fan Notes are added or refined as new details emerge and as circumstances change, for example, there may be shifts in a fan's interests, his upcoming special dates (birthdays or when he gets paid), or personal events in his life. A useful demo example of an amendment to a Fan Note about a person ("David") is in the evidence: a change has been made to update David's salary to $2,000 USD per month, that he tips between $50-$100 and he get paid wages between 15th-17th. Fan Notes of this type are intended to enable a chatter to extract maximum financial benefits when they interact with David.

29. **Scripts** are the templates developed by the agencies to facilitate automated interactions with the fans by their chatters (under the pretence that they are content creators/models). Infloww calls these "scripts" but the same data is described on *OnlyMonster* as "Message Templates". Scripts are built into the messaging interface used by chatters and can be searched for and inserted during live conversations, enabling consistent and efficient responses which may be adapted to reflect the circumstances of an individual interaction. I will provide some examples from the evidence before me from an *OnlyMonster* demo account. In this example "Ryan" is the fan. The script says: "*Hey Ryan, I saw you liked my gym pics yesterday. Want the full video tonight? If you say yes, I'll send for £25".* This template is accompanied with Fan Notes (to assist the chatter interacting with Ryan) with the notes acting as a form of prompt. So the chatter is told: *"Use it only when: mentions gym pics".* Another example script (where the fan is "Brian") says : *"Hey Brian, I saw you liked my bath video yesterday. want the full video tonight?...",* and the prompt in the Fan Notes says: *"Use it only when: replied 'I'm okay' and hasn't bought in 7 days.".*

30. On the *OnlyMonster* platform, if an agency edits a script, any previous entries are deleted, and an entirely different text is produced. I will return to this issue below.

Fan interactions

31. I turn to the agencies in more detail and will use one of the agencies that went over to the Defendants (Typa) whose evidence is before me as an example. Typa manages 50 creators and each one has between 2,000 and 300,000 fans. So, it manages the interactions the creators are having with over 1 million fans on *OnlyFans*. Typa employs a number of chatters as well as copywriters. It explains that Scripts are the mechanism that enables Typa to maintain consistency in fan engagement across different staff members who work in shifts from different time zones. To provide this consistent service

at scale, they rely on CRM tools which allow for Scripts to be subject to layered controls and quality assurance. The COO of Typa (Mr O'Neil), has ultimate control over Scripts and staff including copywriters who produce around three new Scripts per creator per week (administrative staff amend existing Scripts). The amendments to existing Scripts and the new Scripts are informed by new and existing details in the Fan Notes which are populated during chats and Typa uses a team of five chatters working in shifts to provide 24/7 coverage, supervised by a quality control manager. The role of chatters is limited to using the approved Script templates, and, where permitted, completing designated blank spaces with fan-specific details collected in conversations and recorded through the CRM platform. This structure is important because it allows Typa to maintain consistent engagement with the substantial fan base.

The CRMs

32. Although they have differences, both the Claimant and the Defendants operate a business-to-business software-as-a-service ("SaaS") model. In interacting with fans and in other ways I have described above, each *OnlyFans* creator/agency generates significant volumes of data in the course of their businesses. Once they subscribe to a CRM platform, that data is uploaded to it, and operational tools are provided for the creators. In short, the platforms are designed to help agencies and high-volume creators manage large numbers of fan interactions, organise workflows, and optimise revenue. Each of Infloww and *OnlyMonster* make money by charging a recurring subscription fee for access to its software, which includes these tools for content management, fan engagement, analytics, and workflow automation.

III. Infloww and its features

33. Before I turn to the alleged cyber-attacks which form the basis of this claim, I need to describe the way Infloww works in more detail and some of what I describe relies on my description above of *OnlyFans*. What I summarise in this section of my judgment was not disputed by the Defendants.

34. Infloww has three key features that are relevant to these proceedings and the sub-categories of data it seeks to protect:

    34.1 The **fan insights panel**: this displays fan profile data (information about individuals who have subscribed to receive content from a particular online creator). It visualises basic information for each fan, such as their nickname, country and time zone, birthday, source platform, and subscription and purchase data. This data is imported by Infloww from *OnlyFans* to which the creator uploads their material. The fan insights panel includes a fan notes feature, which I have outlined above. It enables Infloww users to input personalised notes or information for each fan.

    34.2 The **communication panel/script feature**: Infloww enables users to communicate directly with fans through the communication panel. To assist content creators (or agencies on their behalf) to communicate directly with fans, the Infloww platform includes a script feature. Users can create a script of preprogrammed communications to communicate with fans. Those preprogrammed messages can be selected by chatters and dropped into the communication panel with the fan.

34.3 The **reports/analytics feature**: Infloww provides users with the ability to generate bespoke reports to measure the effectiveness of marketing activities, including: (i) creator revenue summaries, (ii) employee reports, (iii) fan introduction reports, and (iv) script analytic reports. They enable users to evaluate the performance of their employees (these being the "chatters" communicating with fans as if they were the content creators) and the effectiveness of their marketing strategies.

35. These 3 separate categories of data reflect the Fan Notes, Scripts and Generated Data as defined above. I will refer to them together, as in the pleadings, as "the Extracted Data". It is the Claimant's case that they were the subject of the infiltration and scraping attack. The Defendants quarrel with this description but admit taking the Fan Notes and Scripts (but not the Generated Data).

36. The Infloww platform uses cloud-based architecture. Users of Infloww interact with the platform through the "Client Portal", which they access via a web browser or desktop application. As I understand the position, the Client Portal pulls data from Infinni's servers, which are hosted by third party providers in Germany. Data requests made of the servers pass through a security gateway operated by Cloudflare, a cybersecurity service provider. Fan insights and script data stored on Infinni's servers is encrypted and access is controlled by the use of usernames and passwords. Through Cloudflare, Infinni also deploys a number of other security protocols and protection mechanisms to identify and block unauthorised access or malicious behaviour.

37. It is important to underline that the Client Portal is the only means of access to Infloww made available to users (content creators/agents) (i.e. the "front end" of the system). The Client Portal does not allow users to export or migrate the data and analytics visible to them within the portal *en masse*. In theory, users could attempt to manually copy the data and analytics available to them on Infloww (such as by copying and pasting text or adopting some other analogue solution, such as taking thousands of screenshots). However, as set out in the Defendants' own evidence, this is not a practical solution given the large volume of Fan Notes and Scripts and the difficulty of preserving the link between a Fan Note or Script and the relevant fan and content creator once it was removed from Infloww.

38. Infloww users are not given access to the "back end" of the system. The "back end" of the system contains Infinni's Application Programming Interface ("API"). The API includes a number of "endpoints" (digital locations where the API receives requests for data from Infinni's server). When a user uses the Client Portal, the Client Portal "calls up" information from Infinni's server using those API endpoints. Infloww users do not have access to the API or the API endpoints.

Concessions

39. Mr Ayoo for the Defendants conceded that there was a serious issue to be tried for American Cyanamid purposes. This was in circumstances where his clients accepted they entered the Infloww system and copied large amounts of data (the Fan Notes and Scripts) but they have not been willing to explain how they did this.

40. However, I understand that for present purposes, and as I clarified with Mr Ayoo during his submissions, the Defendants accept that I should proceed on the basis that: (i) the facts posited by the Claimant as to how they entered the systems and copied the Extracted Data (save as to the Generated Data) are correct; and (ii) these actions were unlawful and

give rise to arguable claims of breach of confidence or parallel claims under Spanish or German law.

41. In particular, I understood that the Defendants no longer advance one of the principal points they relied on at the December Hearing. In their Skeleton Argument for that hearing, it was argued at [28] that "...the Extracted Data which forms the basis of the claims is ...not even arguably Infinni's confidential information: it is the information of Infinni's clients, its users. That much is clear from Infinni's Terms of Service". That point has been abandoned for now at least.

42. Although these points are conceded for the purposes of the "serious issue to be tried" test, I need to set out, in at least summary form, what the facts are because they remain relevant to my determination of the contested issues. Mr Singla KC argued that the serious nature of the Defendants' unlawful conduct is relevant to the balance of convenience. Mr Ayoo relied on the history in support of his arguments that the Claimant delayed in taking action.

IV. The Facts

Scraping

43. I turn first to how it is said (without contradiction) the Defendants got into the Infloww system and obtained the Extracted Data from its servers. In total, the Defendants have filed four rounds of evidence: on 17 December 2025, 5 January 2026, 20 January 2026, and 9 February 2026. Unfortunately, the Defendants did not respond to my suggestion, and gentle encouragement at the December Hearing, that at the next hearing they provide a frank explanation of *how* they obtained the data which they appeared to accept they had taken (in large quantities) from the Claimant's servers without its consent. They have been curiously silent in relation to how they got into, and as to what exactly they took from the Claimant's servers.

44. Between December 2024 and November 2025, the Claimant was the victim of a series of data scraping cyberattacks. The Defendants have accepted that they were responsible for these actions, but they disagree with that characterisation.

45. Given some of the points made by the Defendants as to the balance of convenience and implications of delay, I need to begin my narrative with events in early 2025. On 17 January 2025, the Claimant learned that it had been the victim of a data scraping cyberattack targeting its fan insights data. As I understand it, a data scraping attack occurs when an attacker uses automated tools (such as a computer script) to extract large amounts of information from a website without the website owner's permission. The automated tool is directed by the attacker to 'crawl' through data, which it does by methodically viewing every link, page, and piece of data on the website. It then 'scrapes', i.e. compiles and copies, this data.

46. As to the mechanism, the Fourth Defendant gained access to the Infloww Client Portal by being added as a user to several existing agency accounts, thus obtaining a digital 'access token'. Having obtained this token, he then cracked Infinni's security by "reverse-engineering" its encryption. Once the system had been cracked, he deployed an automated crawler program to extract data from the Infinni servers. The crawler program was designed to evade detection by Infinni's security systems.

The Honeytrap: the admitted "cracking" of Infloww

47. In order to obtain evidence that the Defendants were responsible for the attack, the Claimant set a trap (referred to in the evidence as "the Honeytrap"). In summary, Infinni created a simulated agency account on the Infloww platform under the name 'Unheard Agency' and, posing as a potential customer of *OnlyMonster*, contacted the Third Defendant (Mr. Kharmanskyi) via Telegram (a messaging application). In the guise of 'Unheard Agency', the Claimant told him that it was thinking about switching its business from Infloww to *OnlyMonster* but was concerned about losing access to fan data stored on Infloww. In the course of that conversation, Mr. Kharmanskyi said "*...yes, we cracked inflow and can migrate fan notes once you decide to switch*", *and* "*...*Infloww *is a box solution, they don't allow you to scrape anything from them, they also tell you that for some reason and technical issues they cannot export fan notes etc. So we need the way to migrate notes. Sometimes it can be thousands of them which is obviously impossible to get. We found the way.*"

48. Mr. Kharmanskyi then put 'Unheard Agency' in contact with the Fourth Defendant ("Mr Romanov"). In May 2025, he deployed a crawler program and began scraping the 'fan insights' data associated with the simulated account created by Infinni, thus confirming what Mr. Kharmanskyi had said – i.e. that they had "cracked" Infloww and found a way to "scrape" the fan insights data from its servers. It is significant that the technical characteristics of the crawler program used by Mr Romanov to extract this data corresponded to those of the crawler program used in the earlier scraping attacks, thus confirming with a high degree of certainty that Mr Romanov had carried out the earlier attacks too. Indeed, that is not now disputed.

49. The Claimant did not keep detailed logs for the entirety of this period and is therefore unable to say how much data was 'scraped' from its servers in total, or how many separate scraping attacks were carried out. After May 2025, Infinni took steps to upgrade its security systems so as to prevent any further scraping attacks and believed that this had brought an end to the attacks.

50. Separately from the scraping attacks, the Claimant was the victim of a further cyberattack between 27 August and 2 September 2025 which targeted (and successfully extracted) some of its internal business data, including sensitive financial and billing records. This attack (the "Finance Attack") was different from the previous Scraping Attacks in that it did not target the Infloww fan insights data. The methodology was similar to, but not precisely the same as, that of the Scraping Attacks.

51. After learning of the Finance Attack, the Claimant filed proceedings in the United States against 'John Doe' defendants, i.e. persons unknown and I was taken by Mr Ayoo to parts of the US Complaint. The US proceedings enabled the Claimant to obtain subpoenas against entities in the US (including e.g. email providers) who might have relevant information about the Finance Attack. At the time of filing, the Claimant's working theory was that the Finance Attack and the Scraping Attacks were linked. However, the effect of the US proceedings was that another individual came forward purporting to claim sole responsibility for the Finance Attack and claiming to have had no involvement in the initial Scraping Attacks. Before me at the WN Hearing, Mr Singla KC made it clear that there was no suggestion that the Defendants were responsible for the Finance Attack. Indeed, since discovering that (i) the Scraping Attacks have in fact been continuing since July 2025 and (ii) they may not be linked to the Finance Attack, I

understand the Claimant made an application for voluntary dismissal of the US proceedings, which was granted.

52. Matters then went quiet until 14 November 2025 when the Claimant was alerted to a new potential intrusion on its systems. Having investigated further, it learned on 18 November 2025 that – contrary to its previous belief – further Scraping Attacks targeting its fan insights data had occurred between July and November 2025. The technical analysis evidence points strongly towards a conclusion that these further attacks were carried out by the same persons and using substantially the same methodology as the Scraping Attacks which took place between December 2024 and May 2025. I proceed on the basis that they were perpetrated by the Defendants. Indeed, when one looks to the evidence of agencies who have "migrated" to *OnlyMonster*, the Defendants' own case is that they moved over between January and December 2025.

53. On 26 November 2025, the Claimant learned that yet further Scraping Attacks had been carried out on 21, 22, 23 and 24 November 2025, again targeting its fan insights data but also (on 24 November 2025) script data entries. Again, technical analysis confirms with a high degree of certainty that these were carried out by the same persons and using substantially the same methodology as the earlier Scraping Attacks. On 4 December 2025, the Claimant detected a further attack which shared the same machine ID as the 24 November attacks.

54. The Claimant applied for the injunction on 5 December 2025 and I made the Order on 9 December 2025 at the WN Hearing.

Kroll

55. Following the December and January Hearings, the Claimant continued its investigations into the Scraping Attacks to gain a better understanding of (i) how the attacks were conducted, and (ii) what data was obtained as a result of the attacks. Those investigations have most recently involved Kroll, the cybersecurity firm, which has confirmed the Claimant's characterisation of *OnlyMonster's* scraping activities. So, Kroll state as follows:

> "Kroll's assessment of the available evidence led to the classification of all unauthorised activities as a "web scraping" attack. In this context, the unauthorised actor(s) systematically collected data from HTTP services by simulating the behaviour of a legitimate client."

(It is not in issue that "client" here refers to a client in computing terms (a device or software that requests data from a server) – not a customer of the Claimant).

56. Kroll also discovered that the attack had targeted not only Fan Notes and Scripts but also the Generated Data (and the Claimant has amended its pleading to reflect this). Kroll also updated this report on 16 February 2026 with more recent evidence of the scope of the Scraping Attack.

The Extracted Data

57. The Defendants accept that there are 26 agencies whose data was extracted (or in their words, "migrated") from Infloww. On the evidence before me, the attacks appear to have been extensive. According to the updated Kroll report: between 7 May 2025 and 4 December 2025, the Defendants called and extracted data from Infinni's API on 293,138 occasions. They targeted 68 different API endpoints. Of those 68 API endpoints, 32 call data that is generated by Infinni. Of those 32 API endpoints, 11 call data which Infinni considers to be of particular commercial significance and value to Infinni's business. That commercially significant Infinni-generated data includes data such as "total spending amount", "tip amount", "number of paid messages", "message spending amount", "employee performance", and "highest payment time". This data is within the defined Generated Data.

58. I note that the data extracted by the Defendants includes data entries relevant to each of Infloww's three key features referred to above. Specifically, on the basis of the updated Kroll Report, the Defendants extracted the following data during the Scraping Attacks (adopting the definitions I have used earlier):

    58.1 **Fan Data**: 147,783 individual fan profiles between 22 April and 7 May 2025 and 271,395 individual fan profiles between 1 July 2025 and 4 December 2025;

    58.2 **Scripts**: 12,735 script data entries between 1 July 2025 and 4 December 2025; and

    58.3 **Generated Data**: 306 reporting data (Generated Data) entries between 1 July 2025 and 4 December 2025.

V. Fair Presentation

59. This was the first point taken by Mr Ayoo in his excellent and well-structured submissions at the January Hearing. He emphasised that this was the primary basis for the application to discharge and his oral submissions were accordingly principally devoted to this matter. Mr Ayoo relied on three particular alleged failures in the Claimant's duty of fair presentation: (i) the failure fairly to address any question of potential liability under Spanish or German law; (ii) the failure to show the court Infinni's Terms of Service; and (iii) the failure to draw to the court's attention the impact that the Injunction would have on third parties. I will address each in turn below but start by noting that there was no dispute about the applicable principles. The duty of full and frank disclosure "*requires an applicant to make the court aware of the issues likely to arise and the possible difficulties in the claim, but need not extend to a detailed analysis of every possible point which may arise*": Tugushev v Orlov [2019] EWHC 2031 (Comm) at [7]. Moreover, "*a due sense of proportion must be kept. Sensible limits have to be drawn, particularly in more complex and heavy commercial cases where the opportunity to raise arguments about non-disclosure will be all the greater. The question is not whether the evidence in support could have been improved (or one to be approached with the benefit of hindsight). The primary question is whether in all the circumstances its effect was such as to mislead the court in any material respect*": Tugushev at [7(vi)].

Foreign law: Spanish and German law

60. This point was relied on in support of the submission that there was no evidence of a serious issue to be tried under Spanish or German law. It is said that this was a matter that should have been drawn to the Court's attention at the first hearing, although the law

relied on for the main claim in breach of confidence was English law. Before I consider this submission, it is worth underlining that at the hearing before me, it was not suggested by the Defendants that, if Spanish or German law is applicable, there is no serious issue to be tried, or that some form of defence was arguably available under those systems of law which should have been drawn to the Court's attention. As I observed during Mr Ayoo's submissions this foreign law disclosure complaint appears wholly theoretical. I turn however to the substance of the arguments.

61. It was argued that under Article 4 of the Retained Rome II Regulation, the law applicable to Infinni's claim is the law of the country in which the damage occurs. Indeed, Mr Ayoo pointed to Infinni's own evidence which said it is incorporated in Spain and the servers from which the relevant data was extracted are located in Germany; and that Spain or Germany therefore might be said to be the places in which the relevant damage was suffered. Mr Ayoo argued that, despite this, there was no evidence before the court at the first hearing as to what provisions of either Spanish law or German law might apply. He underlined that Infinni's duty of fair presentation on a without notice hearing required it to investigate and address any likely defences, and an obvious defence would be that English law does not apply, and that German or Spanish law applies. He said there was no evidence nor submission identifying any principle of foreign law, or foreign legislative provision, upon which Infinni could rely. Nor was there any attempt made to explain how such principle or provision would be applied: he invited me to compare section 1.3(f) of the Commercial Court Guide.

62. I do not accept the submission that there was any breach in relation to foreign law issues. At the first hearing, Infinni brought to the Court's attention the possibility that German or Spanish law might govern its claim. This was expressly addressed in its evidence which stated that advice about claims under those laws had been taken and arguable claims existed thereunder. It is correct that the Claimant did not set out the relevant provisions of German law or Spanish law, but in my judgment, it was not obliged to do so. At that stage, the Claimant was not itself relying on German or Spanish law but had pleaded its case, as it was entitled to do by reference to English law; and foreign law may never have been relevant if it had not been raised by the Defendants.

63. As to the Defendants' reliance on the requirements of section 1.3(f) of the Commercial Court Guide, I do not consider it to be relevant. That provision concerns the pleading of foreign law. Compliance with the duty of fair presentation did not require Infinni (which was itself relying on English law) to address foreign law in the same level of detail as a party pleading foreign law would have to do.

64. Ultimately, it is significant that the Defendants do not (and could not) complain that Infinni's evidence misled the Court in any material respect. The most they can say is that Infinni could have improved or supplemented its evidence by identifying for the Court what provisions of either Spanish law or German law might apply. And this submission is made in circumstances where Mr Ayoo does not point to any feature of those foreign laws which is of any relevance (in particular, some aspect of those laws which might give some form of defence to the Defendants).

65. There was no breach of the duty of fair presentation in failing to supplement the evidence on foreign law. In any event, Infinni has now provided additional evidence on Spanish and German law and that evidence is unchallenged. The evidence of good claims available under Spanish and German law presented at the first hearing has been shown

to be correct, and was very well founded. The new evidence shows (unsurprisingly) that substantial claims under those laws exist to cover the form of infiltration of servers and scraping, which is the basis of this claim.

66. So, in the facts accepted by the Defendants as established for the purposes of this hearing, I consider there are properly arguable claims under Spanish law as follows: (1) under the Ley de Propiedad Intelectual ("LPI"), the Spanish law implementing the EU Database Directive which gives database makers the right to prevent extraction or reuse of substantial parts of their database without consent; (2) under Article 196 of the LPI which prohibits unauthorized circumvention of technological measures protecting content; (3) under the Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (the "LSE") which protects confidential business information with commercial value if reasonable protection measures are in place.

67. As to German law, there are arguable claims as follows: (1) infringement of section 823(1) and 823 (2) of the German Civil Code for tortious conduct; (2) violation of the sui generis database right infringement (which appears to mirror that described under Spanish law- being derived from the same EU Database Directive); (3) the German law establishing database rights is section 87 of the German Copyright Act; and (4) under the German Act against Unfair Competition, which provides companies may pursue a competitor's violation against wrongful behaviour in competition.

68. It was not suggested by Mr Ayoo that, if Spanish or German law applied, those systems prohibited the grant of interim or indeed final injunctive relief to prevent the claimed wrongdoing of the Defendants in this case. So, this case is not like OJSC TNK-BP v Lazurenko [2012] EWHC 2781 (Ch) at [20] where Russian law as the *lex causae* precluded such relief in confidential information claims.

The Terms of Service

69. Mr Ayoo's second complaint was the failure to place before the court the Infinni Terms of Service ("the Terms"). He underlined that Infinni's claim at the time of the first hearing was solely for breach of confidence, and conspiracy claims where the sole pleaded unlawfulness was such breach of confidence. It is common ground that a claimant must establish: (1) that the information has the necessary quality of confidence; (2) that it was imparted in circumstances importing an obligation of confidence; and (3) that there has been unauthorised use or disclosure of the information to the claimant's detriment. See [] below.

70. Mr Ayoo argued that Infinni, therefore, had to put fairly before the court the question whether the Fan Insights Data and Script Data were in fact Infinni's confidential information. But, he argued that this was information generated by Infinni's users, and Infinni's relationship with its users is governed by its Terms of Service ("the Terms"). He took me to the Terms. They are subject to Spanish law (Section 25), but set out in the English language. He said that the Court was not informed that the Terms explicitly address the status and confidentiality of user data. I will not set out the Terms but will provide a hyperlink here: Terms. It was argued that their effect is that the Fan Insights Data and the Script Data are not Infinni's confidential information, and Infinni has no right to bring any claim in respect of such information. I found this is a surprising submission in circumstances where it is not (now) suggested there is not a serious issue to be tried in relation to the breach of confidence claim. Mr Ayoo's skeleton says in terms

at [5] that the Defendants accept "...that at this hearing the court should proceed on the basis that there is now a serious issue to be tried on Infinni's pleaded case" (my emphasis). But that pleaded case relies *only* on English law. If Mr Ayoo's submission about the effect of the Terms is correct, this would be a knock-out blow under English law breach of confidence claims as regards at least the Fan Notes and Scripts parts of the Extracted Data.

71. Putting these points to one side, I do not consider there to be any substance in this fair presentation complaint. I consider the relevant terms of service are in fact the Infloww terms which I consider at [] below. It is correct that the Claimant did not exhibit these terms to the evidence adduced in support of the without notice application. That said, at the hearing Mr Singla KC did bring the Infloww Terms of Service to the attention of the Court at the hearing in the context of jurisdiction (since the Infloww Terms of Service included an arbitration clause). The point made was that Infinni's claims did not fall within the scope of the arbitration clause. Infinni offered to provide a further statement about this point, but the Court did not consider it necessary. In my judgment, it was reasonable for the Claimant to take that approach at the without notice hearing. Its case is (and was) that the Defendants conducted unauthorised and covert cyberattacks against them. The Defendants were not customers or users of the Infloww platform and did not agree to the Infloww Terms of Service. There was accordingly no privity of contract between Infinni and the Defendants. That is the reason why the Claimant submitted at the WN Hearing that the arbitration clause was not relevant – from the Claimant's perspective, the Defendants had not signed up to it. Moreover, at the time that the without notice application was brought, I accept on the evidence that the Claimant could not have reasonably anticipated that the Defendants' defence would be that agencies had consented to their data being "migrated" from Infloww to *OnlyMonster*. Rather, the more obvious inference based on the facts that were available at the time was that Infinni's data was being systematically targeted by its competitor, who could use that data to poach or lure the Claimant's customers.

Impact on third parties

72. Mr Ayoo's final complaint was that the Claimant failed to draw to the Court's attention what he described as the "significant deleterious impact" of the Injunction on third parties. He underlined that the Claimant's solicitor has accepted that it knew about the earnings structure of content creators and agencies and argued that this was a material matter. In particular, where (as he argued was the case here) an injunction will have an unwarranted effect on the commercial interests of third parties, that may be grounds for refusing an injunction. Mr Ayoo pointed to the Claimant's solicitor's response to this criticism (which is to the effect that it did not know whether any agencies had indeed transferred their business to *OnlyMonster*). But, he argued, the premise for the Injunction was precisely the concern that agencies had transferred their business.

73. There is more substance to this complaint but ultimately I was not persuaded by the submissions. In short, I consider Mr Singla KC was right to argue that at the time that the without notice application was made, the Claimant did not know whether any agencies or content creators had transferred their business to *OnlyMonster* (and had no reason to believe that agencies had consented to the Defendants extracting their data from Infloww, as the Defendants now allege). Indeed, the Claimant did not even know the full extent of the Extracted Data and the customers that might be affected by it. In any event, the Claimant gave a cross-undertaking as to damages that covered third parties. It may be

that with the benefit of hindsight more could have been said but I do not consider the Court to have been materially misled.

74. I reject each of the fair presentation arguments. Standing back from the submissions, in my judgment the Defendants have not shown that in all the circumstances (and without the benefit of hindsight) the court was misled in any material respect at the WN Hearing. The Claimant was largely operating in the dark as to how their systems had been infiltrated and the evidential position was developing over time. I also consider that even if there had been a breach this is a case where the overall merits point towards interim relief of some form being re-granted.

VI. The Cause of Action

75. Although the Defendants have conceded there is a serious issue to be tried, it is necessary to be clear about what that means in practice. As I confirmed at the hearing with Mr Ayoo, the scope of this concession has two relevant aspects. First, that the facts as put forward by the Claimant are the basis on which I should approach the injunction application (that is, I must proceed on the basis that they are correct). Second, that these facts (involving infiltration, scraping and use of the Extracted Data on the *OnlyMonster* platform) give rise to arguable claims of unlawful conduct amounting to breach of confidence in relation to the Extracted Data (in each of the three forms) under English law and (if applicable) the other candidate laws (Spanish or German law).

76. In fairness, I should record that the reason given by Mr Ayoo for the Defendants' change of position (on the serious issue to be tried question) is what he called the Claimant's "pivot" in recently adding to the defined Extracted Data the Generated Data which he said "takes the legs" out of the argument that the data which the Claimant sought to protect was owned or created by the content creators. That said, he does not argue that the Fan Notes and Scripts are not confidential information capable of protection at the suit of the Claimant. So, the overall position for the purposes of the hearing before me, by way of concession, appears to be that *all* of the defined Extracted Data is capable of protection in a claim brought by the Claimant.

77. I could stop there in relation to the cause of action and arguability, but Counsel on both sides could not resist asserting the strength/weakness of the claims as part of their balance of convenience arguments. So, Mr Singla KC asserted his clients had very strong breach of confidence claims as regards the Extracted Data in its entirety. Mr Ayoo said the claims in respect of Fan Notes and Scripts were very weak (and his clients say they did not take any of the Generated Data).

78. In these circumstances, I will briefly deal with the legal position. Ultimately, one might say some data claims (particularly as regards Generated Data) are stronger than others, but I prefer to go no further than to say that the Defendants' concession (that there is a serious issue to be tried) is as far as one can take matters at this early stage. In short, I cannot form a view as to the legal merits which enables me to take it into account in the balance. I do however consider there is a real difference between restraining the Defendants from using the Extracted Data (in all forms) *themselves* and the different acts of providing continuing access to Fan Notes and Scripts to third party agents/content creators using their platform. The former seems at first blush to be more problematic than the latter (and this informs my approach to Options 1 and 2). I turn to how the Claimant's claims are put.

79. The Claimant's primary claim in English law is for breach of confidence. As Mr Singla KC explained at the WN Hearing, it brings its claim on two alternative bases: (i) that the Defendants owed a duty of confidence towards the Claimant *itself* in respect of the Extracted Data; (ii) alternatively, that the Defendants owed a duty of confidence towards the Claimant's customers (that is, content creators/agents) in respect of that data. This second way of putting the claim has been largely retreated from given the evidence that some of the agents themselves consented to transfer of the data. For completeness, I should record that conspiracy claims are also made by the Claimant (and hence the joinder of the personal Defendants). They appear to be parasitic in large part on the confidence claim and I say nothing further about them.

80. It is common ground that the three key elements of the cause of action are those set out in Coco v AN Clark (Engineers) Ltd [1968] FSR 415 ("Coco") at 419-421. More recent decisions such as Playtech Software Ltd v Games Global Ltd [2024] EWHC 3264 (Ch) ("Playtech") (Thompsell J) have expressed the criteria in slightly more helpful modern terms, but the substantive requirements remain the same.

81. Putting to one side issues which might arise in cases with different fact patterns, in this case (which is about what is said to be commercially confidential information) the relevant elements of the cause of action are in broad terms as follows:

    81.1 **CONFIDENTIALITY OF SUBJECT-MATTER.** First, the information "*must be of a confidential nature*" (Coco at 419). Megarry J noted in this context that even information "*that has been constructed solely from materials in the public domain may possess the necessary quality of confidentiality: for something new and confidential may have been brought into being by the application of the skill and ingenuity of the human brain*". This is because "*[n]ovelty depends on the thing itself, and not upon the quality of its constituent parts*". Put differently, the claimant must have had "*a reasonable expectation that the information is confidential or private*" (Playtech at [20(ii)]).

    81.2 **ACTUAL OR IMPLICIT NOTICE OF CONFIDENTIALITY**. Second, "*the information must have been communicated in circumstances importing an obligation of confidence*" (Coco at 419). The test is whether "*any reasonable man standing in the shoes of the recipient of the information would have realised that upon reasonable grounds the information was being given to him in confidence*" (Coco at 420-421). In other words, the claimant must show that "*at the time when the information was accessed or used, the defendant knew, or had sufficient notice, that the information was confidential*" (Playtech at [20(iii)]).

    81.3 **ACTUAL OR INTENDED UNCONSCIONABLE USE**. Third, there must be "*an unauthorised use of that information to the detriment of the party communicating it*" (Coco at 419). The claimant must show that "*that the defendant has used or plans to make use of the information in a way that amounts to an unconscionable misuse*" (*Playtech* at [20(iv)]). That is perhaps a better way and flexible way of putting the requirement than the concept of "detriment". One can also accommodate Article 10 ECHR considerations and the court's duties under section 12 of the Human Rights Act 1998 within the analysis of unconscionability.

82. I will briefly address each of these requirements in turn.

(a) CONFIDENTIALITY OF SUBJECT-MATTER

83. As I have recorded, the Extracted Data falls into broad two categories: first, the Fan Notes and Scripts provided by content creators/agents compiled by Infloww, and second, the Generated Data.

84. I will take the second category first. In my judgment, for the purposes of the hearing before me, I find it is plainly arguable as a matter of English law that the Generated Data is confidential to the Claimant. It covers data generated by the Claimant *itself,* rather than by content creators or their agents. The fact that such data is based on the activities of content creators or their fans does not affect the position. What makes the data confidential is "*the fact that the maker…has used his brain and thus produced a result which can only be produced by somebody who goes through the same process*": Lord Greene MR in Saltman Engineering Co v Campbell Engineering Co (1948) 65 RPC 203 at 215. The reporting and analytics data is commercially valuable, and is one of the main reasons for which users use Infloww. I accept that there is nothing preventing content creators/agents from producing that data themselves, but to do that they would have to take the effort of doing so – using the same (or a similar) process to that used by the Claimant.

85. Although the claim is perhaps not as clear, it is at least arguable that the first category of data (Fan Notes and Scripts) is confidential to the Claimant, although the analysis is slightly different. My reasons for that conclusion are as follows:

    85.1 The key attribute of confidentiality is inaccessibility, rather than secrecy: see e.g. The Racing Partnership Ltd v Sports Information Services Ltd [2021] Ch. 233 at [43]-[77], holding that certain raceday information was confidential notwithstanding that it was theoretically visible to everyone on the racecourse. See also CF Partners (UK) LLP v Barclays Bank plc [2014] EWHC 3049 (Ch) at [124].

    85.2 The confidentiality of the data arises from its *compilation* by the Claimant. In The Racing Partnership Ltd at [75]-[77]**,** Arnold LJ held that a compilation of information (racing data) could be confidential even if none of the individual pieces of information within that compilation was confidential.

    85.3 In CF Partners (UK) LLP v Barclays Bank plc*,* Hildyard J observed at [125]: "*A special collation and presentation of information, the individual components of which are not of themselves or individually confidential, may have the quality of confidence: for example, a customer list may be composed of particular names all of which are publicly available, but the list will nevertheless be confidential*."

    85.4 In HCE v UEH [2026] EWHC 33 (KB), Sheldon J at [19] held that the information on "*a website allowing people who are married to meet others to have marital affairs*" was confidential as an "*overall package*" to the claimant (which operated the website), even though some of the individual pieces of information were likely to be confidential to the users of the website.

86. At the December Hearing, the only basis on which Mr Colton KC, for the Defendants, sought to argue that there was no serious issue in confidence to be tried as a matter of English law (as regards Fan Note and Scripts) was as follows: "*The Extracted Data which forms the basis of Infinni's claim is not even arguably Infinni's confidential information:*

it is the information of Infinni's clients, its users. That much is clear from Infinni's Terms of Service".

87. I agree with Mr Singla KC that it is the Infloww Terms of Service (and not those of Infinni) that are relevant. I also agree with him that there is a serious issue to be tried as to whether the effect of the Infloww Terms of Service is that the Extracted Data is not confidential. Under the Infloww Terms of Service:

    87.1 "*Content*" is defined as "*any material uploaded on the Service by any User…*" (clause 1(b)).

    87.2 Users agree not to "*cause or launch any programs or scripts for the purpose of scraping, indexing, surveying, or otherwise data mining any portion of the Service*" (clause 9(m)).

    87.3 Content published by a User is not confidential and the User authorizes "*the other Users to access and view your Content on the Service for their own lawful and personal use*" (clause 11(a)).

    87.4 "*The Service is owned and operated by Us* [Infinni]. *The visual interfaces, graphics, design, compilation, information, data, computer code (including source code or object code), products, software, services, and all other elements of the Service (the "Materials") provided by us are protected by intellectual property and other laws. All Materials included in the Service are the property of Infinni Innovations S.A. or our third-party licensors. Except as expressly authorized by Infinni Innovations S.A., you may not make use of the Materials and We reserve all rights to the Materials not granted expressly in these Terms of Service.*" (clause 19(i)).

88. The Infloww Terms of Service are governed by Spanish law (see clause 25) and the Claimant has obtained Spanish law advice that the Terms of Service do not undermine its claim to confidentiality. As explained in the unchallenged evidence of its Solicitor:

> "For example, the definition of "Content" (Section 1(b)) refers to the text or data uploaded by the "User" (i.e. a creator) but it obviously does not include the additional data that is generated by Infinni to enable the functionality of the Infloww system. It is the aggregated and repackaged information that is confidential to Infinni. Consistent with this, there is a further definition of "Materials" in Section 19(i) which refers to information, data and code provided by Infinni which cannot be used or taken by Users. That term has not been addressed at all by the Defendants. Finally, it should be noted that Section 11(a) simply clarifies that the Content, once uploaded, can be shared with other Users. This does not mean it is publicly accessible to any third party. This is confirmed in paragraphs 36 and 37 of Bruna 2. As for the other terms, these are not determinative of the question of confidentiality. For example, the existence of IP rights belonging to Users in Content does not preclude a confidentiality right being simultaneously owed to Infinni."

89. Accordingly, I proceed on the basis that the Claimant has (at least) an arguable case that the Notes and Scripts have the quality of confidentiality.

(b) ACTUAL OR IMPLICIT NOTICE OF CONFIDENTIALITY.

90. It is well established that "*the equitable doctrine of confidentiality applies where a person improperly or surreptitiously obtains confidential information*": Toulson & Phipps, 4th edn, [3-094]. In Weiss Technik UK Limited v Christopher Davies [2022] EWHC 2773 (Ch) Bacon J held at [123] that "*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*". Similarly, in XXX v Persons Unknown [2022] EWHC 2776 (KB) Cavanagh J held at [36] that information obtained by computer hacking imported an obligation of confidence.

91. In my judgment, this aptly describes the present case on the unchallenged facts before me. Those facts show the Defendants surreptitiously exfiltrated data from the Claimant's systems for the benefit of their competing business (effectively using the ability to do this a "lure": see the *Honeytrap)*. As I have set out above, the evidence before me strongly suggests that the Defendants obtained access to the "back-end" of the system, which is not otherwise available to users. They then deployed a crawler program to scrape data from the Infloww platform. I have difficulty with Mr Liaskovsky's evidence for the Defendants that they did not bypass security controls and were only using the "*publicly accessible functionality within* Infloww". Although it is only a provisional view, I find this hard to reconcile with what was revealed during the *Honeytrap* operation, where Mr Kharmanskyi said that *OnlyMonster* had "*cracked inflow*" [sic] and "*found the way*" to bulk-extract data. I also note that in an undated WhatsApp exchange with a customer, *OnlyMonster* noted that they were "*working on*" a way to transfer data from Infloww, but that it *"[m]ight take some time*". Further down the chain, *OnlyMonster* notes that the "*tool for scripts migration*" was "*under development*" and would take "*between 1 and 2 weeks*" to be ready. The obvious inference is that these messages were exchanged between December 2024 and April 2025.

(c) ACTUAL OR INTENDED UNCONSCIONABLE USE

92. As regards the Fan Notes and Scripts this is not in issue. Subject to any order of the court, the Defendants will continue to make use of the Fan Notes and Scripts themselves and by providing access to agencies. If this is confidential information which was unlawfully extracted (which I assume for present purposes) it would appear to be unconscionable to use it without consent. Mr Ayoo does however contend (relying on the evidence of Mr Romanov) that the Generated Data has not been uploaded to the *OnlyMonster* platform and there is no intention to use it. This issue however disappeared at the most recent hearing because Mr Ayoo (while maintaining his client's case that they had not taken this data) said his clients would give an undertaking not to make use of the Generated Data.

VII. The Injunction Application

Undertakings

93. Two issues have been helpfully cleared away by undertakings. I will address each briefly.

94. First, the Defendants have given an undertaking in terms of paragraph 1(a) of the original injunction. So, they agree that they will not, without the express written prior consent of

the Claimant, further access or attempt to access any data on, or extract any data from, the Claimant's servers or computer systems in any way. That protects the Claimant against any future conduct. Given the nature of the infiltration and scraping, it was sensible for the Defendants to agree to this restraint against future conduct. Had this been contested, I would have been minded to make an order to that effect in favour of the Claimant. They are entitled to protection pending trial from further scraping and exfiltration attacks.

95. Second, Mr Ayoo, in the course of the hearing on 25 February 2026, gave an undertaking that his clients would not use the Generated Data, although his clients' case was that they did not have possession of it. As to this matter, Mr Ayoo made the realistic concession that what Kroll say about the Defendants accessing the Generated Data is a factual matter for trial to be resolved by expert evidence. Had an undertaking not been forthcoming, I would have made an order restraining use of the Generated Data. I will explain briefly why. The Generated Data consists of Script Analytics and Reports. It was only after the original injunction was granted, and following the investigations of Kroll that the Claimant discovered the Defendants had targeted such data. It amended its claim to include Generated Data on 15 January 2026. Mr Ayoo's original core submission in opposition to any relief in respect of such data was based on Mr Romanov's evidence that the Generated Data had "*...not been uploaded to the OnlyMonster platform*". Mr Romanov clarified that the Generated Data was "*called*" (in the sense that it was accessed), but he says it was not moved from Infloww and into the Defendants' possession, nor was it migrated onto the *OnlyMonster* platform (which has no functionality in this regard). Mr Singla KC submitted that given the history (including the lack of candour on the part of the Defendants as to their actions), an interim injunction restraining use of the Generated Data was justified.

96. Had this been contested, I would have agreed with Mr Singla KC. It is not in issue for the present hearing that this is confidential information belonging to the Claimant, and that it was accessed by surreptitious and arguably unlawful means. I find the explanations from the Defendants as to their actions in relation to API endpoints, to be to say the least, odd. In particular, their case that (despite calling the Generated Data from the relevant API endpoints), the Defendants never extracted it is somewhat surprising. Mr Romanov does not explain why the Defendants targeted several API endpoints that only return Infinni-generated data. For example, the Defendants targeted the API endpoint "*Query Fan Introduction*". That endpoint returns a whole range of reports data generated by the Claimant (such as "total spending amount", "number of paid messages" and "highest payment time"), but no user-generated data. It can fairly be said that if the Defendants truly had no interest in that reports data, they would not have targeted the relevant API endpoint in the first place. I would not in these circumstances have been willing to take it on trust that the Defendants had not in fact extracted the Generated Data and would have been minded to grant an injunction restraining use.

Issues in dispute: the emergence of Options 1 and 2

97. I turn then to what is in dispute and I need to begin with a description of the relevant agencies to explain some of the arguments. Annex A (as amended) to Mr Romanov's 3rd witness statement is a table of the agencies he identifies as having moved over to *OnlyMonster* having, on the Defendants' case, requested "migration" of "their" data held within Infloww. Annex A does not identify the agencies by name but lists 26 of them (using the letters A-Z). It states the date of "migration consent", the date migration was "performed" (a date range between January-December 2025), and "revenues for

November 2025". On the face of Annex A, it appears that *OnlyMonster* has only 16 active current agent clients ("the Active Agencies") from this list of 26. I infer that the 3 agencies who have provided witness statements fall within these 16 Active Agencies. They are Typa Management Limited, Royal Only Fans and Utopia: see [108] below. They are, on their evidence, agencies in relation to whom data was transferred from the Infloww to the *OnlyMonster* platform.

98. The Option 1 or Option 2 dispute turns on whether these 16 Active Agencies should *themselves* be prohibited from accessing and using the Notes and Scripts on the *OnlyMonster* platform (in effect through the Defendants being restrained from providing or facilitating access) (**Option 1**); or whether they should be permitted to make such use through the Defendants continuing to facilitate access (**Option 2**). I set out the full terms of these Options at [106].

99. The issue arises as a choice between these Options because, as I describe below, the terms of the injunction as regards Fan Notes and Scripts is capable of being read as a wider or narrower restraint. In order to describe how this issue eventually emerged, I need to begin with the terms of the original injunction made at the WN Hearing on 15 December 2025, and the approach of the parties to the scope of that restraint. I preface my comments by underlining that at that time, the Claimant was only aware of the scraping of Fan Notes and Scripts (and not the Generated Data).

100. The terms of the original injunction at paragraph 1(b) were as follows

> "...the Respondents must not, without the express written prior consent of the Applicant...use or otherwise exploit, or take any steps in relation to, any data that they have accessed on, or copied, downloaded or extracted from, the "msg_model_fans_remark" table in the pg6 database on the Applicant's server hosted by Amazon Web Services (the "Fan Insights Data") and/or the "msg_script" table in the pg6 database on the Applicant's server hosted by Amazon Web Services (the "Script Data")".

101. On its face, the effect of this restraint might be said to prevent the Defendants from not only using/exploiting the data itself, but to also restrain them from providing access to it to agencies which had come over to *OnlyMonster*. However, the history of events after the original injunction was made suggests that the position may not have been clear. So, in advance of the December Hearing, in the Defendants' Skeleton Argument (at §21) Mr Colton KC and Mr Grimley described the impact of the injunction in the following terms: "*in practice* [the original injunction means] *that although the content creators whose data was extracted continue to access the notes they have made about their fans, the Respondents may no longer be able to assist the content creators and agencies in maintaining such access".* Further, at the hearing itself, Mr Colton KC submitted "*…as we've made clear, the content creators and their agencies are continuing to read the fan data and to use the scripts. That's not a problem*" (Transcript, 23/23-25 to 24/1).

102. Although the December Hearing was devoted in effect to case management (and in particular whether it was appropriate for a discharge application to be heard that day) it was not suggested by Mr Singla KC at that hearing, on behalf of the Claimant, that this interpretation of the original injunction was wrong. But I accept that it was not a matter

specifically considered. Ideally, there would have been a resolution of the issue there and then. For good or bad reasons, the Defendants appear to have proceeded since the date of the original injunction (9 December 2025) on the basis that the Active Agencies could be provided with continued access to the Fan Notes and Scripts.

103. I should record however that in the correspondence between the respective Solicitors following the December Hearing, there was some confusion as to the scope of the injunction as regards the agencies. In the interests of brevity, I will not go through all of that correspondence but at points Enyo (then acting for the Defendants) sought clarification from Cooley (Solicitors for the Claimant) which suggests that they believed there was a restraint on agent use. Equally, Mr Singla KC properly accepted at the January Hearing that in some of the exchanges Cooley had with Enyo, it may have indicated that the original injunction did not prohibit the agencies from using the data on *OnlyMonster's* platform. In particular, I note that on 7 January 2026, Cooley appeared to accept that "*a request to extend an access period of an employee of an agency*" would not contravene the original injunction. I do not however feel able to obtain from the correspondence any clarity. There was confusion. And we know that in fact access continued to be provided by the Defendants to the Active Agencies.

104. In line with the position taken by Mr Colton KC and Mr Grimley at the December Hearing, in their Skeleton Argument for the January Hearing, Mr Ayoo and Ms Goodman observed at [§35] that the original injunction "... permits the content creators and agencies to continue to modify, supplement, overwrite and delete the Extracted Data. If there is a problem with access or functionality, however, the Injunction prevents *OnlyMonster* from providing assistance". Elsewhere in their Skeleton Argument, they expressed a position which suggests that the original injunction in fact had a wider scope so as to prohibit even access. So at [§32] it was said that (by reference to paragraph 1(b)) that the language of taking '*any steps in relation to*' Extracted Data was "...language of the widest import. It prevents the Respondents enabling, assisting, extending or removing access for third parties who might use such access to profit from, supplement, modify, overwrite or delete such data. That breadth appears to have been deliberate...". The Claimant's written submissions did not address this question.

105. Mr Ayoo's oral submissions at the January Hearing were advanced on the basis that it was uncontroversial that the agencies *were* permitted to use the Extracted Data. Having considered those arguments and those of Mr Singla KC at the January Hearing, it was not clear (to me at least) that this was uncontroversial. I asked for clarification of the Claimant's position, and it was in these circumstances that Mr Singla KC and Mr Chandrachud produced Options 1 and 2 in a draft on the morning of the second day of the January Hearing.

106. The draft injunction order produced by them provided at para. 1(b):

"Until further order of this Court, the Defendants must not, without the express written prior consent of the Claimant: "use or otherwise exploit, or take any steps in relation to, any data that they have accessed on, or copied, downloaded or extracted from the API endpoints listed in Schedule 3 to this Order (together, the "Extracted Data").

For the avoidance of doubt:

> **OPTION 1:** a. the Defendants are prohibited from continuing and facilitating the access of the Active Agencies to the Extracted Data on the *OnlyMonster* platform
>
> **OPTION 2:** b. the Defendants are not prohibited from continuing and facilitating the access of the Active Agencies to the Extracted Data on the *OnlyMonster* platform. b. The Defendants must not, without the express written consent of the Claimant: (i) Use the Extracted Data for the purpose of training, fine-tuning, or testing any artificial intelligence, machine learning models, chat training or automated communication algorithms; (ii) Sell, license or distribute the Extracted Data to any third party; (iii) Commercially exploit the Extracted Data for market analytics or to attract new customers; or (iv) Use or display the Extracted Data on any platform other than *OnlyMonster*."

107. So, Options 1 and 2 seek to provide clarification as to whether access to the Extracted Data can, or cannot, be provided to the Active Agencies by the Defendants pending trial. Given the confusion and the fact that the Defendants had clearly not come to the January Hearing to address an injunction with the scope of Option 1, I adjourned the January Hearing for a short time to give Mr Ayoo's clients an opportunity to submit evidence and submissions restricted to that matter (that is, the effect an injunction with the scope of Option 1 would have on the Defendants and the Active Agencies). I directed that Option 2 would apply to hold the ring pending a further hearing.

108. The Defendants in due course provided further evidence from Mr Romanov and from three Active Agencies that had moved over to *OnlyMonster* from Infloww. These agencies are Utopia (evidence of Mr Cobzaru, COO), Typa (evidence of Mr O'Neil, COO) and Royal Girls Only Fans (evidence of Mr Dan, CEO). This evidence expressly addresses (for the first time) the potential impact of the court making an order restraining the Defendants from continuing and facilitating the access of the Active Agencies to the Extracted Data on the *OnlyMonster* platform, in line with Option 1. The Claimant has served responsive evidence from Mr Bruna.

The injunction: submissions in outline

109. There was no dispute as to the law. Counsel made a wide-range of oral and written arguments on the balance of convenience. I will not set them out but will provide a broad overview before setting out the points I found persuasive and my conclusions. Some of the arguments for the Defendants are in relation to the granting of *any* relief and others were focussed on the Option 1 or Option 2 issue.

110. By way of an overarching submission, Mr Ayoo submitted that there had been what he characterised as an "enormous delay" in the bringing of the application for an injunction. He accepted that the Claimants did not know who was responsible for the infiltration in January 2025 but he argued a "persons unknown" form of injunction could have been sought. Mr Ayoo said that in any event by early May 2025, the Claimant took active steps to test what it now complains of: the *Honeytrap*. He submitted that at that

point, the Claimant knew the identity of the alleged wrongdoers and could have taken action. Mr Ayoo said that the Claimant's own evidence further records continued data access in July, August, September and October 2025 and it could have taken action at those times but chose not to do so. He underlined Kroll's instruction in late September 2025 and submitted that it is a reasonable inference that between at least May and September 2025, the Claimant knew the material facts on which it now relies.

111. Mr Ayoo further submitted that over the many months in which no injunctive relief was sought, agencies moved their business over to *OnlyMonster* as set out in the Defendants' evidence. He argued that they will have supplemented, modified, overwritten or deleted the Fan Notes and Scripts and they will be in a very different form when compared to what was migrated. Mr Ayoo said that an injunction would, if granted, therefore now operate in practice on live data held on the affected accounts, which may not bear any real relationship to the Fan Notes and Scripts. He underlined that the Active Agencies would be substantially prejudiced by an injunction with the Option 1 scope and relied strongly on the three agency witness statements to which I have referred above at [108].

112. Mr Singla KC argued that the status quo (which he said was the situation before the extraction and use of the Extracted Data began) should be adopted. He challenged the submission that there was delay and argued that I should take into account the strength of his client's case. Mr Singla KC said the position was straightforward, arguing that it is common ground between the parties: (1) that the Defendants accessed the Claimant's system and extracted large swathes of data from the servers without consent, and (2) there is a serious issue to be tried about whether the Claimant had a right of confidence in that data. Thus, he invited me to proceed on the basis that this is serious wrongdoing by the Defendants. Accordingly, he argued that an injunction should be granted to prevent the continued use of confidential information by the Defendants, which is effectively what the Defendants have been doing by continuing and facilitating the access of the Active Agencies to the Extracted Data on the *OnlyMonster* platform.

113. As to impact on third parties, Mr Singla KC strongly criticised the evidence produced by the Defendants and in particular the three agency witness statements. He submitted that at the January Hearing, when the Defendants maintained that an order in the terms of Option 1 would cause loss to Active Agencies, the Claimant "laid down a marker" that it would be impossible for it to interrogate that evidence without the Defendants identifying those agencies. He argued that, despite that, the Defendants have produced evidence from only three agencies and have refused to name the others. Mr Singla KC said that the Defendants have easy access to the names of all of the Agencies listed in Appendix A, but have taken a deliberate decision not to disclose them without any good reason. In relation to the agencies that have now been identified, he said that the evidence adduced by them is extremely "thin" and includes a great deal of hyperbole (with the use of words such as "*disastrous*" and "*catastrophic*"), but almost no financial information or figures. Mr Singla KC said that none of the Agencies had identified their revenue figures or have even attempted to quantify what profits (if any) they would lose as a result of the injunction sought under Option 1.

114. Mr Singla KC argued that even if it is assumed that that the Fan Notes and Scripts data have been modified so that it is impossible to segregate them from other later added data, I should nevertheless order an injunction that extends to **all** of the mixed Fan Notes and Scripts. He submitted that if the Claimant has a right of confidence in information

obtained by the Defendants, an injunction should be granted to the Claimant to prevent the continued use of their information even if it has been inseparably mixed up with non-confidential materials. The well-known cases of Seager v Copydex [1967] 1 W.L.R. 923 and Roger Bullivant Ltd. v Ellis [1987] FSR 172 were relied upon by analogy. Mr Singla KC rightly accepted however that there was no direct read-across from those cases.

Discussion and conclusions

115. I begin with delay which is a general point taken on behalf of the Defendants. I do not accept Mr Ayoo's arguments. Mr Singla KC was correct to submit that the Claimant had believed in May (and then in November 2025) that it had remedied its systems so as to prevent attacks. It was reasonable for it not to seek interim relief against the Defendants until the attacks began again and I find it acted with appropriate expedition. Also the Claimant did not have knowledge, until the evidence of the Defendants at the December Hearing, that a number of agencies had in fact moved over and had asked for the migration of data. I do not give delay weight against the granting of relief.

116. I first will consider the issue of whether as a minimum Option 2 should be adopted.

Option 2?

117. On the adequacy of damages, I agree with the Claimant that it would be difficult to quantify what losses it might suffer. I also did not have evidence which showed me what losses the Defendant might suffer if a restraint on their own actions was granted. I turn to the balance of convenience.

118. I have concluded that this clearly points towards (as a minimum) the Defendants being restrained from using the Extracted Data for their *own* direct benefit as identified in the sub-clause to Option 2. So, I conclude that, having taken the Extracted Data by surreptitious means and having failed to be open with the court as to how they did this, they should be restrained pending trial from: (i) using the Extracted Data for the purpose of training, fine-tuning, or testing any artificial intelligence, machine learning models, chat training or automated communication algorithms; (ii) selling, licensing or distributing the Extracted Data to any third party; (iii) commercially exploiting the Extracted Data for market analytics or to attract new customers; or (iv) using or displaying the Extracted Data on any platform other than *OnlyMonster*. The Defendants have not provided any convincing evidence as to why they should be allowed to undertake these acts using the Extracted Data, which they accept is confidential to the Claimant for present purposes. In particular, they advance no case as to how such restraints would prejudice them or a third party pending trial.

Option 1?

119. I begin with the issue of adequacy of damages. From the perspective of the Claimant, I do not consider it has clearly identified or evidenced what *further* loss (if any) it stands to suffer (for which damages would be due) if the Active Agencies *continue* to have access to the Extracted Data. The Active Agencies have had essentially unfettered access and made use of this data to date (that may be due to the confusion as to the scope of the original injunction but it has been access, nevertheless).

120. Were such access now to be interrupted, the content creators served by the Active Agencies will suffer immediate financial consequences while (if it is in fact possible) the Fan Notes and Scripts are recreated. How much revenue would have been generated by them if access to the Fan Notes and Scripts had not been denied to Active Agencies would be difficult to quantify. This factor is against granting Option 1 but I will in any event go on to consider the balance of convenience which is where Counsel each focussed their efforts in oral and written submissions.

121. I ask whether granting, or withholding, an interim injunction with the scope of Option 1 is more, or less likely, to cause irremediable prejudice (and to what extent) if it turns out at trial that it should not have been granted or withheld, as the case may be. As is well-established in law, the right course at this early stage in proceedings is that which is likely to cause the least irremediable prejudice to one party or the other. Prejudice to third parties is also relevant.

122. The arguments of fairness and prejudice to the Claimant on the one hand, or to the Defendants, on the other, did not persuade me that either had the better of the case on the balance of convenience when it comes to their own interests. I have however concluded that issues of practicality and considerations of impact and unfairness to the Active Agencies, who are third parties (and who are not said by the Claimant to be anything other than innocent) bring the discretionary balance down against an order with the scope of Option 1. Mr Singla KC submitted that the Defendants had restricted themselves to providing evidence from only three of the Active Agencies. That point does not assist. I consider the general points made about the practical difficulties and prejudice arising under Option 1 must apply as a matter of commonsense across the board. There is no suggestion that the way in which these three agencies operate (in terms of dynamic overwriting, modifying and updating of Fan Notes and Scripts in real time) is not representative of agency operations generally in the content creator agency world.

123. I begin with practicality. On the evidence before me, the apparent simplicity of Option 1 belies the fact that to comply with it, significant technological steps are required. The Notes and Scripts which were migrated from Infloww to *OnlyMonster* consisted of raw information and text. The Defendants did not migrate the "Scripts" or "Fan Notes" widgets or functionalities themselves from Infloww – *OnlyMonster* had its own, self-developed, integrations ("Message Templates" and "Fan's Overview") into which raw data was imported. I am satisfied that the evidence shows that the raw data is itself constantly being edited, overwritten, and deleted by the Active Agencies (indeed, that is part and parcel of their function). As I understand the position, when Scripts are edited, the previous entry will be deleted, with an entirely new text produced. Scripts are not available on the *OnlyFans* platform itself and an agency must use a CRM to access Scripts. When Notes are edited, the string of data is similarly replaced in its entirety. The *OnlyFans* "Notes" functionality appears to be very limited, and it is not linked to the "Notes" functionality on a CRM. There is no technological "switch" which the Defendants can flick which would remove Extracted Data from Active Agencies' *OnlyMonster* accounts.

124. In evidence the Defendants have mooted the development of a code which could somehow isolate initial Fan Notes or initial Scripts, and delete them from updated Fan Notes or updated Scripts. But I accept Mr Ayoo's submission that there are two obvious issues with this: (1) it is entirely speculative whether this code could be created; and (2) the Active Agencies would then be left with an unintelligible "mess", in circumstances where new Fan Notes and Scripts are not simply added line after line, in a chronological order, rather the existing Notes and

Scripts are rewritten. I was taken to an example during submissions of what the text would look like following an isolation and removal exercise and was satisfied it would leave a mess and unintelligible words.

125. In practical terms, therefore, I accept that if I ordered Option 1 the Defendants would have to either (1) delete the affected accounts or disable their access to *OnlyMonster's* chat functionalities; or (2) export live data into a CSV file (for preservation) and then delete all Fan Notes and Scripts from the Active Agencies' accounts (in which case agencies would be able to access the chat functionality, but without any of their data being available to use). Mr Bruna does not meaningfully criticise the Defendants' position on their practical inability to disable Active Agencies' access to Extracted Data. Mr Singla KC's criticisms centre on a purported lack of specificity in Mr Romanov's evidence. He said that Mr Romanov has not identified the demarcation between Extracted Data as initially extracted (down to the level of specific fan/creator conversations and as currently mixed). In my judgment, the Defendants' evidence convincingly demonstrates why this is not practically possible: (i) there is no practical way to demarcate edited 'components' of Fan Notes and Scripts (as when they are edited, new strings of data are produced) without writing a new code that would facilitate comparison and (ii) because of the rapid rate at which Fan Notes and Scripts are in fact being overwritten.

126. As I have recorded above in **Section 2**, teams of chatters employed by agencies communicate with fans continuously (that is, working around the clock) to provide constant engagement and interaction. As Mr Dan (on behalf of Royal) explains, Fan Notes are crucial due to the ongoing nature of conversations, which means that employees coming on shift are instantly up-to-date on the fan/creator conversation – he notes that Royal "*expect our employees to update the Notes hourly based on the live conversations that they are having with the fans*". In my judgment, the Defendants' case as to the continual data mixing follows logically from the nature of the business being carried out on *OnlyMonster* (and indeed on Infloww). Mr Bruna's criticism is that it is "*entirely possible that many of* [the agencies] *will have a number of dormant content creators, whose data has not been overwritten*". Even if that is correct, it is unarguable that there are huge numbers of active fan conversations which would be caught by Option 1.

127. I turn to prejudice and impact on third parties. The Claimant's apparent position is that Notes and Scripts are of limited importance to Active Agencies, such that Option 1 will have little impact on them. I note that Mr Bruna contends that the loss by the Active Agencies of their access to a CRM in general, or to the Notes/Scripts functionalities specifically, is not important because "*many agencies and content creators continue to thrive today without using CRMs*". I was rather surprised by this assertion given his earlier evidence at the WN Hearing (which was concerned with only the Fan Notes and Scripts) that the attacks had targeted Infinni's "*most valuable proprietary data*". Either the Fan Notes and Scripts are so valuable as to merit protection of the nature now sought by the Claimant – the total denial of access to those Fan Notes and Scripts to third parties – or they are not. I accept Mr Ayoo's submission that the Claimant's position is contradicted by the evidence produced by the Defendants, including that of the Active Agencies that, on the contrary, Option 1 stands to have a significant deleterious impact on the businesses of innocent third parties (including both Agencies and creators).

128. Mr Dan notes that "*repeat engagement and high value spending* […] *depends on staff being able to refer to detailed Notes and to use Scripts prepared within OnlyMonster. Without access to that data, Royal would expect a deterioration in the quality and consistency of fan interactions and a reduction in revenue*". Similarly, Mr Cobzaru considers that a loss of

access to Scripts and Notes will be "*disastrous*". Mr O'Neil equally sees Option 1 as "*catastrophic*" for his business. I see no proper basis at an interim hearing to discount this evidence. The Defendants' evidence – unchallenged by the Claimants – is that the Scripts are held on the CRM platform (not on OnlyFans). I note Mr Bruna's response to this is that he would be "*very surprised if the agencies did not have copies of Scripts stored independently*" in a Google document or CSV format. Mr Bruna's conjecture does not however follow: this very dispute is centred on the importation of Scripts from Infloww – if the Agencies had CSV format Scripts at their fingertips, they would plainly have provided those to the Defendants directly to import into *OnlyMonster*.

129. Mr Bruna suggests that agencies do not use Scripts for their highest-value fans – that employees manage the relationship directly, with "institutional" knowledge. This conjecture is directly contradicted by the Active Agencies: for example, Mr O'Neil states that Typa's chatters are restricted to using "*approved Scripts templates*" to ensure quality control. Moreover, I consider it is obvious that Notes will be of particular importance for high-value fan accounts, whose expectations regarding the personalisation and specificity of their chats will self-evidently be higher.

130. As to Fan Notes, Mr Romanov's evidence is that the Notes function on *OnlyMonster* is not linked to the Notes function on OnlyFans. As such, if Option 1 is put into effect, a third-party contractor will not have access to the Agencies' Notes, to be able to recreate those Notes. If Mr Bruna is suggesting that third party contractors log into each individual fan/creator chat and reconstruct Notes manually, that exercise will obviously take time. The evidence is that detailed Notes can be the product of years of conversations. Moreover, a third-party contractor (external to *OnlyMonster* and the OnlyFans ecosystem) is not the same as a trained chatter – the idea that they would have the requisite skillset, or understanding of the subject matter, to reconstruct pertinent Notes, either at all or at the pace suggested by Mr Bruna, is hard to follow.

131. There is a dispute on the evidence as to the direct financial impact of Option 1 on Agencies: the parties disagree on the profit split as between agency and creators – whether it is 15-50% (the Claimant's position) or in the region of 60% (the Defendants' position). Whether the burden falls largely on agencies or on creators is academic, because affected creators are <u>also</u> third parties, who are, if anything, in a more vulnerable position than Agencies (who may have unaffected creators).

132. I come back to the point that in relation to damages the Claimant has failed to identify (still less evidence) what loss it stands to suffer (for which damages would be due to them) should the Active Agencies continue to have access to the Fan Notes and Scripts. In my judgment, there is no identifiable prejudice which it stands to suffer should the more onerous Option 1 not be ordered.

133. Option 1 will, on the other hand, disable the ability of the Defendants to provide services to the Active Agencies, while the ongoing businesses carried out by Agencies and creators will, at the very least, be paralysed whilst they attempt to recreate their own data (which may not ultimately be successful).

134. For these reasons of practicality and prejudice to third parties, in the discretionary balance, the evidence comes down in favour of not making an injunction with the scope of Option 1. I have concluded that the injunction should reflect Option 2. So it will *not* prevent the Active Agencies from using and accessing the Fan Notes and Scripts on the *OnlyMonster* platform (as they have been doing since the migration) and the Defendants maintaining access (for

that limited purpose). But any other form of commercial exploitation of this data by the Defendants will be prohibited.

VIII. The Affidavit Application

135. As modified at the January Hearing, the Claimant seeks an order as follows:

> "The Defendants shall identify, to the best of their ability, in the form of a sworn affidavit to be served on the Claimant's solicitors within 10 working days of the Defendants being served with this Order: (1) all of the Extracted Data that they have accessed on, or copied, downloaded or extracted from, the Claimant's servers or computer systems (and provide a copy of that Extracted Data as it existed at the time of extraction); (2) insofar as any of the Extracted Data was accessed on, or copied, downloaded or extracted from, the Claimant's servers or computer systems by any other person acting on the instructions of the Defendants and subsequently made available to the Defendants or stored on their computer systems, such Extracted Data (and provide a copy of that Extracted Data as it existed at the time of extraction); (3) the dates, times and manner in which the Extracted Data referred to in (a) and (b) above was accessed on, or copied, downloaded or extracted from, the Claimant's servers or computer systems; (4) what use they have made of the Extracted Data referred to in (a) and (b) above.; (5) all of the Extracted Data referred to in (a) and (b) above which remain identifiable as at the date of this order; and (6) insofar as any of the Extracted Data is no longer identifiable as at the date of this order, (i) the reasons why they are no longer identifiable, and (ii) what steps (if any) have been taken by the Defendants to retrieve such data. If the provision of any of this information is likely to incriminate a Defendant, he or it may be entitled to refuse to provide it, but is recommended to take legal advice before refusing to provide the information. Wrongful refusal to provide the information is contempt of court and may render the Defendant (or, in the case of the First and Second Defendants, any of their directors) liable to be imprisoned, fined or have his or its assets seized."

136. Mr Singla KC argued that there is clear authority that the Court can order such disclosure alongside injunctive relief for breach of confidence where it is necessary to obtain information which is required, either to assist in giving effect to the injunctive relief, or to assist a claimant in undoing the harm, which has been unlawfully done: see City Site Solutions Ltd v Baker [2023] EWHC 2064 (KB) per Nigel Cooper KC (sitting as a Deputy High Court Judge) at [76]. He accepted that such an order must not subvert the ordinary accusatorial basis of litigation and turn the process into an inquisitorial one. He forcefully submitted that in this case, such disclosure is necessary to give effect to, and enable Infinni to ensure compliance with, the other injunctive relief sought because Infinni still does not know the full scale of the scraping attacks or the Extracted Data taken. Mr Singla KC also argued that insofar as any of the Extracted Data has been passed to third parties, Infinni needs to know this in order to begin "undoing the harm" (e.g. by pursuing relief against those third parties). He emphasised that the lack of openness of

the Defendants as to how they had got into the Claimant's systems was a further reason why the court should require disclosure.

137. Ms Goodman, who addressed this issue for the Defendants, made well-focussed and persuasive submissions in opposition. She took me to my decision in Delivery Group Limited v Yeo [2021] EWHC 1834 (QB) at [47] and Al Hajeri v Bennett [2013] EWHC 2552 (QB), per HHJ Seymour KC at [9]-[10]. Ms Goodman rightly accepted that the court had jurisdiction to direct a party to make a disclosure affidavit at an interim stage but she underlined the exceptionality of such an order. She also reminded me of the commentary in the *White Book* 2025 (Vol. 1) ¶25.1.44. Ms Goodman submitted that the order sought is in substance an order for early disclosure. She referred in this regard to the submissions advanced by Mr Singla KC at the December Hearing where he relied on lack of of prejudice to the Defendant if they had to comply with the obligation. She argued that this is not a proper use of an ancillary affidavit requirement attached to interim injunctive relief. Ms Goodman argued that precisely because the affidavit sought is an exceptional, contempt-backed measure, there can be no question of the Defendants being required to demonstrate "prejudice" as a condition of resisting it.

138. I start with the principles. First, the court has jurisdiction to make such an order. Second, although the test for making an order has been described as one of "exceptional circumstances", I do not find that to be a helpful test for judicial application - everyone says their case is exceptional. A more workable approach is to ask whether a claimant has shown with clear and convincing evidence that, in the particular circumstances of the case, such an order is strictly necessary to police and give effect to an injunction, or to provide assistance in preventing future harm. I use the qualifier "strictly" because under our civil procedure we still operate an adversarial process. While a defendant must give disclosure at the appropriate time, our processes do not impose contempt penalties for those who fail to provide evidence. Third, this is a discretionary and fact specific decision. That means a court will generally not be assisted by being taken to what other judges in other cases on different facts decided.

139. Applying these broad principles, I consider a modified form of disclosure affidavit should be ordered. Mr Singla KC was right to draw to my attention the fact that the Defendants have not properly responded to letters concerning preservation of disclosable material. Bearing in mind that the court should not make an order which goes beyond disclosure of such information as is necessary in order to police the injunction, my order will require the following. The Defendants must provide disclosure of all of the Extracted Data (in the form at time of extraction) that they (or anyone acting on their behalf) accessed on, or copied, downloaded or extracted from, the Claimant's servers or computer systems. The disclosure must be in the form of a digital image.

140. Although contradictory positions appear to have been presented earlier by the Defendants, Mr Ayoo helpfully clarified that disclosure of the data migrated (in the form it stood) as at the time of extraction was technically possible. The completion of the disclosure task and the accuracy of the image must be verified on affidavit by a responsible officer of the First and Second Defendants. The personal defendants must confirm with their own affidavits, that this affidavit represents the correct position to the best of their knowledge.

141. A requirement to state "*the dates and times*" at which the data was accessed, copied, downloaded or extracted serves no coherent policing function and would be onerous.

Indeed, no such function has been identified by the Claimant. Equally, I consider that knowing what "*use*" has been made is not necessary or proportionate. It is obvious – the Defendants have provided the data to the agencies who have come over to them. The Defendants have already explained this and if they have not been truthful there are consequences for making false statements.

142. As to the requirement that the Defendants disclose "*the manner*" in which they were able to obtain the Extracted Data, I agree with Ms Goodman that this is not necessary. The mechanism is exhaustively described in the detailed Kroll Reports (as updated on 16 February 2026). This was a thorough investigation and it is hard to identify how any legitimate policing function will be assisted by further disclosure from the Defendants at this stage. Disclosure obligations requiring the Defendants, on pain of contempt, to *put their hands up and confess* as to their entry mechanism cannot be justified in an adversarial process. If this remains an issue in due course, and after a disclosure process, a court will draw appropriate inferences against them. I consider that the Claimant is sufficiently protected by an undertaking from any future attacks and that is all that they need at this early stage: there has been no suggestion that there have been further attacks since the original injunction.

IX. Conclusion

143. I dismiss the application to discharge the injunction on fair presentation grounds. The injunction will remain in place on terms modified in accordance with my judgment, and including the undertakings given by the Defendants. I will make an order requiring disclosure of the information and provision of the digital image, as set out above.