Claim No. _____

IN THE HIGH COURT OF JUSTICE
QUEEN'S BENCH DIVISION

BETWEEN:

1. FACEBOOK, INC.
2. FACEBOOK IRELAND LIMITED

Claimants

- and -

1. FATIH HALTAS
2. MOBIBURN LIMITED
3. OAK SMART TECHNOLOGY LIMITED

Defendants

PARTICULARS OF CLAIM

The Parties

The Claimants

1. The First Claimant is a company incorporated in Delaware and based in Menlo Park, California. The Second Claimant is a company incorporated in the Republic of Ireland. The First and Second Claimants are referred to together below as "**Facebook**".

2. Facebook operates and controls a social networking website and mobile application (or app) that enables its users to create their own personal profiles and connect with each other on mobile devices and personal computers. All Facebook users agree to comply with Facebook's Terms of Service and other rules that govern different types of access to, and use of, Facebook. For Facebook users residing in the United Kingdom, Facebook is operated and controlled by the Second Claimant.

3. Facebook also operates a developer platform referred to below as the "**Facebook Platform**". The Facebook Platform enables third-party app developers ("**Developers**") to run apps that interact with Facebook and Facebook users. Facebook permits Developers to access and interact with the Facebook Platform, subject to and restricted

by Facebook's Terms of Service and Platform Policies,[1] referred to further below, by which all Developers agree to be bound.

The Defendants

4. The First Defendant ("**Mr Haltas**") is a computer engineer who was a commercial user of Facebook and was registered as a Developer on the Facebook Platform:

   (a) Mr Haltas created three Facebook user accounts – on 19 October 2007 under the name "*Fatih Haltaş*", on 15 October 2013 under the name "*Gulbeyaz Haltas*", and on 7 September 2016 under the name "*Fatih Haltaş*". Mr Haltas accepted Facebook's Terms of Service when he created each of these accounts. Mr Haltas also was an administrator of 69 Pages – a profile on Facebook used to promote a business or other commercial, political, or charitable organisation or endeavour – that were created between June 2018 and October 2019. He also created five business accounts, including one for the Third Defendant, and he created two Instagram profiles.

   (b) Accordingly, Mr Haltas agreed to be bound by Facebook's Terms of Service.

   (c) Mr Haltas registered a Developer account on the Facebook Platform on 17 January 2015, and operated and administered approximately 400 apps on the Facebook Platform between 2015 and 2019. All Developers using the Facebook Platform agree to the Platform Policies as a condition of using the Facebook Platform. Accordingly, Mr Haltas also agreed to be bound by the Platform Policies.

5. Mr Haltas is and was at all material times the sole director and sole legal and beneficial owner of the shares in the Third Defendant ("**Oak Smart**"), a company incorporated in England and Wales with company number 10862887. Mr Haltas also is and was at all material times the sole director of, and, through Oak Smart, the sole beneficial owner of the shares in, the Second Defendant ("**MobiBurn**"), a company incorporated in England and Wales with company number 11080185. Both Oak Smart and MobiBurn have at all material times acted under the direction and control of Mr Haltas.

[1] Previous versions of the Platform Policies have been called the "*Developer Principles and Policies*", the "*Platform Guidelines*" or the "*Developer Terms of Service*", but the material provisions have been substantially the same.

6. MobiBurn is a company that developed, marketed and distributed both proprietary and third-party software development kits ("**SDKs**") used to collect data through mobile apps. After a user installed one of these apps on their device and essentially "self-compromised", the SDK contained in the app would collect information about the user from their device and their social media accounts where the user logged into the app using those accounts.

7. MobiBurn's own website advertised to app developers and/or publishers that they could "*monetise* [their] *applications' valuable data*" by incorporating into their apps an SDK that "*collects and delivers data to* [MobiBurn's] *data marketing partners*". MobiBurn claimed that it merely distributed SDKs developed by a number of marketing and data monetisation companies, including OneAudience LLC ("**OneAudience**"), PushSpring, Huq and UnifyID.

8. According to Mr Haltas, Oak Smart designs, develops and publishes mobile games. Oak Smart states on its website that it creates utility, security and gaming apps. Between June 2018 and April 2019, Oak Smart created and operated various Facebook accounts, including Pages for its apps. At least one app connected to Oak Smart was created on the Facebook Platform by Mr Haltas. Accordingly, Oak Smart agreed to be bound by Facebook's Terms of Service and Platform Policies.

Relevant provisions of Facebook's Terms of Service and Platform Policies

9. Under Section 3.2.1 of the Terms of Service, Mr Haltas, Oak Smart and each Developer agreed not to do anything (or facilitate or support others engaging in any such conduct) that (i) "*breaches these Terms, our Community Standards and other terms and policies*" and (ii) is "*unlawful, misleading, discriminatory or fraudulent*".

10. Under Section 3.2.3 of the Terms of Service, Mr Haltas, Oak Smart and each Developer agreed not to "*access or collect data from our Products using automated means (without our prior permission) or attempt to access data that you do not have permission to access*".

11. The Platform Policies impose obligations and restrictions on Developers, including that Developers must obtain consent from the users of their apps before they can access their users' data on Facebook. The Platform Policies largely restrict Developers from using

Facebook data outside of the environment of the app, for any purpose other than enhancing the app users' experience on the app.

12. Through the Platform Policies, Developers agree that Facebook can audit their apps to ensure compliance with the Platform Policies and other Facebook policies. Further, Developers agree to provide proof of such compliance if Facebook so requests. Developers agree to the Platform Policies at the time they first sign up to the Facebook Platform, and continue to agree to the Platform Policies as a condition of using the Facebook Platform. Over time, these Platform Policies have imposed substantially the same restrictions on the use and collection of Facebook data.

13. The Platform Policies provide:

    (a) "*Don't sell, license, or purchase any data obtained from us or our services*" (Section 3.9).

    (b) "*Don't directly or indirectly transfer any data that you receive from us (including anonymous, aggregate, or derived data) to any ad network, data broker or other advertising or monetization-related service. By "indirectly" we mean you aren't allowed to, for example, transfer data to a third party who then transfers the data to an ad network*" (Section 3.10).

    (c) "*Comply with all applicable laws and regulations in the jurisdiction where your app is available*" (Section 5.8).

    (d) "[Facebook] *or an independent auditor acting on our behalf may audit your app, systems, and records to ensure your use of Platform and data you receive from us is safe and complies with our Terms, and that you've complied with our requests and requests from people who use Facebook to delete user data obtained through our Platform. If requested, you must provide proof that your app complies with our terms*" (Section 7.9).

14. Facebook will refer at trial to the whole of the Terms of Service and Platform Policies for their full terms and effect.

Development and use of the MobiBurn SDK Bundle

15. From at least April 2018, MobiBurn used its own SDK, as well as SDKs from at least one other company, in order to access and collect data from Facebook, without Facebook's authorisation and in contravention of Facebook's Terms of Service and Platform Policies. MobiBurn did not compromise Facebook; instead it used its SDK – installed by users on their device – to request data from Facebook.

16. Specifically, by at the latest 11 April 2018, Mr Haltas and MobiBurn knowingly developed an SDK bundle designed to obtain data from Facebook (the "**MobiBurn SDK Bundle**"). Mr Haltas and MobiBurn knowingly promoted and distributed the MobiBurn SDK Bundle to Developers for profit and their own commercial interests.

17. Third-party apps containing the MobiBurn SDK Bundle were distributed online to app users on various app stores. After a user installed one of these apps on their device and self-compromised, the MobiBurn SDK Bundle enabled MobiBurn (and its partners) to collect information about the user from their device and their Facebook account.

18. The MobiBurn SDK Bundle incorporated at least two distinct SDKs: (i) MobiBurn's own proprietary SDK (the "**MobiBurn SDK**") as well as (ii) one SDK from OneAudience (the "**OneAudience SDK**"). OneAudience is the subject of separate court proceedings brought by the First Claimant in the United States District Court in the Northern District of California (Case No. 3:20-cv-01461) concerning the malicious OneAudience SDK.

19. The MobiBurn SDK and the OneAudience SDK were knowingly included by Mr Haltas and MobiBurn within the MobiBurn SDK Bundle.

20. In particular, both the MobiBurn SDK and the OneAudience SDK, included in the app that the user would install, were programmed to collect the digital key that Facebook assigned exclusively to that app for a single user in order to make automated requests for data from Facebook. This digital key was associated with the ability to log in to a third-party app using one's Facebook login information. Mr Haltas and MobiBurn caused the MobiBurn SDK to misrepresent the source of those requests as the third-party app authorised to use the digital key. In fact, it was the malicious MobiBurn SDK that made the requests on behalf of Mr Haltas and MobiBurn. The OneAudience SDK

included by Mr Haltas and MobiBurn in the MobiBurn SDK Bundle also made similar requests.

21. Specifically, the MobiBurn SDK and the OneAudience SDK sent automated requests for data to Facebook computers in approximately 24-hour intervals. The data requested in this way included a user's name, locale, time zone, email address, Facebook ID, and gender. Facebook's technical restrictions prevented MobiBurn from accessing any user data that the user had not authorised the app to obtain. For example, if a user had not authorised the app to access gender information, Facebook computers denied the malicious SDK's request for the app user's gender. In instances where the MobiBurn SDK was able to obtain Facebook data, it was programmed to send that data to a remote server controlled by MobiBurn using the domain www.mobiburn.com/api/configs.

22. The MobiBurn SDK also collected data from the user's device, but the collection of that information was unrelated to Facebook. The MobiBurn SDK collected call logs, cell tower and other location information, contacts, browser information, email, and information about apps installed on the device.

23. Mr Haltas caused MobiBurn knowingly to develop and distribute the malicious MobiBurn SDK Bundle and promote it to Developers. Mr Haltas, acting through MobiBurn, provided the malicious MobiBurn SDK Bundle to Developers for incorporation into their apps.

24. Mr Haltas caused MobiBurn to provide the malicious MobiBurn SDK Bundle (and/or OneAudience's SDK directly) to Developers to further his and its own commercial interests:

    (a) MobiBurn either paid, or facilitated payment from data monetisation companies to, Developers to incorporate the malicious SDK into their apps and bundle it with other software components.

    (b) MobiBurn's own website advertised to Developers that it could enable "*the monetization of your applications' valuable data in a safe and confidential way*".

    (c) Mr Haltas caused MobiBurn to do this in order to obtain financial remuneration from data monetisation companies – directly or indirectly – for the data improperly obtained by the malicious SDK.

25. Developers received payment in return for incorporating the malicious SDK into their apps, and MobiBurn also received remuneration from the data monetisation companies. Information provided to Facebook by MobiBurn demonstrates that MobiBurn received payments from data monetisation companies.

Enforcement action taken by Facebook

26. In November 2019, Facebook took technical and legal enforcement measures against MobiBurn and OneAudience, including disabling apps, sending a cease-and-desist letter, notifying users, and requesting an audit pursuant to Section 7.9 of the Platform Policies.

27. On or about 21 November 2019, Facebook's U.S. counsel wrote to Mr Haltas in his capacity as CEO of MobiBurn (the "**November Letter**") explaining that Facebook had evidence that MobiBurn had violated and facilitated violations of Facebook's Terms of Service and policies, and in particular that MobiBurn had developed an SDK designed to improperly:

> "*obtain certain types of data from Facebook endpoints, namely, user IDs, name, gender, email address, and locale information. MobiBurn paid third-party app developers to install the SDK and transferred data obtained from the SDK to third parties for marketing purposes.*"

28. The November Letter demanded that Mr Haltas and MobiBurn cease all unauthorised access to Facebook user data. It also informed Mr Haltas and MobiBurn that their licences to access Facebook had been revoked, together with those of any agents or employees, and explained that Facebook had taken appropriate technical measures in connection with such revocation.

29. In addition, the November Letter demanded, among other things, that MobiBurn:

    (a) provide a full accounting of any Facebook user data in its possession;

    (b) identify all apps that had installed the malicious SDK;

    (c) provide marketing, communications and promotional material distributed or shared with clients or prospective clients regarding the SDKs;

    (d) provide a copy of the software code used to interact with Facebook; and

(e) delete and destroy all Facebook user data and provide evidence verifying that this had taken place.

30. MobiBurn (through Mr Haltas) responded on 25 November 2019, claiming that it did not develop or distribute any SDKs and that it did not have any products or services that interact with Facebook. Instead, it claimed that it "*ha*[d] *no access to the data collected by app developers nor do we process or store such data… We get in touch with mobile application developers and/or publishers and introduce them to data monetization companies like oneAudience, PushSpring, Huq or UNIFYID. We receive a certain portion of the fee paid by the monetization company to the developer as a commission fee*".

31. MobiBurn also stated that it had no employees or agents.

32. Following these responses, Facebook investigated further and confirmed that the MobiBurn SDK was present in at least version 1.5.3 (dated 11 April 2018) through to version 1.9.0 (dated 17 June 2019) of the MobiBurn SDK Bundle. Furthermore, versions of the MobiBurn SDK Bundle prior to version 1.9.0 also included the OneAudience SDK.

33. On 4 December 2019, Facebook's U.S. counsel attempted to schedule a call with Mobiburn (through Mr Haltas). The following day, Mr Haltas provided further misleading information and blamed the OneAudience SDK for any issues with the MobiBurn SDK Bundle.

34. On 12 December 2019, Facebook, through its U.S. counsel, sent further correspondence to MobiBurn (through Mr Haltas), repeating each of the requests set out at paragraph 29 above.

35. Mr Haltas responded on 16 December 2019, reiterating his prior responses of 5 December 2019 and denying that MobiBurn had acquired any Facebook data.

36. In light of these responses, on 3 January 2020, Facebook's U.S. counsel notified MobiBurn and Oak Smart that Facebook was invoking its audit rights against Oak Smart under the Platform Policies, since MobiBurn did not have any employees, and requested truthful responses from MobiBurn and Oak Smart to additional requests for information, including (once again) each of the requests set out at paragraph 29 above.

37. MobiBurn and Oak Smart, through Mr Haltas, responded again by claiming that MobiBurn had not used any methods to improperly access, transfer or store Facebook data, that MobiBurn did not know about the malicious code in version 1.9.0 of the MobiBurn SDK Bundle, but that, in any event, the code was "*irrelevant*".

38. Furthermore, Oak Smart did not respond or agree to Facebook's request to conduct an audit pursuant to its contractual rights under the Platform Policies.

39. On 7 February 2020 and 2 March 2020, Facebook's U.S. counsel sent further correspondence notifying Mr Haltas, MobiBurn and Oak Smart that Facebook was invoking its audit rights under Section 7.9 of the Platform Policies, but Mr Haltas, MobiBurn and Oak Smart continued to ignore these audit requests and failed to provide the information previously requested.

40. Moreover, as noted above, Mr Haltas' responses on behalf of MobiBurn dated 25 November 2019, 5 December 2019 and 16 December 2019 were not responsive to Facebook's requests.

41. Therefore, on 18 June 2020, Facebook sent a formal pre-action letter to Mr Haltas, MobiBurn and Oak Smart.

Mr Haltas breached his contract with Facebook Ireland

42. Mr Haltas has created at least one app on the Facebook Platform, called *Hardik Messenger* (Facebook ID No. 488130021540418) – created on 10 August 2017 and operated until November 2019 when Facebook disabled the app. This app had previously contained the malicious MobiBurn SDK Bundle.

43. Furthermore, through his actions described above, Mr Haltas has acted in breach of Facebook's Platform Policies by:

    (a) selling data obtained from Facebook or its services, in breach of Section 3.9 of the Platform Policies; and/or

    (b) directly or indirectly transferring data obtained from Facebook to data monetisation services, in breach of Section 3.10 of the Platform Policies.

44. As noted above, Mr Haltas also failed to respond to a letter sent to him by Facebook's U.S. counsel on Facebook's behalf on 7 February 2020, invoking Facebook's right of

audit against him personally (as a Developer registered on the Facebook Platform) under Section 7.9 of the Platform Policies. When he finally responded on 9 March 2020 to a further letter from Facebook's U.S. counsel, his response was wholly unsatisfactory: he failed to provide the information requested and refused to agree to the audit request.

45. In failing or refusing to grant Facebook's audit request made in the 7 February 2020 letter, Mr Haltas has breached his obligations under Section 7.9 of the Platform Policies.

Mr Haltas and MobiBurn induced or procured breaches of Developers' contracts with Facebook

46. Further or alternatively, Mr Haltas acting by MobiBurn, and MobiBurn, intentionally induced or procured those Developers who integrated the MobiBurn SDK Bundle into their apps to breach their contractual obligations to Facebook under the Terms of Service and the Platform Policies.

Interference with contractual relations

47. In knowledge of the contractual obligations owed by Developers to Facebook under the Terms of Service and Platform Policies, Mr Haltas acting by MobiBurn, and MobiBurn, knowingly and intentionally induced or procured Developers to breach the Terms of Service and Platform Policies.

48. Mr Haltas acting by MobiBurn, and MobiBurn, did this by promoting and providing the MobiBurn SDK Bundle to Developers for incorporation into their apps, in the knowledge that such incorporation would be inconsistent with the performance of the Developers' contracts with Facebook and a breach of the Developers' contractual obligations to Facebook.

49. Prior to disclosure and/or the provision of further information herein, Facebook cannot identify all of the Developers that Mr Haltas acting by MobiBurn, and MobiBurn, induced or procured to knowingly breach the Terms of Service and Platform Policies in this way. However, each such Developer who incorporated the malicious MobiBurn SDK Bundle into its app was induced or procured by Mr Haltas acting by MobiBurn, and MobiBurn, to breach the Terms of Service and Platform Policies in this way.

Breaches of contracts between Developers and Facebook

50. By incorporating the MobiBurn SDK Bundle into their apps and operating such apps on the Facebook Platform, it is to be inferred that each such Developer committed the following breaches of their contractual obligations:

(a) Used Facebook Products to do (or facilitate or support others to do) things in breach of Facebook's Terms of Service and Platform Policies, as set out below, in breach of Section 3.2.1 of the Terms of Service; and/or

(b) Facilitated or supported MobiBurn and others in accessing, attempting to access, and collecting data from Facebook Products using automated means without permission, including data that MobiBurn and others did not otherwise have access to, in breach of Section 3.2.3 of the Terms of Service; and/or

(c) Accessed, attempted to access, and collected data from Facebook Products using automated means, namely the MobiBurn SDK Bundle, without Facebook's prior permission, in breach of Section 3.2.3 of the Terms of Service; and/or

(d) sold data obtained from Facebook or its services, in breach of Section 3.9 of the Platform Policies; and/or directly or indirectly transferred data obtained from Facebook to data monetisation services, in breach of Section 3.10 of the Platform Policies.

51. These breaches of contract by the Developers were intentionally induced or procured by Mr Haltas (through MobiBurn) and MobiBurn in the full knowledge that such actions would cause damage to Facebook.

Knowledge of contracts between Developers and Facebook

52. Mr Haltas and MobiBurn so acted with knowledge of the Developers' contractual obligations to Facebook.

53. Mr Haltas, as a user of Facebook and a Developer on the Facebook Platform, agreed to be bound by Facebook's Terms of Service and Platform Policies and was accordingly aware of the terms thereof and that all Developers were bound thereby.

54. This knowledge on the part of Mr Haltas is attributed to MobiBurn of which he is the sole director and sole indirect beneficial owner and which has at all times acted under his direction and control.

Intention to induce or procure breaches of Developers' contracts with Facebook

55. Mr Haltas and MobiBurn so acted with the intention of inducing or procuring breaches by the Developers of the Developers' contractual obligations to Facebook, in that they acted deliberately and appreciated that the inevitable or alternatively probable consequences would be that the Developers would breach their contractual obligations owed to Facebook.

Damage

56. In late 2019, Facebook was notified that MobiBurn was paying Developers to integrate malicious SDKs into apps, including those available to Facebook users.

57. Facebook promptly commenced an investigation into the use of the malicious MobiBurn SDK Bundle in apps on the Facebook Platform. Facebook notified users and disabled apps created by or associated with Mr Haltas, MobiBurn and/or Oak Smart, and through its U.S. counsel entered into correspondence with and sent cease-and-desist letters to Mr Haltas, MobiBurn and Oak Smart.

58. As noted above, in the course of that correspondence with Facebook's U.S. counsel, Mr Haltas, acting on his own behalf and on behalf of MobiBurn, repeatedly refused to identify all apps that had incorporated the malicious MobiBurn SDK Bundle and to cooperate with reasonable requests for information.

59. Facebook incurred substantial cost and expense in carrying out the investigation, responding to MobiBurn's unauthorised access, notifying users and corresponding with Mr Haltas and MobiBurn. Full particulars will be provided in a schedule of loss in due course.

Oak Smart breached its contract with Facebook Ireland

60. As set out above, Oak Smart is bound by Facebook's Terms of Service and Platform Policies. The Platform Policies include at Section 7.9 a contractual right for Facebook to audit Oak Smart.

61. In breach of Section 7.9 of the Platform Policies, Oak Smart has refused requests by Facebook to allow an audit.

62. Facebook invoked its contractual right of audit against Oak Smart in a letter sent by Facebook's U.S. counsel on 3 January 2020. In an email sent by Mr Haltas on behalf of Oak Smart on 13 February 2020, he refused to allow Facebook to exercise its contractual audit right with respect to Oak Smart.

Relief claimed

63. By reason of the breaches of contract by Mr Haltas and Oak Smart and the inducing or procuring by Mr Haltas and MobiBurn of breaches by Developers of their contractual obligations owed to Facebook, Facebook has suffered loss and damage. Paragraph 59 above is repeated.

64. Facebook is entitled to and claims interest on all sums recoverable pursuant to section 35A of the Senior Courts Act 1981 to be assessed.

65. Further, Facebook is entitled to and claims an account by the Defendants of:

(a) all data obtained directly or indirectly from Facebook;

(b) all Developers to whom Mr Haltas and/or MobiBurn distributed the MobiBurn SDK Bundle or SDKs provided by a data monetisation company (including OneAudience's SDK);

(c) all payments made to Developers by or at the direction of Mr Haltas and/or MobiBurn, in connection with the distribution of the MobiBurn SDK Bundle or SDKs provided by a data monetisation company (including OneAudience's SDK);

(d) all payments received by Mr Haltas and/or MobiBurn in connection with the distribution of the MobiBurn SDK Bundle or SDKs provided by a data monetisation company (including OneAudience's SDK).

66. Further, unless restrained by the Court the Defendants will continue to distribute the malicious MobiBurn SDK Bundle and to induce or procure breaches by Developers of their contractual obligations owed to Facebook, and Facebook is entitled to and claims an injunction against each of them to prevent them from continuing to do so.

67. Further, Facebook is entitled to and claims a declaration that Mr Haltas and Oak Smart must comply with Facebook's audit rights under Section 7.9 of the Platform Policies, and respond, fully and accurately, to Facebook's requests for information and proof of compliance with Facebook's policies, including a forensic data audit.

AND THE CLAIMANTS CLAIM:

(1) Damages to be assessed.

(2) Interest pursuant to section 35A of the Senior Courts Act 1981 to be assessed.

(3) An account by the Defendants of:

(a) all data obtained directly or indirectly from Facebook;

(b) all Developers to whom Mr Haltas and/or MobiBurn distributed the MobiBurn SDK Bundle or SDKs provided by any data monetisation company (including OneAudience's SDK);

(c) all payments made to Developers by or at the direction of Mr Haltas and/or MobiBurn, in connection with the distribution of the MobiBurn SDK Bundle or SDKs provided by any data monetisation company (including OneAudience's SDK);

(d) all payments received by Mr Haltas and/or MobiBurn in connection with the distribution of the MobiBurn SDK Bundle or SDKs provided by any data monetisation company (including OneAudience's SDK).

(4) An injunction to restrain each of the Defendants, whether acting by their servants or agents or otherwise howsoever, from:

(a) developing, selling, offering for download, distributing and/or facilitating the distribution by any person of any malicious software that interacts with Facebook or any of Facebook's Products;

(b) inducing or procuring any Developer to act inconsistently with the Developer's contractual obligations to Facebook under the Terms of Service and Platform Policies;

(c) accessing Facebook and the Facebook Platform and/or using Facebook Products (including the Instagram service) for any reason whatsoever;

(d) including any reference to Facebook in any and all websites that he or it owns or has the ability to control.

(5) A declaration that Mr Haltas and Oak Smart must comply with Facebook's audit rights under Section 7.9 of the Platform Policies, and respond, fully and accurately, to Facebook's requests for information and proof of compliance with Facebook's policies, including a forensic data audit.

(6) Further or other relief.

(7) Costs.

ANTONY WHITE QC

Statement of Truth

The Claimants believe that the facts stated in these Particulars of Claim are true. I understand that proceedings for contempt of court may be brought against anyone who makes, or causes to be made, a false statement in a document verified by a statement of truth without an honest belief in its truth. I am duly authorised by the Claimants to sign these Particulars of Claim.

Signed: .....

Position: Partner, White & Case LLP

Served this 27th day of August 2020 by White & Case LLP, 5 Old Broad Street, London EC2N 1DW, Solicitors for the Claimants