

DATA PROTECTION ACT 1998

SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER

MONETARY PENALTY NOTICE

To: Equifax Ltd

Of: Capital House, 25 Chapel St, Marylebone, London NW1 5DH

Introduction

1. The Information Commissioner ("the Commissioner") has decided to issue Equifax Ltd with a monetary penalty under section 55A of the Data Protection Act 1998 ("DPA").
2. The amount of the monetary penalty is **£500,000**.
3. The monetary penalty concerns a cyber attack which took place between 13 May and 30 July 2017, affecting data held by Equifax Inc, in the United States of America ("US") (the "data breach"). The affected data included personal data contained in up to 15 million unique records of UK individuals (the "UK data").
4. For the reasons set out below, the Commissioner finds that the UK data was controlled by Equifax Ltd and was processed by Equifax Ltd's parent company and data processor, Equifax Inc. In respect of the UK data, Equifax Ltd had failed to take appropriate technical and organisational measures against unauthorised and unlawful processing of that data. The Commissioner also finds that in respect of certain of the UK data, it

had been retained by Equifax Inc in the US for longer than was necessary for the purpose(s) for which it was transferred there.

5. The Commissioner's view is that, in all the circumstances, these failures constituted a serious contravention by Equifax Ltd of the fifth and seventh data protection principles ("DPP5" / "DPP7") in Schedule 1 to the DPA. The Commissioner has made a further finding that there was also a breach of the first data protection principle ("DPP1") in respect of how the data was handled, the second data protection principle ("DPP2") in respect of the purpose to process the personal data, and the eighth data protection principle ("DPP8") in relation to the transfer of the UK data to the US.
6. The Commissioner finds that the conditions for issuing a monetary penalty are satisfied, that it is appropriate to issue such a penalty in this case, and that the amount of £500,000 is reasonable and proportionate.
7. This Monetary Penalty Notice is served pursuant to section 55A of the DPA.

Legal framework

8. The DPA implements European legislation (Directive 95/46/EC) ("the Directive") aimed at the protection of the individual's fundamental right to the protection of personal data. The DPA must be applied so as to give effect to that Directive.
9. Equifax Ltd is a data controller for the personal data identified below. Section 4(4) of the DPA provides that, subject to section 27(1) of the DPA, it is the duty of a data controller to comply with the data protection

principles in relation to all personal data in respect of which he is the data controller.

10. Schedule 1 of the DPA contains the eight data protection principles. In the present case, the relevant principles are DPP1, DPP2, DPP5, DPP7 and DPP8, which stipulate as follows:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

*...
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.*

*...
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.*

*...
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.*

8. Personal data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

11. As regards DPP1, the interpretative provisions in Part II of Schedule 1 to the DPA provide:

1(1) In determining for the purposes of the first principle whether personal data are processed fairly, regard is to be had to the method by which they are obtained, including in particular whether any person from whom they are obtained is deceived or misled as to the purpose or purposes for which they are to be processed.

(2) Subject to paragraph 2, for the purposes of the first principle data are to be treated as obtained fairly if they consist of information obtained from a person who—

*(a) is authorised by or under any enactment to supply it, or
(b) is required to supply it by or under any enactment or by any convention or other instrument imposing an international obligation on the United Kingdom.*

2(1) Subject to paragraph 3, for the purposes of the first principle personal data are not to be treated as processed fairly unless—

(a) in the case of data obtained from the data subject, the data controller ensures so far as practicable that the data subject has, is provided with, or has made readily available to him, the information specified in sub-paragraph (3), and

(b) in any other case, the data controller ensures so far as practicable that, before the relevant time or as soon as practicable after that time, the data subject has, is provided with, or has made readily available to him, the information specified in sub-paragraph (3).

(2) In sub-paragraph (1)(b) "the relevant time" means—

*(a) the time when the data controller first processes the data, or
(b) in a case where at that time disclosure to a third party within a reasonable period is envisaged—*

(i) if the data are in fact disclosed to such a person within that period, the time when the data are first disclosed,

(ii) if within that period the data controller becomes, or ought to become, aware that the data are unlikely to be disclosed to such a person within that period, the time when the data controller does become, or ought to become, so aware, or

(iii) in any other case, the end of that period.

(3) The information referred to in sub-paragraph (1) is as follows, namely—

(a) the identity of the data controller,

(b) if he has nominated a representative for the purposes of this Act, the identity of that representative,

(c) the purpose or purposes for which the data are intended to be processed, and

(d) any further information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair.

3(1) Paragraph 2(1)(b) does not apply where either of the primary conditions in sub-paragraph (2), together with such further conditions as may be prescribed by the [F1 Secretary of State] by order, are met.

(2) The primary conditions referred to in sub-paragraph (1) are—

(a) that the provision of that information would involve a disproportionate effort, or

(b) that the recording of the information to be contained in the data by, or the disclosure of the data by, the data controller is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

4(1) Personal data which contain a general identifier falling within a description prescribed by the [F2 Secretary of State] by order are not to be treated as processed fairly and lawfully unless they are processed in compliance with any conditions so prescribed in relation to general identifiers of that description.

(2) In sub-paragraph (1) "a general identifier" means any identifier (such as, for example, a number or code used for identification purposes) which—

(a) relates to an individual, and

(b) forms part of a set of similar identifiers which is of general application.

12. As regards DPP2, the interpretative provisions in Part II of Schedule 1 to the DPA provide:

5 The purpose or purposes for which personal data are obtained may in particular be specified—

(a) in a notice given for the purposes of paragraph 2 by the data controller to the data subject, or

(b) in a notification given to the Commissioner under Part III of this Act.

6 In determining whether any disclosure of personal data is compatible with the purpose or purposes for which the data were obtained, regard is to be had to the purpose or purposes for which the personal data are intended to be processed by any person to whom they are disclosed.

13. As regards DPP7, the interpretative provisions in Part II of Schedule 1 to the DPA provide:

9. Having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to—

(a) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle, and

(b) the nature of the data to be protected.

10. The data controller must take reasonable steps to ensure the reliability of any employees of his who have access to the personal data.

11. Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller must in order to comply with the seventh principle—

(a) choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out, and

(b) take reasonable steps to ensure compliance with those measures.

12. Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller is not to be regarded as complying with the seventh principle unless—

(a) the processing is carried out under a contract—

(i) which is made or evidenced in writing, and

(ii) under which the data processor is to act only on instructions from the data controller, and

(b) the contract requires the data processor to comply with obligations equivalent to those imposed on a data controller by the seventh principle.

14. As regards DPP8, the interpretative provisions in Part II of Schedule 1 to the DPA provide:

13. An adequate level of protection is one which is adequate in all the circumstances of the case, having regard in particular to—

(a) the nature of the personal data,

(b) the country or territory of origin of the information contained in the data,

(c) the country or territory of final destination of that information,

(d) the purposes for which and period during which the data are intended to be processed,

(e) the law in force in the country or territory in question,

(f) the international obligations of that country or territory,

(g) any relevant codes of conduct or other rules which are enforceable in that country or territory (whether generally or by arrangement in particular cases), and

(h) any security measures taken in respect of the data in that country or territory.

14. *The eighth principle does not apply to a transfer falling within any paragraph of Schedule 4, except in such circumstances and to such extent as the Secretary of State may by order provide.*^[1]

15.

(1) Where—

(a) in any proceedings under this Act any question arises as to whether the requirement of the eighth principle as to an adequate level of protection is met in relation to the transfer of any personal data to a country or territory outside the European Economic Area, and

(b) a Community finding has been made in relation to transfers of the kind in question, that question is to be determined in accordance with that finding.

(2) In sub-paragraph (1) "Community finding" means a finding of the European Commission, under the procedure provided for in Article 31(2) of the Data Protection Directive, that a country or territory outside the European Economic Area does, or does not, ensure an adequate level of protection within the meaning of Article 25(2) of the Directive.

15. Section 55A of the DPA empowers the Commissioner to issue monetary penalties. The relevant provisions are as follows:

(1) The Commissioner may serve a data controller with a monetary penalty notice if the Commissioner is satisfied that—

(a) there has been a serious contravention of section 4(4) by the data controller,

(b) the contravention was of a kind likely to cause substantial damage or substantial distress, and

(c) subsection (2) or (3) applies.

(2) This subsection applies if the contravention was deliberate.

(3) This subsection applies if the data controller—

(a) knew or ought to have known —

(i) that there was a risk that the contravention would occur, and
(ii) that such a contravention would be of a kind likely to cause substantial damage or substantial distress, but

(b) failed to take reasonable steps to prevent the contravention.

¹ Schedule 4 to the DPA sets out the cases where DPP8 does not apply.

16. Regulation 2 of the Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010 prescribe that the amount of any penalty determined by the Commissioner must not exceed £500,000.
17. The Commissioner has issued and published statutory guidance under section 55C (1) of the DPA about the issuing of monetary penalties.²

Background to the contravention

18. Equifax Ltd is a major credit reference agency. It has been operating in the UK since 1990 and is a UK data controller. Equifax Ltd states that it has "*one of the largest sources of detailed consumer and business data in the UK.*"³
19. One of the products Equifax Ltd supplies to its clients is Equifax Identity Verifier ("EIV"). It describes this as "*the market leader in providing reliable, robust and instant customer validation and authentication.*"⁴ The product allows Equifax Ltd's clients to verify a consumer's identity online, over the telephone or in person and is used, for instance, to comply with anti-money-laundering requirements. In order to verify an individual's identity, the client enters that individual's personal information on the system, which is then checked against other sources of data held by Equifax Ltd.
20. Equifax Ltd has been supplying EIV in the UK since 2011. Initially, EIV was hosted by Equifax Inc in the US as the product was already operational there for US citizens at the time.

² Available at: <https://ico.org.uk/media/for-organisations/documents/1043720/ico-guidance-on-monetary-penalties.pdf>

³ See https://www.equifax.co.uk/about-equifax/company-profile/en_gb

⁴ See https://www.equifax.co.uk/business/equifax-identity-verifier/en_gb

21. In 2016, Equifax Ltd moved the EIV product to be hosted in the UK (except in relation to two clients). At this point all UK data (bar in relation to those two clients) should have been removed from the US environment or, at a minimum, a process by which this was to be undertaken should have been fully established and promptly initiated. However, some UK data stored on the US system was not deleted when migrating the product from the US to the UK (the "EIV dataset"). The Commissioner considers that the process for migrating this data to the UK, and its subsequent deletion in the US, was insufficient and/or not adequately effective.
22. The EIV dataset contained up to 15 million individual records containing personal data of UK data subjects, and was amongst the data compromised in the data breach:
 - (1) In respect of 19,993 UK data subjects, the following data was compromised: name, date of birth, telephone number and driving licence number.
 - (2) In respect of 637,430 UK data subjects the following data was compromised: name, date of birth and telephone number.
 - (3) In respect of up to 15 million UK data subjects the following data was compromised: name and date of birth.
23. Equifax Ltd subsequently acknowledged that another set of UK data was also being processed in the US by Equifax Inc as its data processor (the "GCS dataset") and that within this dataset, data relating to 27,047 UK individuals had also been compromised in the data breach. In respect of 12,086 UK individuals, the compromised data was the email address connected to their Equifax account in 2014. In respect of 14,961 UK

individuals, the compromised data was account information for Equifax's credit services and included data subjects' name, address, date of birth, username, password (in plaintext), secret question and answer (in plaintext), credit card number (obscured) and some payment amounts. The compromised personal data was held in a plaintext file, known as the "Standard Fraud Daily" report file ("the File"), which is described by Equifax Ltd as a 'snapshot in time' of the GCS dataset, as opposed to the actual database where the GCS dataset was held. However, the Commissioner observes that in order for Equifax to include actual passwords within the File, those passwords must logically either have been already stored in plaintext form, or Equifax was otherwise able to determine what those passwords were, despite the company's Cryptography Standard specifically requiring that passwords were to be stored in encrypted, hashed, masked, tokenised or other approved form.

24. The File was held in a fileshare, which was accessible by multiple users (including system administrators and middleware technicians), for the purposes of maintenance and/or the release of application code. The File contained 'live' data taken from the GCS dataset which was created for testing purposes, with the intention of eventually sending it to Equifax Ltd's Fraud Investigations Team in the UK.
25. Some of the UK data was stored together with US data, differentiated within the File only by an entry labelling it "GBR". Contrary to Equifax's applicable data handling standard, the File (which included "consumer-protected data" such as personal identifying information comprising names, dates of birth, etc.) was not encrypted. Equifax Ltd has stated that the File was used in order to perform password analysis for the purposes of fraud prevention. However, the Commissioner has seen no adequate evidence or explanation indicating that this was a valid reason for this data not being processed in accordance with Equifax's data

handling and cryptography standards, particularly given the existence of several other fraud prevention techniques in use at the time, none of which required personal data to be stored in plaintext form.

26. On 8 September 2017, Equifax Ltd notified the Commissioner that Equifax Inc had been subject to the data breach. As part of that data breach, Equifax initially considered that records of some 1.49 million UK data subjects had been lost. It only later emerged that the records of up to 15 million UK data subjects had been affected by the data breach to varying degrees (as described in paragraphs 22 and 23 above).
27. Equifax Inc informed Equifax Ltd of the data breach late on 7 September 2017, although (i) the data breach was first discovered by Equifax Inc on 29 July 2017, and (ii) Equifax Inc became aware that UK data might be affected in late August 2017. The data protection breach notification Equifax Ltd submitted to the Commissioner on 8 September 2017 stated that *"the data elements potentially accessed ... do not include residential addresses or any financial information."* It later emerged, however, that for a small subset of individuals (the 14,961 individuals whose data was part of the GCS dataset, as described in paragraph 23 above) passwords and obscured financial information were also compromised.
28. Following the data breach, on 2 August 2017, Equifax Inc engaged the services of a specialist IT security company ("Mandiant") to provide incident response services, help contain the consequences of the breach and carry out an investigation.
29. The documentation Equifax Ltd has provided to the Commissioner (which include reports by Equifax's and Mandiant's forensic investigators and the public record of the statement given to the US Subcommittee on Digital Commerce and Consumer Protection on 3 October 2017 by Equifax Inc's then-CEO) and its subsequent representations, made in

response to the Notice of Intent issued by the Commissioner 21 May 2018, suggest that:

- (1) The attack exploited a vulnerability in the Apache Struts 2 web application framework that Equifax Inc used in its consumer-facing online disputes portal in the US. The vulnerability, CVE 2017-5638, was disclosed to Equifax Inc on 8 March 2017 by the US Department of Homeland Security Computer Emergency Readiness Team ("US CERT"). It was given a score of 10.0 on the Common Vulnerability Scoring System ("CVSS") Calculator maintained at the National Vulnerability Database of the US National Institute of Standards and Technology⁵. A CVSS score of 10.0 is the highest score, indicating a critical vulnerability that requires immediate attention. US CERT informed Equifax Inc of the need to patch the vulnerability concerned⁶. On 9 March 2017, Equifax Inc disseminated US CERT's notification internally among key personnel responsible for installations of Apache Struts within its web estate. However, the particular installation on the consumer-facing disputes portal was not identified and was therefore not patched;
- (2) The first evidence of interaction using the vulnerability occurred on 10 March 2017, with the first evidence of an attacker accessing files or sensitive information on the Equifax Inc system being recorded on 13 May 2017;
- (3) On 15 March 2017, Equifax Inc instructed its information security department to run scans of its network to identify any other systems and services that were subject to the same

⁵ <https://nvd.nist.gov/vuln/detail/CVE-2017-5638>

⁶ <https://investor.equifax.com/news-and-events/news/2017/09-15-2017-224018832>

vulnerability. These scans did not identify the vulnerability within the consumer-facing disputes portal, meaning that it remained at risk after the patching process was undertaken;

- (4) On 29 July 2017 the Equifax Inc security team observed suspicious network traffic, which led to the attack being discovered and the affected system being taken offline on 30 July 2017;
 - (5) Unauthorised access took place between 13 May 2017 and 30 July 2017;
 - (6) In total the personal data of some 146 million individuals in the US was compromised in the attack, as well as personal data of individuals in Canada and in the UK.
 - (7) The affected UK data comprised records relating to up to 15 million UK data subjects, dating from between 2011 and 2016, which were compromised to varying degrees, as stated in paragraphs 22-23. As regards the EIV data, for the majority of data subjects their name and date of birth was lost. In respect of some 657,423 individuals other identifiers (including telephone numbers and driving licence numbers for some) were compromised. As regards the GCS dataset, personal data, including name, address, date of birth, username, password (in plaintext), secret question and answer (both in plaintext), credit card number (obscured) and some payment amounts, of 14,961 UK data subjects were also compromised.
30. In response to an Information Notice dated 13 September 2017 and a number of further enquiries as well as in its representations made in response to the Notice of Intent issued by the Commissioner 21 May

2018, Equifax Ltd provided the Commissioner with additional information about this matter. The Commissioner investigated and the outcome of this investigation is as follows.

The contravention

31. Based on the factual matters set out above, the Commissioner's view is that at the relevant times Equifax Ltd contravened DPP5 (as well as DPP1 and DPP2), DPP7 and DPP8 in the manner set out below.
32. As regards DPP5:
 - (1) Upon the migration of EIV from the US to the UK (bar in respect of two clients of Equifax Ltd), it was no longer necessary to keep any of the EIV dataset, including in particular the compromised UK data, on the US system. Despite this, the relevant EIV dataset was not deleted in full from the US environment and/or the migration process was inadequate in this respect.
 - (2) In respect of the GCS dataset stored on the US system, Equifax Ltd did not appear to be sufficiently aware of the purpose for which it was being processed until after the breach. Absent any lawful purpose to process such data, it was not necessary to keep it. The purpose(s) for continued processing of that data should have been properly ascertained and, failing that, the data should have been deleted.
 - (3) Equifax Ltd failed to adequately follow up or check to ensure that all relevant UK data had been removed from the US environment or to have in place an adequate process to ensure this was done.

33. The aforesaid failures in relation to the GCS dataset also amount to a breach of DPP1 in that the relevant data was not being processed fairly and lawfully and a breach of DPP2 in that the relevant data was not being processed for any specified and lawful purpose at the material time.
34. Equifax subsequently submitted that it relied upon consent as defined in Schedule 2 Paragraph 1 of the DPA for processing certain personal data from the GCS dataset, specifically the creation of the File for the purposes of fraud prevention. While the DPA does not define consent, Article 2(h) of the Directive states that "*the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.*" Equifax suggested that informing data subjects that their passwords would be stored in plaintext form would have created a security risk. The Commissioner's view is that this type of processing activity was an inappropriate security risk, particularly given the state of the art and costs of implementation as regards appropriate technical measures to protect personal data, the resources available to an organisation of Equifax's size, and the nature of the processing it undertook. Especially in the absence of any stated good reason, data subjects could not have anticipated that the processing of their data would involve the storage of passwords in plaintext form, in breach of the company's Cryptography Standard. Having not been provided with the relevant information, any consent given by data subjects could not be regarded as being adequately specific and/or informed, as required under the Directive. On that basis, the Commissioner's assessment is that any consent relied upon by Equifax was invalid in this context, thereby amounting to a contravention of DPP1 in that the data was not fairly and lawfully processed.

35. As regards DPP7, the material submitted by Equifax Ltd has informed the Commissioner's assessment of the technical and organisational measures that were in place at the material time. The Commissioner's view is that there was a breach of DPP7, for the following reasons which include but are not limited to:

- (1) As described above, the data breach compromised the personal data of up to 15 million individuals in the UK.
- (2) Equifax Ltd did not undertake an adequate risk assessment(s) of the security arrangements put in place by Equifax Inc before transferring data to it and/or following the transfer.
- (3) The Data Processing Agreement 2014 between Equifax Ltd (as a data controller) and Equifax Inc (as a data processor) dated 23 October 2014 was inadequate in that it (i) failed to provide appropriate safeguards including but not limited to security requirements; and (ii) failed to incorporate the required standard contractual clauses.
- (4) Amongst others, Equifax Ltd has been unable to provide to the Commissioner the original Annex B to Schedule 2 of the 2014 agreement (containing the standard contractual clauses), which is stated to contain the relevant technical and operational security measures to be maintained by Equifax Inc. A Variation Agreement was entered into between Equifax Ltd and Equifax Inc on 2 February 2016 which included a new Annex B stating:

"Description of the technical and organisational security measures implemented by the data importer in accordance with Clause 4(d) and 5(c) (or documentation/legislation attached):

Industry-leading technical and organisational security measurers: the data importer is a leading credit reference agency with market-leading positions in a number of territories worldwide. It deploys extensive technical and organisational security measures to achieve robust information security and management practices. The data importer will apply the full range of corporate policies and procedures to the personal data."

- (5) The Data Processing Agreement 2017 (dated 28 February 2017) between Equifax Ltd (as a data controller) and Equifax Inc (as a data processor) was also inadequate in that it failed to provide adequate safeguards / security requirements.
- (6) Despite having clear contractual permission to do so, Equifax Ltd did not carry out appropriate audits of Equifax Inc and failed to carry out adequate checks on Equifax Inc to ensure it complied with the relevant security requirements.
- (7) Equifax Ltd failed to ensure adequate security measures were in place and/or to notice or address that Equifax Inc had failed to take such measures, including:
 - i. Not adequately encrypting all personal data held on its system;
 - ii. Not adequately protecting user passwords. Equifax Ltd has submitted to the Commissioner that user passwords for the GCS dataset were stored in a plaintext file for the purposes of fraud prevention and password analysis. The Commissioner does not accept this is a valid reason for storing personal data in plaintext, particularly as the

same aim may be achieved by other means that do not require storage of personal data in plaintext form and that Equifax has subsequently ceased the practice of storing passwords in plaintext whilst still being able to achieve its fraud prevention aims;

- iii. Failing to address known IT vulnerabilities, including those that had been identified and reported at a senior level, by promptly identifying and applying appropriate patches to all vulnerable systems / parts of the system;
- iv. Not having fully up-to-date software;
- v. Failing to undertake sufficient and/or sufficiently regular system scans, and/or using inadequate scanning tools;
- vi. Failing to ensure appropriate network segregation;
- vii. Permitting accounts to have more permissions than needed;
- viii. Storing service account passwords in plaintext within files and allowing such files to be accessed by staff; and
- ix. Failing to ensure that other technical measures provided appropriate protection (particularly as regards exploitation of the Apache Struts vulnerability), due to an expired certificate in an SSL decryptor which prevented traffic being properly checked by its Intrusion Prevention System. The certificate expired in January 2016 and was not fixed until July 2017. Equifax has provided no adequate reason why this expired certificate was not detected prior to the data breach or why it went undetected for this amount of time.

- (8) Equifax Ltd's processes for keeping track of personal data were deficient in relation to both the EIV dataset and GSC dataset, allowing personal data to remain on a system based overseas without having an identified lawful purpose for its (continued) processing.
- (9) Communications between Equifax Ltd and Equifax Inc were inadequate, as evidenced by the delay of over a month between Equifax Inc becoming aware of the data breach and Equifax Ltd being informed of it. Even in respect of the loss of UK data, Equifax Inc became aware of this at least over a week before Equifax Ltd was informed (and then took steps to inform the affected data subjects and the Commissioner). This failure to communicate in a timely manner suggests that communications procedures were inadequate and/or not followed.
36. Having regard to the state of technological development, the cost of implementing any measures, the nature of the relevant personal data and the harm that might ensue from its misuse, the Commissioner's view is that Equifax Ltd contravened DPP7 in respect of the data processing arrangements applicable to EIV and GCS datasets at the relevant time.
37. In the Commissioner's view, each of the inadequacies listed above would have constituted a contravention of DPP7. The Commissioner has, however, assessed the arrangements in the round: on that cumulative basis, the Commissioner's view is that there was a contravention of DPP7 in this case.
38. As regards DPP8:

- (1) The US is a third country outside the European Economic Area, so that transfers of personal data to the US are prohibited by DPP8 unless one of the derogations in Schedule 4 applies; on the facts, no derogations applied.
- (2) The Data Processing Agreement 2014 between Equifax Ltd (as a data controller) and Equifax Inc (as a data processor), was inadequate in that it failed to incorporate the required standard contractual clauses as a separate agreement and/or to provide appropriate safeguards for data transfers outside the EEA.
- (3) The Data Processing Agreement 2017 between Equifax Ltd (as a data controller) and Equifax Inc (as a data processor) was inadequate in that it failed to provide appropriate safeguards for data transfers outside the EEA.

39. It is the Commissioner's view that the aforesaid breaches of DPP7 and/or DPP8 also amount to a breach of DPP1, in that the relevant data was not being processed fairly and lawfully.

The issuing of a monetary penalty

40. The Commissioner's view is that the conditions for issuing a monetary penalty under section 55A have been met in this case.
41. The Commissioner considers that this contravention was serious, in that:
 - (1) Equifax Ltd contravened multiple data protection principles.
 - (2) The contravention entailed several systemic inadequacies in Equifax Ltd's technical and organisational measures for the

safeguarding of the relevant personal data. Cumulatively, this multi-faceted contravention was extremely serious.

- (3) A number of the inadequacies related to significant measures needed for a robust data management system, as outlined above.
- (4) The multiple organisational inadequacies were particularly problematic in light of, *inter alia*, the nature of Equifax Ltd's business, the volume of personal data being processed, and the number of data subjects involved.
- (5) The Commissioner has not received a satisfactory explanation for those individual and cumulative inadequacies.
- (6) At least a number of the inadequacies appear to have been in place for a long period of time without being discovered or addressed.
- (7) The inadequacies put the personal data of millions of data subjects at risk.
- (8) The period of vulnerability for the affected UK data extended over an extended period of time and the data breach was not detected promptly. It was not reported to the Commissioner until over two months after the event.
- (9) In respect of the UK records that were compromised, there were and remain significant opportunities for misuse. The relevant personal data is liable to be useful to scammers and fraudsters.

42. The Commissioner considers that this contravention was of a kind likely to cause substantial damage or substantial distress, in that:

- (1) Given the scope of the data held by Equifax Ltd, in many cases the individuals whose data was compromised would not have been aware that Equifax Ltd was processing their personal data. In those circumstances, learning about the data breach 'out of the blue' is likely to have caused them particular distress.
- (2) The loss of their personal data by a credit rating agency is also liable to cause individuals particular distress because of the nature of its business. For instance, affected individuals are likely to fear (rightly or wrongly) that their credit rating may be adversely affected as a result of the misuse of the compromised data.
- (3) As a result of the inadequacies outlined above, some of the relevant personal data had the potential to be misused in furtherance of fraud and/or other criminal activity. Individuals whose driving licence numbers (contained in the EIV dataset) / passwords, secret questions and answers, and financial information (contained in the GCS dataset) were lost are at particular risk of becoming the victims of criminal activity exploiting the data breach.
- (4) Such activity is likely to result in at least some affected data subjects suffering serious harm, such as becoming victims of identity theft and/or providing their bank details to scammers and/or being defrauded and/or having their bank accounts used for money laundering. Those consequences would constitute substantial damage.

- (5) The very significant scale of the data breach is liable to undermine trust in the wider financial system.
43. The Commissioner considers that Equifax Ltd knew or ought reasonably to have known that there was a risk that the contravention would (a) occur, and (b) be of a kind likely to cause substantial damage or substantial distress. She further considers that Equifax Ltd failed to take reasonable steps to prevent such a contravention, in that:
- (1) Equifax Ltd is a large, well-resourced and experienced data controller. It should have been aware of the risks entailed by the inadequate procedures outlined above. It should have appreciated that misuse of the relevant personal data was likely to cause substantial damage or distress.
 - (2) Equifax Ltd had ample opportunity over a long period of time to ascertain / ensure the implementation of appropriate technical and organisational measures in respect of EIV, but it failed to do so. For example, it failed to put in place appropriate audits of its data processor and failed to ensure that data was fully deleted from the US environment upon the migration to the UK.
 - (3) Equifax Ltd failed to undertake adequate risk assessment(s) and/or, where risks were identified, failed to address these sufficiently promptly and effectively.
 - (4) Communication and notification procedures were deficient, engendering avoidable delay in notifying and responding to the data breach after its occurrence.

The Commissioner's decision to impose a monetary penalty

44. The Commissioner's view is therefore that the statutory conditions for issuing a monetary penalty have been met in this case. She has considered all the circumstances and has reached the view that it is appropriate to issue a monetary penalty in this case.
45. That view is based on the multiple, systemic and serious inadequacies identified above in respect of the way in which Equifax Inc processed data on behalf of Equifax Ltd and Equifax Ltd's failure to adequately address these shortcomings / ensure they were remedied. The Commissioner has also considered the importance of deterring future contraventions of this kind, both by Equifax Ltd and by others. The Commissioner considers that this objective would be furthered by the issuing of a monetary penalty in this case.
46. The Commissioner has taken into account the following mitigating features of this case:
- The relevant data was, for the most part, not of itself highly sensitive in terms of its impact on data subjects' privacy;
 - The affected data subjects, as well as Equifax Ltd, have been the victim of the malicious actions of third party individuals;
 - Equifax Ltd proactively reported this matter to the Commissioner, promptly after learning about it from Equifax Inc, albeit a significant time after the actual data breach;
 - Equifax Ltd deleted at least some of the data remaining in the US environment following migration of EIV to the UK;

- Equifax Ltd and Equifax Inc took steps to minimise potentially harmful consequences such as engaging specialist IT security experts to manage the data breach, offering free credit monitoring services to UK data subjects affected by the breach, and working with the relevant regulators in the US, Canada, and the UK; and
- Equifax Ltd and Equifax Inc have implemented certain measures to prevent the recurrence of such incidents, for example Equifax Inc has increased system scanning capability and is now storing passwords within a cryptographic hash value, whilst strengthened procedures are now in effect.

47. The Commissioner has also taken into account the following aggravating features of this case:

- The security breach impacted many more individuals than just the UK data subjects. 146 million data subjects' personal data was compromised and the data of millions more was put at risk;
- Those risks appear to have persisted for a prolonged period of time given the systemic inadequacies identified above;
- Some of the failures concern failures to identify / ensure appropriate security measures such as implementation of patches and the encryption of personal data and the appropriate securing of passwords;
- The data breach exploited a known vulnerability and therefore could potentially have been prevented. In particular, the security breach arose out of a failure to implement a patch to the affected system(s) which it failed to identify as vulnerable; and
- Equifax Ltd's contractual arrangements with Equifax Inc were inadequate in material respects.

Conclusion and amount of penalty


48. The Commissioner confirms that she has taken account of Equifax Ltd's written submissions in response to her Notice of Intent.
49. Notwithstanding those submissions, the Commissioner has decided that she can and should issue a monetary penalty in this case, for the reasons explained above.
50. The Commissioner has also taken into account her underlying objective in imposing a monetary penalty notice, namely to promote compliance with the DPA. She considers that, given the nature, seriousness and potential consequences of the contravention arising in this case, that objective would not be adequately served by an unduly lenient penalty.
51. The Commissioner has considered evidence of Equifax Ltd's financial position. She does not consider that the payment of a penalty of the above amount would cause Equifax Ltd undue hardship.
52. Taking into account all of the above, the Commissioner has decided that a penalty in the sum of **£500,000 (Five hundred thousand pounds)** is reasonable and proportionate given the particular facts of the case and the underlying objective in imposing the penalty.
52. The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by **19 October 2018** at the latest. The monetary penalty is not kept by the Commissioner but will be paid into the Consolidated Fund which is the Government's general bank account at the Bank of England.

53. If the Commissioner receives full payment of the monetary penalty by **18 October 2018** the Commissioner will reduce the monetary penalty by 20% to **£400,000 (Four hundred thousand pounds)**. However, you should be aware that the early payment discount is not available if you decide to exercise your right of appeal.
54. There is a right of appeal to the First-tier Tribunal (Information Rights) against:
- a) the imposition of the monetary penalty and/or;
 - b) the amount of the penalty specified in the monetary penalty notice.
55. Any notice of appeal should be received by the Tribunal within 28 days of the date of this monetary penalty notice.
56. Information about appeals is set out in Annex 1.
57. The Commissioner will not take action to enforce a monetary penalty unless:
- the period specified within the notice within which a monetary penalty must be paid has expired and all or any of the monetary penalty has not been paid;
 - all relevant appeals against the monetary penalty notice and any variation of it have either been decided or withdrawn; and

- the period for appealing against the monetary penalty and any variation of it has expired.

58. In England, Wales and Northern Ireland, the monetary penalty is recoverable by Order of the County Court or the High Court. In Scotland, the monetary penalty can be enforced in the same manner as an extract registered decree arbitral bearing a warrant for execution issued by the sheriff court of any sheriffdom in Scotland.

Dated the 19th day of September 2018

Signed ..  ..

Elizabeth Denham
Information Commissioner

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

ANNEX 1

SECTION 55 A-E OF THE DATA PROTECTION ACT 1998

RIGHTS OF APPEAL AGAINST DECISIONS OF THE COMMISSIONER

1. Section 48 of the Data Protection Act 1998 gives any person upon whom a monetary penalty notice or variation notice has been served a right of appeal to the First-tier Tribunal (Information Rights) (the 'Tribunal') against the notice.

2. If you decide to appeal and if the Tribunal considers:-
 - a) that the notice against which the appeal is brought is not in accordance with the law; or

 - b) to the extent that the notice involved an exercise of discretion by the Commissioner, that she ought to have exercised her discretion differently,

the Tribunal will allow the appeal or substitute such other decision as could have been made by the Commissioner. In any other case the Tribunal will dismiss the appeal.

3. You may bring an appeal by serving a notice of appeal on the Tribunal at the following address:

GRC & GRP Tribunals
PO Box 9300
Arnhem House
31 Waterloo Way
Leicester
LE1 8DJ

- a) The notice of appeal should be sent so it is received by the Tribunal within 28 days of the date of the notice.
 - b) If your notice of appeal is late the Tribunal will not admit it unless the Tribunal has extended the time for complying with this rule.
-
4. The notice of appeal should state:-
- a) your name and address/name and address of your representative (if any);
 - b) an address where documents may be sent or delivered to you;
 - c) the name and address of the Information Commissioner;
 - d) details of the decision to which the proceedings relate;
 - e) the result that you are seeking;
-
- f) the grounds on which you rely;
 - g) you must provide with the notice of appeal a copy of the monetary penalty notice or variation notice;
 - h) if you have exceeded the time limit mentioned above the notice of appeal must include a request for an extension of time and the reason why the notice of appeal was not provided in time.

5. Before deciding whether or not to appeal you may wish to consult your solicitor or another adviser. At the hearing of an appeal a party may conduct his case himself or may be represented by any person whom he may appoint for that purpose.

6. The statutory provisions concerning appeals to the First-tier Tribunal (Information Rights) are contained in sections 48 and 49 of, and Schedule 6 to, the Data Protection Act 1998, and Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules 2009 (Statutory Instrument 2009 No. 1976 (L.20)).

