DATA PROTECTION ACT 2018
(PART 6, SECTION 149)

ENFORCEMENT POWERS OF THE INFORMATION COMMISSIONER

ENFORCEMENT NOTICE

To: Experian Limited

Of: The Sir John Peace Building, Experian Way, NG2 Business Park, Nottingham, NG80 1ZZ

1. Experian Limited ("Experian") is a "controller" as variously defined in sections 3(6) and 5 of the Data Protection Act 2018 ("the DPA") and Article 4(7) of the General Data Protection Regulation ("the GDPR"). Experian is a credit reference agency but processes personal data in the course of wider business activities, including the provision of marketing services. This Enforcement Notice specifically relates to Experian's processing of personal data in the provision of offline marketing services.[1]

2. The Information Commissioner ("the Commissioner") has decided to issue Experian with an Enforcement Notice under section 149 DPA. This Notice is in relation to contraventions of the data protection principles set out in Article 5 GDPR, and in relation to the rights of data subjects provided for in Chapter III GDPR. This Notice is accordingly issued under sections 149(2)(a) and (b) DPA.

[1] "Offline" marketing services, as referred to in this Notice, focus on the provision of marketing to individuals through methods other than the internet. This can include postal, telephone and SMS marketing. It also means that the focus of the profiling activities investigated and addressed in this Notice does not include data collected about an individual's online behaviours. This activity is being investigated separately.

3. Following the issue of a Preliminary Enforcement Notice to Experian on 17 April 2019, the Commissioner received detailed representations from Experian, and a number of successive communications and further documents, including material evidencing steps taken or proposed by Experian to address certain aspects of the Commissioner's concerns. A revised Draft Enforcement Notice was provided to Experian on 20 April 2020, and this was followed by further detailed representations and accompanying documentation from Experian. Careful consideration has been given to all of the material provided by Experian throughout this process, although it has not been necessary to refer to every point or argument made in Experian's representations. The Commissioner recognises the constructive and responsible approach taken by Experian so as to address a number of the breaches identified in the Preliminary Enforcement Notice. Where appropriate, a narrative description of breaches that have been addressed by Experian is set out in this Notice: this information is included in the interests of transparency, so as to identify areas where Experian has itself taken remedial steps and hence the Commissioner has decided not to take enforcement action.

4. The Commissioner recognises that this has been an unusually lengthy process, including since the Preliminary Enforcement Notice was issued. However, that is because of the detailed nature of the audit work undertaken by the Commissioner; the extensive representations made by Experian; the extensive changes made by Experian subsequent to the audit and to the Preliminary Notice; the significant degree of engagement between the Commissioner and Experian during the process as a whole; the important and cross-cutting nature of some of the issues addressed in this Notice; and the opportunity given to Experian to

make further detailed representations in response to the Draft Enforcement Notice dated 20 April 2020. The Commissioner has throughout sought to balance taking time to consider the position of Experian and ensure that the issues were properly addressed, with the need to ensure that breaches of the rights of data subjects are effectively remedied.

5. This Notice explains the Commissioner's decision.

6. The Commissioner's investigation into processing by credit reference agencies originally commenced under the Data Protection Act 1998. Having paused that investigation, she returned to it following the GDPR taking effect on 25 May 2018. She did so to ensure that the significant processing activities of the credit reference agencies were addressed under the modern data protection regime (and by reference to its wider powers of regulatory audit), rather than based upon a historic legal position. This Notice is accordingly issued under the DPA and GDPR only.

Legal framework for this Notice

7. The DPA contains enforcement provisions in Part 6 which are exercisable by the Commissioner.

8. Section 149 DPA materially provides:

"(1) Where the Commissioner is satisfied that a person has failed, or is failing, as described in subsection (2), (3), (4) or (5), the Commissioner may give the person a written notice (an "enforcement notice") which requires the person—

(a) to take steps specified in the notice, or

(b) to refrain from taking steps specified in the notice,

or both (and see also sections 150 and 151).

(2) The first type of failure is where a controller or processor has failed, or is failing, to comply with any of the following—

(a) a provision of Chapter II of the GDPR or Chapter 2 of Part 3 or Chapter 2 of Part 4 of this Act (principles of processing);

(b) a provision of Articles 12 to 22 of the GDPR or Part 3 or 4 of this Act conferring rights on a data subject;

(c) a provision of Articles 25 to 39 of the GDPR or section 64 or 65 of this Act (obligations of controllers and processors);

(d) a requirement to communicate a personal data breach to the Commissioner or a data subject under section 67, 68 or 108 of this Act;

(e) the principles for transfers of personal data to third countries, non-Convention countries and international organisations in Articles 44 to 49 of the GDPR or in sections 73 to 78 or 109 of this Act.

...

(6) An enforcement notice given in reliance on subsection (2), (3) or (5) may only impose requirements which the Commissioner considers appropriate for the purpose of remedying the failure."

9. Section 150 DPA materially provides:

"(1) An enforcement notice must—

(a) state what the person has failed or is failing to do, and

(b) give the Commissioner's reasons for reaching that opinion.

(2) In deciding whether to give an enforcement notice in reliance on section 149(2), the Commissioner must consider whether the failure has caused or is likely to cause any person damage or distress.

(3) In relation to an enforcement notice given in reliance on section 149(2), the Commissioner's power under section 149(1)(b) to require a person to refrain from taking specified steps includes power—

(a) to impose a ban relating to all processing of personal data, or

(b) to impose a ban relating only to a specified description of processing of personal data, including by specifying one or more of the following—

(i) a description of personal data;

(ii) the purpose or manner of the processing;

(iii) the time when the processing takes place.

(4) An enforcement notice may specify the time or times at which, or period or periods within which, a requirement imposed by the notice must be complied with (but see the restrictions in subsections (6) to (8)).”

10. Article 4 GDPR contains definitions of relevant terms. Along with the definition of personal data and controller, Article 4(4) defines "profiling":

"'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal

preferences, interests, reliability, behaviour, location or movements".

11. The data protection principles are now set out in Article 5(1) GDPR. Compliance with the principles is the responsibility of the controller: Article 5(2). The first of the principles is provided for in Article 5(1)(a):

"Personal data shall be…processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')".

12. Article 5(1)(a) is supplemented by recital (39), which materially provides:

"Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing."

13. For processing to be lawful under Article 5(1)(a), processing must be in accordance with one of the bases set out in Article 6 GDPR, relevantly including:

> "1. Processing shall be lawful only if and to the extent that at least one of the following applies:
>
> (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
>
> ...
>
> (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

14. Chapter III of the GDPR makes provision for the rights afforded to data subjects. These include the rights of subject access, rectification, erasure and restriction of processing. Article 21 entitles a data subject to object to the processing of his personal data where it is done on the basis of the controller's legitimate interests (Article 21(1)) or where the processing is for direct marketing purposes including profiling for direct marketing (Article 21(2)). In the latter instance, the receipt of an objection must cause the processing to cease: Article 21(3).

15. Another right of data subjects is that contained in Article 14: the right to be informed of processing by a controller where the controller did not themselves obtain the data from the data subject. Article 14 provides:

"1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) the categories of personal data concerned;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(c) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;
(d) where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
(e) the right to lodge a complaint with a supervisory authority;
(f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;
(g) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. The controller shall provide the information referred to in paragraphs 1 and 2:

(a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;
(b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or
(c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

4. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

5. Paragraphs 1 to 4 shall not apply where and insofar as:

(a) the data subject already has the information;

(b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;

(c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or

(d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy."

16. The Commissioner considers that compliance with Article 14 is a vitally important element of transparent processing in accordance with Article 5(1)(a).

Experian's Processing of Personal Data

17. The Commissioner's investigation into Experian has focussed on its processing of personal data in relation to the provision of offline marketing services (as defined in footnote 1 to paragraph 1, above). Hence the findings set out in this Notice, and the requirements set out in Annex 1, relate to Experian's provision of offline marketing services: outside this area, the Commissioner expresses no view as to whether or not Experian's processing of personal data is compliant. The Commissioner's understanding of Experian's processing, and her findings in this Notice, are based on the information she has received as a result of the Assessment Notice issued to Experian on 20 July 2018 under section 146 DPA, together with the further information provided by Experian throughout this process, including in Experian's representations in response to the Preliminary Enforcement Notice dated 17 April 2019 and the Draft Enforcement Notice dated 20 April 2020.

18. Experian has asserted in its various representations that its processing takes the form of data analytics, rather than marketing in Experian's own name. Nonetheless, the purpose of Experian's data analytics business is, in this context, to further the direct marketing activities of third parties. Experian's processing facilitates such marketing; Experian is a controller in relation to such processing; and the processing is for direct marketing purposes. Moreover, the scale and scope of the processing in question is on a very significant scale.

19. Experian runs two primary databases: ConsumerView and ChannelView. These contain personal data concerning some 49.8 million adults (of some 52 million estimated to live in the United Kingdom overall). A range of more than 500 attributes, propensities and segmentations are applied to each identified name and address, across 15 categories. An attribute may be actual information, or it may be modelled information. A propensity is the likelihood of a characteristic in the form of a score. A segmentation is modelled information at a non-identifiable level, added to individuals. In ConsumerView, some 30 million records are flagged as being available to sell to third party organisations for marketing purposes.

20. ChannelView is principally used by Experian internally to link contact details with existing name and address profiles in ConsumerView, and is also used to add Mosaic information (see below) to individual profiles [redacted]

21. Experian Marketing Services acquires personal data of individual data subjects from a variety of sources. It uses publicly available sources such as the Open Electoral Register. The Commissioner understands (based upon discussions with Experian in September 2019) that it uses six data suppliers who have acquired data through their interactions with individuals. It uses general opt-out service data from the Telephone and Mail Preference Services, or other sources which indicate notification of changes in an individual's status or data. It also uses names and addresses from the credit reference aspect of its business to validate existing marketing records and for use in modelled attributes relating to household composition. Experian has sought to emphasise in its

representations that it uses credit reference data only for the following purposes:

(a) Validating an individual's name, address and age (over or under 18) for accuracy and screening purposes;
(b) Matching and linking records;
(c) Building models of groups of individuals by reference to certain characteristics (age, residency, households); and
(d) Screening out customers with inappropriate credit history.

The Commissioner notes that even the use of data for these purposes may involve accessing credit reference data in unexpected ways, such as establishing an individual's current or most recent address by checking for recent credit repayments from that address.

22. Along with selling records (under a licence format) for marketing, Experian provides further segmentation products. It enables third parties to compare their own data with Experian's records (to update contact details, for example, which enables those third parties to trace individuals with whom they have lost contact in order to send them direct marketing), and to revise third party databases so as to screen out records no longer appropriate or relevant. Experian also operates screening products such as Delphi for Marketing, with scorecards constructed from credit and marketing data.

23. Mosaic is a database which uses ConsumerView – as well as third party datasets – to build segments illustrating demographic and lifestyle attributes at postcode and household levels. It classifies all records into a set of lifestyle types, with 155 person types, 66 household types and 15 overarching groups. Attributes at postcode and household level are not reflective of specific details

of an individual, but are based upon aggregated individual data to create geodemographic probability groups. Some of the codes reflect likely ethnic make-up, although Experian's representations explained that these have not been used for new sales since February 2019 following concerns expressed by the Commissioner. Experian has not historically treated Mosaic as processing personal data because it is an aggregated and non-identifiable level. Attributes may be appended to individuals and once a Mosaic code has been so appended in, say, ConsumerView it is treated as personal data.

24. Experian publishes on the 'Consumer Information Portal' ("CIP") information about its processing of personal data. At the time of the audit, Experian's privacy policy referred generally to providing personal data to "resellers, distributors and agents", but was not more specific. The CIP now provides more detail about the sectors with which Experian might share data. As further explained below, Experian has continued to revise the CIP during the period leading up to the Commissioner's decision to issue this Enforcement Notice, and has continued to provide information to the Commissioner about these revisions. The Commissioner has taken account of all of this information when considering whether to issue this Enforcement Notice. Following Experian's representations in response to the Draft Enforcement Notice dated 20 April 2020, the Commissioner carried out a further review of the CIP in its most recent version, to ensure that the latest iteration of the CIP had been fully taken into account before issuing this Enforcement Notice.

25. Experian also makes available and relies on the Credit Reference Agency Information Notice ("CRAIN"), the most recent version of which was published in March 2020. The CRAIN is a general

notice produced and used by credit reference agencies. It focuses on the credit reference rather than the data broking aspects of these agencies' business. It sets out the wide variety of public sources used by Experian to obtain data about individuals, from the Electoral Register to statutory registers maintained by the Registry Trust Ltd. It advises readers how agencies such as Experian may use that data, and informs them that it may be used to screen people out of marketing lists but will not be used to identify or select people in order to send them marketing materials. The Commissioner acknowledges that a revised version of the CRAIN was published by the credit reference agencies in March 2020. She welcomes the work of the agencies to update and improve the CRAIN, but notes that it forms only one part of the privacy information provided by Experian. The focus in the Commissioner's investigation has been on that privacy information. The revisions to the CRAIN that took effect in March 2020 have been reviewed and taken into account by the Commissioner, but do not affect the conclusions set out below as to the legality of Experian's processing and as to the further steps that Experian is now required to take.

26. The commercial data suppliers used by Experian are required to set out in their own privacy information that data will be passed to Experian.

The Contraventions

27. The Commissioner is satisfied that Experian has committed a number of contraventions of the GDPR. These contraventions are addressed below in five separate categories (identified as categories A-E). Categories D and E relate to matters where the Commissioner considers that enforcement action is no longer

required. They are nevertheless addressed in this Notice in the interests of transparency, to explain the conclusions reached by the Commissioner and the reasons for those conclusions.

Category A: Fair and Transparent Processing: Article 5(1)(a)

28. Agencies such as Experian build up huge datasets about many millions of people. They use these datasets to produce a variety of marketing-led products, which are sold to third parties to enable more targeted and effective direct marketing to data subjects by those third parties. The Commissioner accepts that where an individual provides data about themselves or their circumstances in a publicly available context – be it via the Open Electoral Register, by involvement in the judicial system, or through Land Registry records – the use of that personal data is not prohibited by the GDPR simply because it was not provided directly to Experian or the third party. However, the collation of a wide range of personal data about a huge number of data subjects constitutes processing on a scale and for detailed analytical purposes which few data subjects would expect. These purposes include data profiling within the meaning of Article 4(4) GDPR.

29. It is therefore incumbent on controllers such as Experian to ensure that they are as transparent as possible, in accordance with Article 5(1)(a), about the data they are using, where it has been obtained from, and the ways in which it is used. Without clear, detailed and transparent information provided in a way that a data subject can readily understand, the data subject is precluded from being able to exercise the rights afforded by the GDPR.

30. The requirement of transparency in Article 5(1)(a) includes, but goes beyond, simple compliance with Article 14 GDPR. It is a context-dependent obligation, having regard to the nature and circumstances of the personal data being processed.

31. In her Preliminary Enforcement Notice, the Commissioner explained her provisional findings that Experian's privacy notices and the CIP generally did not comply with the requirement of transparency in Article 5(1)(a). The privacy notices and the CIP were insufficiently clear in explaining how data is collected, processed and sold. They did not make clear that credit data is processed in connection with direct marketing: the data in question, and the purposes for which it is used, are set out in paragraph 21 above. Although Experian argue that this is relatively limited processing of credit reference-derived data, it is nonetheless used to model and to link data subject profiles, in a manner which then feeds into profiles used for direct marketing products. The data subject would be unable to understand the limited references to this sort of processing in Experian's privacy notices, without understanding Experian's internal processes and the various datasets that it maintains. The privacy notices did not specify what personal data is collected and used, from exactly where it had been sourced, the precise publicly available sources relied upon, or to whom the data might be provided or sold. The privacy notices did not provide examples of how data is being processed to aid the data subject's understanding of the application of the data and its possible impact on the data subject. For the avoidance of doubt, the Commissioner considers that this analysis applies to all uses of credit data for direct marketing purposes, including screening, validation, matching and linking, and modelling.

32. The CIP did not expressly detail all the rights available to data subjects, for example, the rights of rectification or restriction of processing under Articles 16 and 18 GDPR; nor did it give a precise retention period for which personal data held for marketing purposes will be processed.

33. Where Experian databases, such as Mosaic or other datasets using the work of Mosaic, attach information or attributes to an individual data subject in the context of data analysis – whether or not the product sold to or used by third parties contains that level of data – that is the processing of personal data and, specifically, it is processing in the form of profiling within the meaning of Article 4(4) GDPR. Experian did not ensure that such processing was transparently explained in its privacy notices and properly assessed for a lawful basis of processing in order to comply with Article 5(1)(a).

34. Experian's Club Canvasse product is a closed member group which pools data from [redacted] members. [redacted]. The Club Canvasse members are clearly controllers of the data that they provide to Experian themselves. However, when Experian enriches the existing data with characteristics or attributes Experian has applied to the same data subject in the course of its own processing, then that processing is done by Experian as a controller. Experian accepted that it was a controller as a result of the audit process; but in order to provide transparency to data

subjects, it was also necessary to ensure that such processing was fully addressed by Experian in the CIP and other relevant privacy notices.

35. In the light of the Preliminary Enforcement Notice and Audit Report, Experian explained to the Commissioner that it had undertaken extensive work to, in particular, change the CIP in order to improve transparency. That work had sought specifically to address the following matters: explaining details of the attributes that Experian processes, in a clear and illustrative manner; the processing of modelled data and the profiling undertaken; retention periods; data subject rights; and the processing related to Club Canvasse in respect of which Experian is the controller. Experian will also update its terms and conditions with Club Canvasse members, to require the privacy notices of those members to reach a similar level of clarity as the CIP. Experian will carry out six-monthly reviews of those privacy notices to ensure satisfactory compliance.

36. The Commissioner has carefully reviewed all of the successive changes that Experian has made to the CIP, and she welcomes Experian's willingness to make them. In the light of the work done by Experian up to that point, she reviewed the version of the CIP current in October 2019 to establish whether it would be appropriate to impose any enforcement requirements on Experian in relation to these matters. Thereafter, the Commissioner has continued to review the information provided to her by Experian in relation to subsequent changes to the CIP: as part of this continuing work, the Commissioner carried out a final review of the up to date version of the CIP directly prior to the service of this Notice. The Commissioner also reviewed the user research undertaken by Experian in December 2019. Although such a

testing process is not directly mandated by data protection law, the Commissioner agrees that it can assist Experian in seeking to demonstrate (under the accountability principle in Article 5(2)) that they have taken steps to comply with their obligations concerning transparency. The user research (although conducted with a very small group) was generally positive about the language, detail and functionality of the CIP, but the Commissioner notes that user understanding of Experian processing appears to have been tested on a reading of the CIP in isolation (rather than a comparison between an explanation of the processing concerned and a reading of the CIP). She also notes that in some cases (such as Mosaic) individuals struggled to understand the processing or how it benefited them, and that individuals often failed to find the CIP when looking for Experian's privacy information. Accordingly, the testing conducted by Experian does not provide the Commissioner sufficient assurance that her concerns set out below are assuaged.

37. The Commissioner acknowledges that the CIP is now much improved, both as compared with what was seen by the Commissioner during the audit (such as in relation to data subject rights), and more generally as compared with privacy information found elsewhere. Nevertheless, the Commissioner considers that even in its most recent version the CIP still fails to achieve the necessary transparency to ensure individuals understand the complex processing of their personal data for marketing purposes. In particular:

    a. The CIP still fails to set out clearly in one place and at the forefront of the privacy information the attributes (actual and modelled) that may be processed about an individual;

b. Information likely to surprise individuals (for example, that data will be used to trace individuals for marketing, or used to allow clients with only email addresses to profile those individuals) is held in the third or fourth layer of the CIP: this is contrary to clear guidance from the Article 29 Working Party (now adopted by the European Data Protection Board, or "EDPB") and the Commissioner that such information should always be to the forefront of privacy information (see further paragraph 45 below as to the relevant guidance);
c. The language of the CIP emphasises the benefits of data broking, without giving any real explanation of potential drawbacks or outcomes that individuals may find undesirable. Whilst Experian is welcome to explain why they think individuals may not object to the processing, the lack of balance and use of language designed to persuade an audience about the benefits of processing for marketing purposes can obscure an individual's understanding of the risks of such processing (cf. GDPR recital (39)): this is so, for instance, when the language focuses exclusively on possible benefits, and characterises licensing for financial gain as "sharing";
d. Individuals are still likely to be unclear about the potential outcomes of the processing for them, in real-world terms (for example, with how many different organisations is their data likely to be shared in order to achieve that they receive more relevant marketing? Will the processing result in organisations such as political parties profiling the individual?);
e. Use of industry language like "insight" is likely to have little meaning for an average individual as the term covers a large variety of processing activities (with different potential

outcomes) that will not be readily understood by the intended audience (although the Commissioner notes in this regard the efforts made in the latest version of the CIP to explain what is meant by "segmentation");

f. Examples of processing from point of collection to some real use cases are still absent in some sections (though the Commissioner notes the additional examples given in the most recent version of the CIP, e.g. in the data linkage section), making it harder for individuals to visualise the complex processing of their personal data. Although examples are not specifically required by Articles 13 or 14, in the circumstances the Commissioner considers that they are vital to ensuring that Experian meets its wider transparency obligations.

38. Experian also continues to contravene Article 5(1)(a) in other respects.

39. The implicit assertion in the CRAIN (prior to the revised version published on March 2020) was that processing the personal data of individuals obtained from credit referencing processing, and particularly data connected to their actual or profiled wealth and finances, in order to screen out from receipt of direct marketing those calculated to be insufficiently wealthy to warrant receipt of the marketing communications in issue, does not constitute processing for direct marketing purposes. The CRAIN explained that such screening out occurs, and states that this prevents the receipt of irrelevant marketing and is not used to identify and send marketing material, which indicates that such processing is not for direct marketing purposes. The Commissioner does not agree. It is processing for direct marketing purposes, just as the decision to screen in a data subject on the basis of their financial

information is processing for direct marketing purposes. These two types of processing are the opposite sides of the same direct marketing coin. The failure of the CRAIN – or any other privacy notice relied on by Experian – to make this clear is a breach of the duty of transparency. Although the version of the CRAIN published in March 2020 addresses some of these deficiencies, the fundamental problems addressed in paragraphs 40 and 41 below in relation to the processing of credit reference data for direct marketing purposes still remain.

40. The processing referred to in the previous paragraph leads to the processing of credit reference data of the data subject for direct marketing purposes in a manner which would not be expected by the data subject and is, in addition, unfair processing. Processing personal data collected specifically for the creation and maintenance of credit reference files for screening or any other direct marketing purpose should cease unless and until it is transparently explained and the individuals in question have consented to the processing.

41. This processing is unlikely to be expected by the data subject, is of a higher level of intrusion, and individuals have no choice about whether their data is shared with Experian for credit referencing purposes; indeed, if it were not, the individual is likely to struggle to access credit. In these circumstances, it is not appropriate for credit reference data to be licensed by Experian for direct marketing purposes without the active agreement of the individuals concerned. To be clear, the Commissioner does not expect individuals to have to provide consent to a lender sharing their data with Experian for credit referencing purposes. Rather, the Commissioner expects that Experian would obtain consent for their credit reference information to be used for direct marketing

in this manner: such consent could either be obtained by Experian directly from the individual, or by the lender on Experian's behalf, clearly and separately from the collection of data to be shared for credit referencing purposes.

42. The Commissioner is aware that some credit reference file information is gathered from publicly available sources (such as County Court judgments or individual voluntary arrangements), and that one solution for Experian may be to obtain elements of the publicly available personal data (that constitutes credit reference information) for both credit referencing purposes and additionally for their own direct marketing purpose. This could involve separating the transparency and legitimate interest assessments from the credit referencing business. The Commissioner has no objection to such work in principle and reserves her judgement on the compliance of the activity, noting merely that the processing of publicly available data must in all respects comply with the requirements of the data protection legislation.

Category B: Article 14 GDPR

43. Relatedly, Experian has contravened Article 14 GDPR in failing to notify data subjects that their personal data has been acquired by Experian and is being processed for direct marketing purposes.

44. Where Experian acquires the personal data of a data subject from a third party, Experian does not provide Article 14 privacy information to the data subject directly. Experian proceeds on the basis that the data subject will already have been given the information set out in Article 14, so that Article 14(5)(a) disapplies the requirement for Experian itself to provide the

information directly to the data subject. In this regard, Experian relies on the privacy policies of the third parties, which in many cases provide links to the policies of Experian. Experian asserts that some 90% of data subjects will have received "notifications" in this sense in relation to Experian's processing, as a result of those data subjects' engagement with the third party data suppliers. The Commissioner notes that, even on the basis of Experian's figures, some 10% of data subjects (amounting to about 4-5 million individuals) will not have received such notifications.

45. The Commissioner does not accept that Article 14(5)(a) is satisfied so as to exempt Experian from its own Article 14 obligations. While a data subject is likely reasonably to expect their credit data to be provided to a credit reference agency for credit referencing purposes, they are not likely to expect that data to also be used by the credit reference agency for direct marketing purposes. They would only discover such a possibility if they reviewed both the third party supplier's privacy policy and the CRAIN and the CIP of Experian; but the CRAIN and CIP do not clearly draw attention to the provision of data to Experian and the use of that data for direct marketing purposes. This is inconsistent with the Commissioner's guidance on 'The right to be informed'[2] and the guidance of the EDPB in 'Guidelines on Transparency under Regulation 2016/679' (WP 260rev.01)[3] that when using layered privacy notices, the first layer most likely to be seen by the data subject must draw attention to the most

[2] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/

[3] At its first plenary meeting the EDPB endorsed and adopted the GDPR-related guidelines, including WP 260rev.01, produced by its predecessor body, the Article 29 Working Party.

significant, impactful processing and the processing which is least likely to be expected by the data subject. Such processing should be immediately apparent to the data subject without having to scour through multiple policies. Applying this guidance is even more important where the data has been supplied to Experian by third party data suppliers which the data subject would not or probably would not expect to have passed their data to Experian at all, let alone for the extensive direct marketing and profiling purposes for which Experian obtains it.

46. Experian appears, in its representations, to rely upon direct notification involving a disproportionate effort as a basis for its reliance on Article 14(5)(a). This is not legally correct. Either the data subject already has the information required by Article 14 and hence falls within Article 14(5)(a), or they do not have that information and hence fall outside Article 14(5)(a). Either way, proportionality is irrelevant. The Commissioner does not accept that *any* of the data subjects who are not direct customers of Experian have the necessary information to satisfy Article 14(5)(a): still less does she accept, as asserted by Experian, that *all* of the individuals whose data are provided to Experian through third parties have the necessary information. Article 14(5)(a) cannot therefore apply.

47. Where personal data has been acquired from publicly available sources – such as the Open Electoral Register – rather than via third parties, Experian does not issue Article 14 privacy information to the affected data subjects. For this cohort of data subjects, Experian does not rely on Article 14(5)(a): these data subjects fall within the 10% figure referred to in paragraph 44 above (albeit the Commissioner notes there are overlapping notification issues here as individuals may well be on both the

Open Electoral Register and in datasets obtained from third parties). Instead Experian asserts that it would involve a disproportionate effort to notify those data subjects: hence Experian relies on Article 14(5)(b) in respect of these data subjects, on the basis of disproportionate cost. Generally, Experian relies on Article 14(5)(b) in respect of any data subjects for whom Article 14(5)(a) is not satisfied.

48. Save for one specific exception (explained at paragraph 54 below), the Commissioner does not accept that Article 14(5)(b) is satisfied. Therefore Experian is subject to the requirement that it directly provide privacy information both: (i) to data subjects whose personal data Experian has acquired from publicly available sources; and (ii) to any other data subject to whom Article 14(5)(a) does not apply.

49. Experian suggests that its processing is not intrusive and is likely to be expected, and that any direct notification exercise will be extremely costly and ignored by data subjects. On this basis, Experian contends that the direct notification of data subjects would be disproportionate. The Commissioner has taken into account all of the representations made by Experian, including the detailed points about cost that are set out in Experian's representations in response to the Draft Enforcement Notice dated 20 April 2020. Overall, the Commissioner's view remains that direct notification is not disproportionate and that Experian cannot therefore rely on Article 14(5)(b).

50. The question of proportionality must be considered in the light of the extensive processing carried out by Experian, coupled with the largely invisible nature of that processing (in particular, the profiling of data subjects by which Experian compiles public and non-public data to create marketing profiles of individuals for its

clients). While the Commissioner does not suggest that Experian's processing is at the most intrusive end, it nonetheless involves the compilation of a wide range of data from public and private sources so as to build a profile of some 49.8 million data subjects. Few data subjects would expect such processing on a mass scale in order that a profile can be built of them and their preferences for the purpose of targeted direct marketing. Such processing is intrusive of privacy.

51. Moreover, it is relevant that the processing is a matter of choice on the part of Experian, and that it follows from Experian's own business model. Where a controller's business model depends upon the mass collection and processing of personal data, it does not assist the controller to assert that compliance with legal requirements would be disproportionately burdensome. The situation Experian has placed itself in is, for example, quite unlike that of the examples given in the Commissioner's and EDPB's guidance (referred to in paragraph 45 above). Article 14 imposes a particularly important obligation, given the especial need for transparency in respect of data subjects who would otherwise not be aware that the controller is processing their data. Exceptions to that principle should be narrowly construed. Further, the following points are material.

- The fact that there are large numbers of data subjects cannot in itself be a determinative factor against the proportionality of notification: otherwise controllers are given a perverse incentive to accumulate data about as many individuals as possible, in order to support their case on proportionality and hence reduce the burden of notification.

- It is recognised that compliance with Article 14 may be costly to Experian (although it is not accepted that all of the sums proposed need to be incurred at the level set out by Experian in its representations, or indeed at all). However, the cost will inevitably be high if viewed in isolation; this is because it is the cost of catching up on an accumulation of many years during which there has been a failure to give notifications. It cannot be right that a controller can fail over many years to give notifications to data subjects, and then rely on the cost of rectifying that failure as providing a justification for taking no further action: such an approach likewise creates a perverse incentive for a data controller to fail to comply with its Article 14 obligations over a prolonged period.

The Commissioner also has regard to the fact that in the context of this processing, it is inherently likely that Experian has relevant contact details for the data subjects, since without such contact details, the processing for marketing purposes would be ineffectual. As all affected data subjects will require the same privacy information it will not be necessary for Experian to create individualised information. Whether or not the data subject wishes to read and digest the information provided to them is a matter of choice for that data subject: it is not for Experian to deny them that choice but rather, in accordance with Article 14, to draw their attention to the processing.

52. Experian relies on its rights under Article 16 of the EU Charter of Fundamental Rights ("the Charter"), which relates to the freedom to conduct business. That does not assist. The Commissioner takes this action to secure the fundamental Charter rights under Article 7 (privacy) and Article 8 (personal data) of some 49.8 million data subjects. In the circumstances, including the wider

concerns the Commissioner has had to express through this process about compliance with transparency obligations, the proportionality balance does not favour prioritising the protection of Experian's business model over the data rights of the huge number of affected data subjects.

53. In its representations and other correspondence with the Commissioner, Experian has advanced a number of alternative solutions to avoid the costs of a direct notification exercise by mail. The Commissioner accepts that the requirements of Article 14 could, in theory, be met by means other than direct mail. However, there are a number of constraints on acceptable compliance. A newspaper, TV or other advertising campaign alone would not be sufficient because (leaving aside any difficulties with ensuring the information in each limb of Article 14 was provided with sufficient clarity) it cannot be guaranteed that a given individual would see the campaign, meaning some individuals would continue to be unable to exercise their rights. Individuals must themselves be given the notification by Experian; merely placing it somewhere in the hope that they will see it is not acceptable. In any case, a general advertisement would not be directed to the individual viewing it, meaning the individual could not know whether Experian was, or was not, processing their data. An unaddressed mailshot to every UK postal address would fail for the same reason. The Commissioner is also aware of consideration being given in the data broker industry more widely to a joint notification from some or all data brokers in order to share costs. Although there is no reason in principle to reject such a project, a joint notification may fail to be transparent by being overly generic (insofar as not every data broker will be processing the data of every recipient of the notice), overly simplistic (thereby failing to provide acceptable transparency) or overly

long (and risking key transparency information being lost in that length).

54. The exception referred to in paragraph 48 above relates to the collection of personal data by Experian from the Open Electoral Register. The statutory context to the Open Register means that data subjects who do not opt-out of it may for present purposes be taken to be aware that their data contained in the Open Register could be used and shared for marketing purposes[4] (even if they would not be aware that Experian in particular might have obtained it). Article 14(5)(a) does not apply (since data subjects do not have all the information required by Article 14). As to Article 14(5)(b), it is on balance disproportionate for Experian to notify individuals on the Open Register that it is processing their data. However, this exception only applies to use and sale by Experian of the Open Register alone, or data derived solely from the Open Register (such as date of births being deduced from comparing Open Registers). Such processing might include, for example, the use of the Open Register as a validation tool to check addresses. Where data from the Open Register is combined with other data (for example, where it is used to form part of a data subject profile, to fill 'gaps', or to otherwise supplement or be supplemented by other sources), the Commissioner considers that this is processing which goes beyond the reasonable expectation and understanding of the data subject based on the statutory notice provided to them. The proportionality assessment under Article 14(5)(b) therefore favours the notification of such processing: the processing falls within the scope of the reasoning

[4] The Commissioner sees no force, however, in any argument that the same reasoning should apply to any other public source from which personal data has been harvested, such as court judgments. While such data is publicly available, it is quite unlike the Open Electoral Register which has been made available so that data subjects may be the subject of direct marketing (amongst other reasons).

set out at paragraphs 43-53 above rather than within the exception set out earlier in the present paragraph.

Category C: Lawful Processing: Article 5(1)(a) and Article 6(1)

55. Experian has contravened Article 5(1)(a), in that the Commissioner is not satisfied that it has properly assessed the lawful basis of processing under Article 6(1) GDPR.

56. Experian processes all of the personal data it holds for direct marketing purposes on the basis of its legitimate interests. This includes data obtained from publicly available information, data drawn from its credit referencing business and data purchased from third party suppliers. However, those third party suppliers usually obtain that data directly from data subjects on the basis of their consent.

57. Experian has generally carried out legitimate interest assessments. In no instance shown to the Commissioner has any assessment concluded, or any decision been taken, that the balance of interests did not justify the processing (although Experian assert that products which do not satisfy compliance standards have not been proceeded with). In circumstances where a very large amount of personal data is being processed in highly targeted ways, and particularly where there are significant issues of non-transparency as set out above (as to which, see recital (47) GDPR), the Commissioner is not satisfied that Experian has correctly or properly concluded that it has a lawful basis for processing personal data. In her Preliminary Enforcement Notice, the Commissioner indicated to Experian that she would require that assessments of the balance of legitimate interests should be carried out afresh, in the light of the wider

matters set out in that Notice and the remedial work undertaken by Experian following the Audit and the Preliminary Enforcement Notice. The Commissioner notes that Experian's representations did not dispute the need to re-conduct those assessments in this context[5].

58. The various assessments carried out by Experian conclude that processing for profiling is not intrusive of privacy, and Experian repeats this in its representations. That approach is unjustified and indicative of a failure to properly balance the interests engaged. For example European data protection authorities have been clear for many years that profiling activity is likely to present a significant intrusion into the privacy of the data subject and the controller's interest will be overridden as a result.[6] See also in this regard recitals (60) and (70) GDPR. Experian's assessment has not reflected this guidance or the necessary degree of granularity and specificity to explain why a different conclusion is warranted. The Commissioner has explained in her own guidance that little weight can be attached to supposed benefit of the data subject consumer receiving direct marketing communications more 'appropriate' to them, when this is a consequence of processing and profiling to which they have not

[5] The Commissioner also notes the Article 29 Working Party Opinion 03/2013 on 'Purpose limitation' (WP 203) concerning the appropriate lawful bases "for tracking and profiling for purposes of direct marketing, behavioural advertisement [or] data-brokering", issued under the previous Directive, which provides that: "The second potential scenario is when an organisation specifically wants to analyse or predict the personal preferences, behaviour and attitudes of individual customers, which will subsequently inform 'measures or decisions' that are taken with regard to those customers. In these cases, free, specific, informed and unambiguous 'opt-in' consent would almost always be required, otherwise further use cannot be considered compatible. Importantly, such consent should be required, for example, for tracking and profiling for purposes of direct marketing, behavioural advertisement, data-brokering, location-based advertising or tracking-based digital market research." (p.46)

[6] See Article 29 Working Party Opinion 06/2014 on the 'Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' (WP 217); that Opinion remains of relevance even though it related to Directive 95/46/EC and not to the GDPR

consented. The Commissioner considers that it is unlikely that a controller will be able to apply legitimate interests for intrusive profiling for direct marketing purposes. This type of profiling is not generally in an individual's reasonable expectations and is rarely transparent enough. Nothing in the particular circumstances of Experian's processing warrants a different conclusion. Where profiling for direct marketing purposes is not intrusive, legitimate interests may still be used. Intrusiveness is necessarily a qualitative contextual assessment, based on matters such as:

- the qualities of the data being used (for example, Experian uses modelled data – which is likely to be less intrusive than direct behavioural or location-based tracking – but the type of data modelled, including predicted wealth and family background, can still be intrusive);
- the amount of data concerning an individual being used (intrusiveness can be cumulative, so the more attributes being predicted, the more likely the processing is to be intrusive); and
- the expectations of the individuals being profiled (feelings of intrusion are likely to increase where processing is surprising based either on the activity or the relationship with the controller).

59. In relation to personal data obtained from third party data suppliers, where those suppliers purport to rely upon consent, the Commissioner is of the view that Experian is unable to further process that data on the basis of its own legitimate interests. Where data is collected by a third party and shared with Experian for direct marketing purposes on the basis of consent, then the appropriate lawful basis for any subsequent processing for direct

marketing purposes will also be consent. The Commissioner makes the following points in this regard.

- Switching to legitimate interests as the basis for sharing or other onwards processing of data, after collection on the basis of consent, would mean the original consent was no longer specific or informed, and would misrepresent the degree of control and the nature of the relationship with the individual.
- GDPR recital (32) explains that consent should cover all processing activities carried out for the same purpose or purposes. Individuals cannot give valid consent for their data to be onward processed in a way that goes beyond the scope of their specific consent: if "consent" of this nature were valid, then this would be inconsistent with the requirement under the GDPR that consent must be specific and informed (see recital (32) and Article 4(11)).
- The right of data subjects to withdraw their consent in an effective manner, provided for in Article 7(3), would be materially undermined by the change of basis from consent to legitimate interests.
- Controllers with whom data will be shared on the basis of consent must be named when consent is collected, but sharing data on the basis of legitimate interest does not require this level of granularity; a transition from consent to legitimate interest-based processing could result in an individual's data being shared far more widely than they had anticipated when they consented.
- This misrepresentation and the impact on the effectiveness of consent withdrawal mechanisms would also cause a problem with the legitimate interest assessment balancing test, meaning that it would inevitably cause the balance to be against Experian.

60. In addition, the Commissioner's review of Experian's suppliers suggests that the consent being relied upon by those suppliers is insufficiently informed, specific and granular to meet the requirements of the GDPR. For example:

a. Requests for consent do not adequately describe the processing and sharing (and the intended recipients) at the point where consent is captured, but in second or subsequent layers;
b. Language is not clear, plain or easy to understand, but is highly euphemistic and does not focus on specific processing activities or outcomes to help inform individuals;
c. The data subject does not have granular options between the multiple direct marketing purposes described (e.g. prospecting, matching, appending, modelling and tracing for marketing).

Personal data provided to Experian which has been collected in a non-compliant manner cannot be lawfully processed by Experian on the basis of either Article 6(1)(a) or Article 6(1)(f).

61. In February 2020, Experian provided to the Commissioner a suite of new legitimate interest assessments (LIAs) for its direct marketing processing activity, having undertaken a thorough review with external challenge from its external solicitors. The Commissioner acknowledges the improvement in these assessments and the effort put into them. However, the assessments continue to reflect Experian's erroneous views concerning the limited intrusiveness of direct marketing processing, place a low value on the benefits and necessity of transparency, and in some cases rely on the ongoing use of legitimate interests as a lawful basis despite the collection of that

data on consent. The assessments cannot therefore be considered to be properly or lawfully balanced. This is so, even if the template followed by Experian in carrying out these LIAs is sound.

62. Relatedly, the Commissioner was concerned that in the course of her investigation she saw evidence that the data suppliers who supply Experian have privacy notices which themselves were not compliant with the GDPR and failed to set out equivalent levels of detail to Experian's own CIP (even prior to the necessary remedial work done to that notice). As set out above, it is not sufficient to comply with Article 14 that the suppliers have policies which simply link to Experian's own, given the extensive and intrusive nature of the processing. Some of the processing carried out by Experian on the data obtained by these suppliers would not be expected by data subjects, and compliance with Article 14 requires it to be drawn to their attention. Experian has represented to the Commissioner that it has conducted an audit of the privacy notices of its data suppliers, and reduced the number of those suppliers as a result. It re-audits every three months. Experian states that it has revisited its supplier questionnaires and enhanced them to address this issue. Experian has also informed the Commissioner that it will also update its terms and conditions with [redacted] to require the privacy notices of members to be similarly clear to the CIP, and will carry out six-monthly reviews of those privacy notices to ensure satisfactory compliance.

63. The Commissioner recognises that some work has been done by Experian. Although Experian does not say so in such terms, this work rather bears out the validity of the concerns expressed by the Commissioner in the Preliminary Enforcement Notice. There is no need for further enforcement action in relation to the actions

taken in connection with [redacted]. Although Experian has conducted an audit of its data suppliers, the Commissioner is not satisfied that the privacy information and data capture mechanisms of those suppliers are sufficient to meet the transparency and lawful basis obligations of the GDPR.

64. The Commissioner carried out a further review of two sample data supplier sites, in so far as these relate to Experian [redacted], subsequent to Experian's representations in response to the Draft Enforcement Notice dated 20 April 2020 and prior to the issue of this Notice. The Commissioner notes that the privacy policies for both [redacted] have changed in recent months and now purport to collect data once for multiple processing activities, some of which use the basis of consent (such as operating their own sites and marketing unrelated to Experian), and some of which use the basis of legitimate interests (specifically, the onward sharing of data with marketing services providers like Experian). In addition, new text on the data collection pages provides more detail about the activities of marketing services providers, and specifically names Experian. It is unclear to the Commissioner if Experian believes the collection of such data is now in compliance, and if so whether they believe the compliance to be retrospective (thereby justifying Experian's ongoing use of data collected under historical notices by third party suppliers). An analysis of the current and historical positions is therefore provided to address both scenarios.

65. The transparency of the *current collection model* exemplified by the [redacted] web page is undoubtedly improved, by bringing information about the onward sharing of information to the first layer and placing it near the submission button. The brief

paragraph summarises the profiling and analysis for direct marketing purposes reasonably cogently, albeit there is no unambiguous explanation of how many companies may receive submitted data. The second layer, more detailed privacy policy is somewhat improved (for example, there is a new retention section) but continues to lack detail, uses language that is unlikely to enlighten a lay audience, and requires an individual to scour multiple privacy policies to understand the likely impact of submitting their data. In addition, it appears likely that individuals will be confused about whether [redacted] is processing their submitted data on the basis of consent or legitimate interests; the second layer explains that [redacted] believe individuals have consented to certain activities (the use of their data for managing website membership, sending advertising from [redacted] and sending individuals' data to named third parties), but have not consented to the sharing of their data with marketing service providers like Experian – but that this sharing can be carried out on the basis of legitimate interests. One-off collection for multiple activities using different lawful bases is not prevented by GDPR, but such collection must be very clear about the degree of control being afforded to individuals about the use of their data, to avoid misrepresentation. At present, it seems likely in this situation that an individual could be confused about which marketing activities they had, or had not, consented to, and how much control they had over the onwards processing of their data. As stated above, misrepresentation of control will make subsequent LIAs (such as those of Experian) very hard to balance, even if subsequent transparency and Article 14 notices are acceptable.

66. *Historically*, the Commissioner had concerns about the collection mechanisms of both [redacted]; in both cases requests for consent to onward processing and disclosure to other

organisations were inadequate to constitute informed or specific consent under the GDPR. Privacy information was insufficiently clear to enable data subjects to grasp the substantial nature of the processing, or how widely their data might be shared. As with Experian's own privacy information, information that was likely to be surprising to data subjects was buried within long privacy notices or in second and subsequent layers. Data collected in this manner could not have been deemed compliant, and subsequent changes to privacy policies cannot retrospectively make compliant data that was collected in this fashion.

67. The Commissioner has not reviewed each of the websites (numbering, she estimates, potentially in excess of [redacted] such sites) that capture data which subsequently makes its way to Experian, because it is for Experian to evidence in line with the accountability principle in Article 5(2) that its processing is compliant with the GDPR. In the absence of evidence to that effect from Experian and the fact that the two example sites which the Commissioner has reviewed are still not compliant, the Commissioner considers it appropriate to make further requirements of Experian to ensure that data obtained from all of Experian's third party suppliers is either compliant or else not processed.

68. Experian does not in general process special category data, but the Commissioner identified certain categorisations used by Mosaic as amounting to special category data when appended to identifiable data subjects. In particular, the allocation by Mosaic of records to categories set by reference to ethnicity (e.g. 'Asian Heritage') constituted the processing of special category data. Experian had not considered or established whether it could satisfy any condition under Article 9 GDPR to process special

category data in this manner. In the light of this issue being identified by the Commissioner, Experian has addressed it by removing or amending such categories so that they did not include (and could not be taken to include) the processing of special category personal data. It follows that no enforcement action is required in this regard.

Category D: Article 21 GDPR

69. [redacted]

70. [redacted]

71. In the light of the Preliminary Enforcement Notice and the Audit, Experian has carried out remediation work to address the breaches related to Article 21 GDPR identified by the Commissioner. Having considered the steps taken, the

Commissioner is satisfied that no enforcement action in this respect is required in the light of Experian's co-operative and responsible reaction. The Commissioner reserves the right to review the practical operation of the changes made to address the breaches identified to ensure compliance.

Category E: Experian's Status as Controller

72. Experian has contravened the GDPR in that it has wrongly considered itself to be a data processor and not a controller in certain processing contexts, with the consequence that it has not addressed this processing in accordance with Article 5(1)(a) and the requirement of transparency.

73. [redacted]

74. Experian has submitted to the Commissioner that it is updating the terms and conditions it has with its clients to make sure that its retention of this supplied data is clear, and that it intends to

re-conduct a legitimate interests assessment. Experian has also submitted that it will separate the Link data cleansing tool into separate instances, one for each client. In this way, novel data supplied from that client will be used and accessible for that client only and not integrated into Experian's product more widely; Experian does not assume controllership of the new data. The Commissioner agrees that those are appropriate remedial steps and no enforcement action is required in those respects.

75. Some of the screening or directory enquiry datasets that Experian use have been acquired from third parties, such as the TPS, BT or Royal Mail, under licence. The Commissioner considers that in using these datasets to operate suppression and preference lists, Experian is processing the data in them for its own purposes and in the manner of its choosing, and is a controller. Experian agrees. In response to the Preliminary Enforcement Notice, Experian has explained that it has amended the CIP to explain the use of TPS and Royal Mail lists within the sources of data and that it intends to review its legitimate interests assessment in this respect. The Commissioner accepts that those steps are appropriate, and does not require any additional notification for compliance with Article 14 in the context of processing for the purposes of suppression where the individual has actively opted to be on such lists (as it would be unambiguously counter-productive) or directory enquiries. No enforcement action is required in this respect. Suppression lists created without the participation of the data subject (for example, created from comparisons of property sale websites) will still need to be notified in line with the preceding paragraphs.

Issue of the Notice

76. The Commissioner considers that the contraventions are significant ones which warrant enforcement action. Her reasons for this conclusion include that:

- An extremely large number of data subjects are affected.
- The nature of the processing is significant in privacy terms, including elements of profiling and collation of wide arrays of personal data from different sources. Experian's characterisation (in its representations) of its processing as being "not entirely privacy neutral" is something of an understatement. That there can be more intrusive forms of processing is indisputable, but not an answer to the scale and scope of Experian's processing.
- Even with an element of consumer-facing parts to its overall business, there is a significant element of Experian processing of personal data which is invisible to the data subject; i.e. most will not know that their data has been obtained by Experian and is being processed for direct marketing purposes.[7] Without that knowledge, data subjects are unable to consider the exercise of their rights under the GDPR to prevent that processing.
- At least to some extent, the scale and scope of Experian's business operating model appears dependent on the processing being invisible, in the sense that it relies on data subjects not being likely to exercise their rights to object to

[7] Experian makes reference in its representations to various publicity and advertising campaigns as part of a desire that the public understand that it holds and process 'Your data self'. The Commissioner is happy to recognise the work done by Experian in this respect, although its focus appears to be on the credit reference side of Experian's process and not on the extensive profiling for direct marketing. But even if those who watch the publicity are broadly aware that Experian may collect various sorts of data about various people, that does not equate to them understanding the full scale and scope of Experian's processing.

the processing so as to maintain the fullest coverage of the UK adult population possible.

- There is little or no wider public interest in Experian's processing beyond its own commercial interests, and the commercial interests of its third party clients. Commercial interests are valid interests, but a business cannot create an operating model based upon mass processing of personal data and then rely on that model to seek to avoid any of the requirements of the GDPR.
- The Commissioner originally commenced her investigation into processing by credit reference agencies in 2018. Although Experian has co-operated with the Assessment Notice and the Commissioner's investigation, and has made substantial attempts to revise its processing practices in the light of the GDPR, there remains regulatory and public concern about processing by data brokers such as Experian which has been justified by the Commissioner's investigative work.

77. The Commissioner considered, as she is required to do under section 150(2) DPA when deciding whether to serve an Enforcement Notice, whether any contravention has caused or is likely to cause any person damage or distress. The Commissioner considers that, for at least some data subjects, distress is likely in the present context. She does not accept Experian's assertion that its processing is "essentially anodyne". Mass processing of personal data for marketing purposes, without adequate transparency, is likely to lead to a significant number of data subjects receiving direct marketing which they did not expect to receive, and for some data subjects this is likely to cause distress. Further, where data is being used as part of an extensive exercise in profiling individuals and their tastes, without

data subjects being made aware that their data is being used in this way, then the Commissioner considers that it is likely that distress will be caused to data subjects: this is by reason of their perceived loss of control of their data, and their likely reaction to the failure of Experian to adhere to their expectations regarding the use of their data. This approach does not require the Commissioner to have received specific complaints from data subjects to this effect, but it accords with the Commissioner's own market research into how members of the public perceive the use of their data. A significant majority consider the sale of personal data, and the use of personal data to profile, in the offline marketing context, to be unacceptable.

78. Moreover, data subjects are, at the least, likely to be concerned about the processing of their personal data in the manner set out above, in circumstances where the nature of that processing is not clearly drawn to their attention. A controller cannot avoid enforcement action on the basis of an absence of complaints, if the absence of complaints is a result of data subjects being unaware of the processing in whole or in part because of the default of the controller in drawing that processing to the attention of the subject.

79. Furthermore, and in any event, the Commissioner considers that compliance with the principles in Article 5 and the Chapter III GDPR rights is a matter of central importance to data protection law. Even if a failure to comply has not, or is not likely, to cause any person damage or distress, the issue of this Enforcement Notice to compel compliance would nonetheless be an appropriate exercise of the Commissioner's enforcement powers.

80. The Commissioner has also had regard to the desirability of promoting economic growth and the potential impact her Notice might have on Experian's contribution to economic growth. However, she considers that the steps required on the part of Experian to bring its processing into compliance – even if they involve an element of cost to the business of the controller – are necessary and proportionate to ensure fair and lawful processing of very large amounts of personal data. A controller whose business model relies upon processing personal data must ensure that the model is a lawful one.

81. Experian argue in their representations that to take enforcement action against it would have anti-competitive results, where no action is taken against online data brokers, such that there will be adverse economic impacts on Experian. The Commissioner is not persuaded. It will always be possible for a controller faced with regulatory action to argue that requiring it to take steps to act within the law will cost it money, and to assert that others are also acting unlawfully. But good data protection compliance can increase the trustworthiness, and therefore profitability, of a brand; controllers should see the positives in compliance. Other controllers in other or linked industries may also become the subject of regulatory investigation and action on the part of the Commissioner in due course.

82. Having regard to the significant and multiple nature of the contraventions, the scale of the personal data being processed and the context in which it is processed, and the inability of the data subject to obtain clear information as to that processing reducing the effectiveness of their other rights under the GDPR, the Commissioner considers that this Enforcement Notice is the proportionate regulatory step to bring Experian into compliance.

83. In its representations, Experian sought to suggest that the time frame for compliance, as set out in Annex 1 to the Draft Enforcement Notice, was too short. The Commissioner had originally set time periods of two and three months for the requirements then imposed. Experian suggested that it needed no less than 19 months. The Commissioner considers that such a timescale is not in the interests of data subjects which this Notice seeks to protect and is inconsistent with the claimed desire of Experian to act compliantly with the legislation. The Commissioner has however taken full account of the points made by Experian and has sought to act proportionately by varying the periods for compliance to three and nine months respectively.

84. In deciding to issue this Enforcement Notice, the Commissioner has had regard to her 'Regulatory Action Policy'. It is to be noted that the circumstances specified in the Policy in which an Enforcement Notice may be issued are expressly described to be not exhaustive. The Commissioner considers that the contraventions found in this Notice are ones which show Experian failing to meet information rights obligations and are of a serious and ongoing nature. Such circumstances are, in her view, plainly within the scope of types of case the Policy anticipates will justify an Enforcement Notice.

85. She has also considered the issue of this Notice against her published approach to regulation during the COVID-19 pandemic. Some significant investigations, such as in relation to the adtech industry, were paused during the pandemic. The present Notice is not analogous to such investigations, which are expected to be resumed in any event. The Commissioner's consideration of Experian's processing, and her correspondence with Experian

about the issues identified in this Notice (and earlier iterations of this Notice), long pre-dates the pandemic and although the public health position further slowed the ability of both the Commissioner's officials and Experian to finalise this process, it could not justify an outright cessation. By 24 September 2020, the situation – including the adoption of new ways of working – had sufficiently developed to allow the Commissioner to announce resumptions of various areas of work and regulatory activity in any event[8].

86. The Commissioner has, however, sought and carefully considered the representations of Experian on the impact of the pandemic on its business in the context of the potential requirements of this Notice. Experian has argued that it is inappropriate for the Commissioner to seek to make it more difficult and expensive for Experian to conduct its business in the financial context of the pandemic; that this Notice will materially impair the ability of thousands of small and medium sized enterprises to recover from the pandemic; and that it will adversely affect competition in the marketing sector.

87. The Commissioner does not accept that the enforcement notice will have the extreme consequences asserted by Experian. She recognises that if Experian wishes to continue to process personal data in the same way as it has been doing, the requirements imposed by this Notice will come with a financial cost to it. That is, however, the cost of lawful processing, and results from Experian's own choices as to how it conducts its business.[9] She

[8] See the updated version of the ICO's regulatory approach in response to the coronavirus pandemic, available here: https://ico.org.uk/media/about-the-ico/policies-and-procedures/2617613/ico-regulatory-approach-during-coronavirus.pdf

[9] It is also plainly inconsistent for Experian on the one hand to insist that the Commissioner is wrong in her interpretation of the law in this Notice and on the other to claim that the Notice should not be issued because it would expose Experian to a risk of damages awards in civil claims for breach of the GDPR.

does not accept that this regulatory action will materially affect the wider UK economy, still less cause the wider detriment to a wide range of parties to whom the Notice is not directed. Experian's assertions in this regard are inherently implausible. In particular, they appear to depend upon an implicit assumption that no SME can survive without reliance on unlawful offline marketing. Nor does the Commissioner accept that this Notice will have anti-competitive effects; to the extent that Experian is one sector of the market and competitors in other sectors, including online marketing, have not yet been the subject of enforcement action that is simply an accident of timing and not of principle; the Commissioner's work in related areas of the market continues.

88. For the avoidance of doubt, the Commissioner has restricted this Notice to the most significant contraventions identified in her investigation. In relation to some of the matters set out above (see Category D and E above) the Commissioner has concluded that no regulatory action is required. She will continue to address other potential contraventions and matters of good practice in her reports to Experian arising out of her Assessment Notice and in other regulatory engagement. The Commissioner considers that this draws a proportionate line between matters requiring regulatory enforcement action and matters for which continued regulatory engagement with Experian is sufficient for the present.

Terms of the Notice

89. The Commissioner has decided to exercise her powers under section 149 DPA to serve an Enforcement Notice requiring Experian to take the specified steps to comply with the GDPR. The terms of the Notice are set out in Annex 1 of this Notice.

Consequences of Failing to Comply with the Notice

90. If a person fails to comply with an Enforcement Notice, the Commissioner may serve a penalty notice on that person under section 155(1)(b) DPA, requiring payment of a penalty in an amount up to 20 million Euros or 4% of annual worldwide turnover, whichever is the higher.

Right of Appeal

91. By virtue of section 162(1)(c) DPA there is a right of appeal against this Notice to the First-tier Tribunal (Information Rights). If an appeal is brought against this Notice, it need not be complied with pending determination or withdrawal of that appeal. Information about the appeals process may be obtained from:

First-tier Tribunal (Information Rights)
GRC Tribunals
PO Box 9300
Leicester
LE1 8DJ

Tel: 0300 1234504
Fax: 0870 7395836
Email: GRC@hmcts.gsi.gov.uk
Website: www.justice.gov.uk/tribunals/general-regulatory-chamber

92. Any Notice of Appeal should be served on the Tribunal within 28 calendar days of the date on which this Notice is sent.

Dated the 12th day of October 2020

Signed: .....

Elizabeth Denham
Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

ANNEX 1

TERMS OF THE PROPOSED ENFORCEMENT NOTICE

Experian shall within three months of the date of this Notice:

Category A

1) Revise the CIP to:
   a) set out clearly in one place and at the forefront of the privacy information an "at a glance" summary of the direct marketing processing that Experian undertakes, including what attributes (actual and modelled) Experian processes about individual data subjects;
   b) place information that is likely to surprise individuals (for example, that connect together multiple data sources to build a marketing profile) more prominently than in the third or fourth layers;
   c) include language concise, clear and not unduly euphemistic or industry-based language (such as "insight") to ensure it is intelligible to data subjects; and
   d) include intelligible information about each source of data (including modelled data), each use of data and the onward disclosure of data and illustrate them with examples and possible outcomes.
2) Cease using credit reference derived data for any direct marketing purposes except that requested by data subjects, including the screening out of individuals from marketing lists.

Category C

3) Delete any data supplied on the basis of consent which is now being processed on the basis of Experian's legitimate interests.

Experian shall within nine months of the date of this Notice and in the light of the actions taken above:

Category B

4) Directly provide all data subjects with an Article 14-compliant privacy notice (by mail or other acceptable means of communications) where Experian has acquired their personal data from any source other than the data subject, which clearly and directly informs the data subject that their personal data has been obtained by Experian for purposes which include direct marketing and the form that processing for marketing purposes takes, in terms and form consistent with paragraph 1) above (save that no notice is required to be sent where Experian's processing concerns only the retention or sale of the Open Electoral Register and no other processing of the personal data in that Open Register has occurred, or relates to the obtaining and use of directory enquiry databases like BT OSIS or suppression databases like the TPS).
5) Cease the processing of the personal data of any data subject to whom an Article 14-compliant notice is not sent.

Category C

6) Cease processing any personal data where the objective legitimate interest assessment cannot be said to favour the interests of Experian, having particular regard to the transparency of the processing and the intrusive nature of profiling.
7) In the case of all suppliers of personal data to Experian, review the compliance with the GDPR of the privacy notices and data capture mechanisms of those suppliers and collect data from only those suppliers where it is the case that:
   a) the suppliers' notices provide the same standard of transparency as the CIP,

b) the suppliers' consent capture mechanisms are sufficient to constitute valid consent (including being informed and specific) to the collection, disclosure and onward processing of the data; and
c) the suppliers' privacy information is clear and intelligible, with processing that the individual is unlikely to expect or would be surprised by to the fore and not buried in lengthy and jargon-heavy text.

8) Cease the processing of any personal data where there is insufficient evidence that it was collected in a compliant manner.