FINANCIAL CONDUCT AUTHORITY

12 Endeavour Square
London
E20 1JN

Tel: +44 (0)20 7066 1000
Fax: +44 (0)20 7066 1099
www.fca.org.uk

FINAL NOTICE

To: **Equifax Limited**

Reference Number: **739000**

Address: **1 Angel Court, London EC2R 7HJ**

Date: **3 October 2023**

1. ACTION

1.1. For the reasons given in this Final Notice, the Authority hereby imposes on Equifax Limited ("Equifax Ltd") a financial penalty of **£11,164,400** pursuant to section 206 of the Act.

1.2. Equifax Ltd agreed to resolve this matter and qualified for a 30% (Stage 1) discount under the Authority's executive settlement procedures. Were it not for this discount, the Authority would have imposed a financial penalty of **£15,949,200** (before 30% discount) on Equifax Ltd.

2. SUMMARY OF REASONS

2.1. Equifax Ltd is a credit reference agency and data, analytics and technology business. Equifax Ltd's business model is dependent on holding and analysing large volumes of data. The data Equifax Ltd holds is personal, valuable to others and requires protection.

2.2. In 2017, Equifax Ltd's parent company, Equifax Inc, was the subject of one of the largest cybersecurity incidents resulting in unauthorised access to personal data in history. The cybersecurity incident affected not only Equifax Inc, but Equifax Ltd and Equifax Inc's Canadian subsidiary. It exposed millions of US, UK and Canadian citizens to the risk of financial crime. More precisely, intruders obtained the personal data of approximately 147.9 million individuals in the US; approximately 13.8 million individuals in the UK; and 19,000 individuals in Canada. The cyber-attack and unauthorised access to data was foreseeable and entirely preventable.

2.3. Intruders were able to access UK consumer data on Equifax Inc's servers in Alpharetta, Georgia because Equifax Ltd transferred UK consumer data to Equifax Inc to process for two Equifax Ltd products. The data was vulnerable because Equifax Ltd failed to put in place an appropriate framework for monitoring and managing the security of the UK consumer data it had outsourced for processing to Equifax Inc. Following the cybersecurity incident, Equifax Ltd published several public statements regarding the impact of the Incident on UK consumers which did not meet the Authority's requirements in relation to fair, clear and not misleading communications.

2.4. A timeline of key events is set out below.

Date	**Event**
10 March 2017 - 29 July 2017	Intruders scan Equifax Inc's computer systems for vulnerabilities and start accessing data from Equifax Inc's servers. Equifax Inc detects the unauthorised data access on 29 July 2017 and secures its systems.
23 August 2017 - 29 August 2017	Equifax Inc becomes aware that a database table containing UK consumer data could have been involved in the Incident. By 29 August 2017, Equifax Inc determines that UK consumer data may have been accessed in the Incident.
1 September 2017	The Security Executive is informed about the Incident. The Security Executive has told the Authority that he was told he would be dismissed if he asked further questions or informed anyone else about the Incident. He remains silent.
7 September 2017	Equifax Inc informs Equifax Ltd about the Incident. This notification occurs approximately five minutes before Equifax Inc announces the Incident to the public at 21:30 BST. The information came, in the words of a Senior Executive of Equifax Ltd, as "*a bad surprise*". The same evening Equifax Ltd's Board directed its compliance officer to notify the Authority in the morning.
8 September 2017	The Authority learns about the Incident through a press report and contacts Equifax Ltd to ask questions about the UK impact of the Incident. Equifax Ltd is unable to answer the Authority's questions because it does not have the information.
7 September 2017 - May 2018	The volume of complaints soon overwhelms Equifax Ltd and, to help it process the complaints, it stops key processes designed to check the quality of the complaints handling team's work during this period.
From 15 September 2017	Equifax Ltd publishes several public statements regarding the impact of the Incident on UK consumers which do not meet the Authority's requirements. Notably, Equifax Ltd does not take appropriate steps to correct certain public statements when it becomes apparent that the language is being interpreted in an inaccurate way.

2.5. Firms regulated by the Authority need to have effective cyber security arrangements to protect the personal data they hold. An essential element of this is keeping systems and software up to date and fully patched to prevent unauthorised access by increasingly sophisticated threat actors. Where the processing of data is outsourced, including to an intra-group company, firms regulated by the Authority remain responsible for ensuring that all regulatory requirements are met. This means that where an FCA authorised firm outsources the processing of data it must exercise appropriate oversight over outsourced functions. Equifax Ltd failed to put in place an appropriate framework for monitoring and managing the security of the UK consumer data where it had outsourced the processing of that data to Equifax Inc. Notably, prior to the Incident, Equifax Ltd was aware of serious security patching problems at Equifax Inc but failed to take action in response.

2.6. Additionally, when an FCA authorised firm becomes aware of a data breach, it is essential that the firm pays due regard to the interests of customers and treats them fairly. This includes promptly notifying affected individuals about the breach in a way which is fair, clear and not misleading and implementing fair complaints handling procedures. Contrary to these requirements, Equifax Ltd's outsourcing arrangements with Equifax Inc resulted in delays in obtaining information that it needed in order to notify affected UK consumers. Further, following the Incident, Equifax Ltd exposed consumers to unfair treatment by ceasing vital quality assurance checks on its complaints handling processes and publishing several public statements about the impact of the Incident on UK consumers which did not meet the Authority's requirements.

2.7. The data accessed in the Incident included UK consumers' names, DOBs, phone numbers, Equifax membership login details, partially exposed credit card details, and residential addresses. In total, records relating to a maximum number of 13,764,291 UK consumers were accessed without authorisation in the Incident. However, it took Equifax Ltd many months to establish this number. Whilst Equifax Ltd's investigations were ongoing, its understanding, and therefore the information it gave to the Authority, involved different categories of data and different numbers of people affected. The table below summarises the data accessed in the Incident and the number of people affected.

Data accessed	**Number of people affected**
Name, DOB, phone number, Equifax membership login details (username and password) with secret Q&A and partially exposed credit card details, and residential addresses	14,961
Name, DOB, Phone number, and Driving Licence number	28,649
Name, DOB, email address and phone number	12,086
Name, DOB, phone number	1,218,909
Name, DOB, mobile and/or landline phone number (where the number was also listed on a publicly available commercial directory)	166,741
Name and DOB	12,322,945

Data accessed	Number of people affected
TOTAL	**13,764,291**

Principle breaches

2.8. Equifax Ltd's breaches of the Authority's Principles of Businesses are summarised below and fully in Section 5 of this Notice.

Principle 3 breaches

2.9. Principle 3 requires a firm to take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems. Equifax Ltd breached Principle 3 because:

(1) Equifax Ltd failed to put in place an appropriate risk management framework that allowed it to identify, manage, monitor, and mitigate the risks inherent in outsourcing the processing of data to its parent, Equifax Inc. Most significantly:

(a) Equifax Ltd approved a risk framework in November 2015 which was deficient because it failed to identify the risks inherent in the transfer, processing, and storage of UK consumer data to Equifax Inc, an intra-group outsourced service provider. Its Outsourcing Policy, introduced in December 2015, also failed to address these risks. There were specific risks that Equifax Ltd should have identified and sought to mitigate. In particular:

(i) Equifax Ltd was subject to the Equifax Security Incident Handling Policy & Procedures ("SIHPP"). This meant that, in the event of a security breach affecting data processed and stored by an intra-group company, there was a risk that the interests of other parts of the Equifax group could be placed above the interests of Equifax Ltd.

(ii) The Security Executive that was responsible for Equifax Ltd's security function reported to Equifax Inc's global security executive, further contributing to the risk in (i) above.

(iii) There were also risks common in many cases of intra-group outsourcing, including that known weaknesses at the group entity level would not be treated by Equifax Ltd with the same degree of seriousness as would be the case if the outsourcing had been to a third party, and that the risks associated with the outsourced processing of data by Equifax Inc would not be managed with the degree of rigour required.

(b) All of these risks crystallised in the Incident:

(i) Prior to the Incident, Equifax Ltd was aware of serious security patching problems at Equifax Inc. Had Equifax Ltd treated the arrangements as outsourcing, it would have been required under its Outsourcing Policy and risk management framework to take action in response.

(i) Equifax Ltd had not kept records of the data it had sent to Equifax Inc because it wrongly believed that the data had been deleted (see below). Ordinarily Equifax Ltd had remote access to Equifax Inc's servers, access which was restricted when the Incident was discovered as a security measure. This meant Equifax Ltd was unable to obtain the subset of UK data residing on Equifax Inc's servers which had been accessed in the Incident and therefore caused Equifax Ltd delay in identifying and notifying affected UK consumers.

(ii) Equifax Ltd also failed to properly ensure that millions of data records were deleted from Equifax Inc's servers when it substantially ceased outsourcing its EIV product to Equifax Inc in September 2016.

(iii) When the Incident occurred, the way that Equifax Ltd had managed the outsourcing arrangements meant that it was not made aware in a timely manner by Equifax Inc that UK consumer data had been accessed. This contributed to the delays in contacting UK consumers and in Equifax Ltd's inability to cope with the complaints it received when the Incident was announced.

(2) Equifax Ltd failed to put in place adequate systems and controls for ensuring the security of UK consumer data processed by Equifax Inc and stored on its US servers.

Principle 6 breaches

2.10. Principle 6 requires a firm to pay due regard to the interests of its customers and treat them fairly. When a firm becomes aware of a data breach, it is essential that it promptly notifies affected individuals and informs them of the steps that they can take to protect themselves. Equifax Ltd breached Principle 6 because:

(1) It failed to properly manage its outsourcing arrangements with Equifax Inc and this caused it to fail to promptly identify and notify individuals.

(2) Equifax Ltd failed to inform over half a million individuals whose names, DOBs, and telephone numbers were accessed without authorisation that this had occurred. Although Equifax Ltd contacted the other individuals who fell into this category, it declined to inform this subgroup because it could not confirm their addresses without applying a special process to the data, a process it considered too "*resource intensive*". Equifax Ltd had, however, applied those processes to the data which applied to thousands of other affected individuals.

(3) Equifax Ltd exposed consumers who complained to the risk of unfair outcomes by:

(a) Ceasing to exercise Quality Assurance ("QA") checks over complaints processed by a third party between September 2017 and February 2018.

(b) Removing most QA oversight of GCS Ops' complaint handling function in different stages between September 2017 and May 2018.

(c) Failing to immediately reinstate QA following concerns raised in October and November 2017 by Equifax Ltd's Compliance team.

(d) Relying on complaints handling MI from a third party that contained "obvious anomalies" and was otherwise inaccurate and insufficient.

Principle 7 breaches

2.11. Principle 7 requires a firm to pay due regard to the information needs of its clients and communicate information to them in a way which is clear, fair and not misleading. Equifax Ltd breached Principle 7 because:

(1) It published several statements following the Incident which gave, most significantly, an inaccurate impression of the number of consumers affected by the Incident.

2.12. As a result, the Authority hereby imposes a financial penalty on Equifax Ltd in the amount of £11,164,400 (after the Stage 1 discount) pursuant to section 206 of the Act.

3. DEFINITIONS

3.1. The definitions below are used in this Notice:

(1) "Act" means the Financial Services and Markets Act 2000.

(2) "Authority" means the body corporate known as the Financial Conduct Authority.

(3) "Board" means Equifax Ltd's board of directors, the body corporate which governed Equifax Ltd from time to time. References to the Board should not be construed as a reference to any particular director.

(4) "BT OSIS" means a publicly available fee-based commercial directory.

(5) "Consumer" includes for the purposes of this Final Notice: (a) an individual about whom information relevant to the individual's financial standing is or was, may be or may have been held by Equifax Ltd; and (b) a person who used Equifax Ltd's services.

(6) "ConnectSelect" means a publicly available fee-based marketing database.

(7) "CRA" means credit reference agency, a firm that provides credit references.

(8) "DPA 2014" means the data processing agreement between Equifax Ltd and Equifax Ltd dated 23 October 2014.

(9) "DPA 2017" means the data processing agreement between Equifax Ltd and Equifax Inc dated 28 February 2017.

(10) "Data Processing Agreement" means the DPA 2014 or DPA 2017.

(11) "Equifax Inc" means the US parent of Equifax Ltd.

(12) "Equifax Ltd" means Equifax Limited, a CRA located in the United Kingdom and a subsidiary of Equifax Inc.

(13) "GCS Ops" means the operations team for Equifax Ltd's GCS product.

(14) "ICO" means the Information Commissioner's Office.

(15) "Incident" means the 2017 cybersecurity incident at Equifax Inc which affected UK individuals' data transmitted to Equifax Inc by Equifax Ltd.

(16) "Outsourcing" means an arrangement of any form between a firm and a service provider by which that service provider performs a process, a service or an activity which would otherwise be undertaken by the firm itself.

(17) "Part 4A Permission" means the permission granted by the Authority to a firm to carry on regulated activities in the UK.

(18) "Patch Audit" means the internal Equifax Inc 2015 Patch Audit.

(19) "Principles" means the Principles for Businesses set out in the Authority's Handbook.

(20) "Relevant Period" means two separate periods. Element A is the period related to the outsourcing failure and misleading announcements from 1 April 2014 (the date Equifax Ltd became susceptible to FCA regulation) to 31 December 2017 (the date by which Equifax Inc put in place a data security transformation programme). Element B is the period from 7 September 2017 (the date when Equifax Ltd ceased monthly QA work on GCS Ops' own complaints handling performed by GSC Ops' Complaints Specialist Team) and 1 September 2018 (the date by which Equifax Ltd started to address the underlying complaints handling problems).

(21) "Security Executive" means a senior executive employed by Equifax Ltd who had a solid reporting line to Equifax Inc and was responsible for the security teams in Europe, and the liaison between Equifax Ltd and Equifax Inc.

(22) "Threshold Conditions" ("TC") are defined in s 55B(1) of the Act and set out in Part 1B of Schedule 6 to the Act and the COND module of the Handbook and mean the minimum conditions a firm is required to satisfy, and continue to satisfy, in order to be given and to retain Part 4A permission. The Threshold Condition relevant to this matter is "Effective Supervision" (paragraph 2C of Schedule 6 to FSMA) (COND 2.3 G). The Effective Supervision TC says that a firm must be capable of being supervised effectively by the Authority. The factors the Authority will consider in assessing that TC include, among other factors, whether a firm's membership of the group is likely to prevent the Authority's supervision of the firm.

(23) "US-CERT" means the United States Computer Emergency Readiness Team which was, until 2018, an organisation within the Department of Homeland Security's Cyber Security and Infrastructure Security Agency. It is a global exchange for cyber and communications information which it shares with the cybersecurity community.

4. FACTS AND MATTERS

The regulatory framework governing intra-group outsourcing

4.1. Equifax Ltd became subject to Authority regulation on 1 April 2014. From that date, Equifax Ltd was required to comply with the Authority's Principles and have

appropriate arrangements in place to identify and mitigate the risks that outsourcing posed and to ensure that its outsourcing arrangements did not undermine its compliance with the Threshold Conditions.

The FCA's Handbook's Rules on Outsourcing

4.2. The FCA's Handbook's rules and guidance on outsourcing are contained in SYSC 8. SYSC 8.1.6 R imposes several requirements on firms engaged in outsourcing. It provides that: "*If a firm … outsources critical or important operational functions or any relevant services or activities, it remains fully responsible for discharging all of its obligations under the regulatory system...*"

4.3. The FCA's Handbook defines "*outsourcing*" as "*an arrangement of any form between a firm and a service provider by which that service provider performs a process, a service or an activity which would otherwise be undertaken by the firm itself*". Equifax Ltd "outsourced" the storage and processing of significant volumes of UK data to Equifax Inc. Although Equifax Ltd and Equifax Inc are members of the same group and Equifax Ltd is a subsidiary of Equifax Inc, the relationship was nevertheless one of outsourcing and the same considerations and regulatory requirements that apply to a firm outsourcing services to an unrelated third-party apply in the intra-group context.

Equifax Inc

4.4. Equifax Inc is a credit reference agency and global data, analytics, and technology business, operating in North America, Asia Pacific, Europe, and Latin America. Equifax Inc is the parent company of Equifax Ltd. During the Relevant Period, Equifax Inc stored and processed UK consumer data on behalf of Equifax Ltd under a Data Processing Agreement.

4.5. Underlying Equifax Inc's business is data about individuals from all over the world. It holds data on their salaries, debts, financial obligations, spending patterns, late payments, property holdings and losses, political affiliations, email addresses, home addresses, birthdays, marriages, and divorces.

Equifax Ltd

4.6. Equifax Ltd's business lines broadly reflect those of its ultimate parent. Equifax Ltd acts as a traditional CRA providing credit reference information and reports to businesses in respect of individuals and commercial entities. It also acts in a substantially broader capacity. In particular, Equifax Ltd also collects and analyses data from clients and other sources and uses this information for marketing or other purposes. Equifax Ltd holds consumer credit data for most of the adult population of the UK.

Direct to consumer products and services

4.7. Equifax Ltd's primary consumer product is Global Consumer Solutions ("GCS"). The GCS product gives consumers access to their credit reports and it also provides a web monitoring service. It sells GCS products to retail consumers directly and indirectly:

(1) Direct: Consumers obtain their credit reports from Equifax Ltd on a statutory basis or on a subscription basis which gives them access to other services including credit scores, credit alerts and web monitoring.

(2) Indirect: Equifax Ltd sells credit report data to third party firms that, in turn, sell this information to their customers.

4.8. Equifax Ltd had 290,301 UK GCS Direct consumers and generated 1,999,767 credit reports on behalf of those consumers in 2017.

4.9. Equifax Ltd outsourced the processing of GCS Direct consumer data to Equifax Inc and Equifax Inc stored the data on its servers at a facility in Alpharetta, Georgia. During the Relevant Period, Equifax Ltd did not outsource the processing of GCS Indirect consumer data to Equifax Inc. Nor was GCS Indirect data stored on Equifax Inc's servers in the US.

Business-to-business products and services

4.10. Equifax Ltd provides data and products to a variety of business customers across the banking, financial services, telecommunications, utilities, retail and government sectors ("B2B"). Equifax Ltd's B2B business is divisible into consumer services, commercial services, and marketing services. A substantial volume of consumer data underlies these products.

4.11. B2B customers use Equifax Ltd's databases or analytics to obtain information about their end users. The Equifax Identity Verifier ("EIV") product is one of the B2B services Equifax Ltd provides to business customers. The EIV product helps businesses to verify and authenticate their customers' identities.

4.12. At the end of 31 December 2018, Equifax Ltd had 3,038 B2B customers.

Data storage

4.13. During the Relevant Period, Equifax Ltd stored UK data on Equifax Inc's servers located in the UK and Ireland, and on Equifax Inc's servers in the United States (including in Alpharetta, Georgia).

4.14. At the time of the Incident, Equifax Ltd stored substantial volumes of UK consumer data underlying the EIV and GCS Direct products on Equifax Inc's servers in Alpharetta, Georgia. More specifically:

(1) The EIV data consisted of approximately 26,891,466 records which equated to 13,737,244 discrete individuals.

(2) The GCS Direct data consisted of approximately 4,611,736 records. Of these, 80,974 records which equated to 14,961 discrete individuals, were accessed in the Incident.

The Incident

10 March 2017 – 29 July 2017

Intruders scan Equifax Inc's computer systems undetected

4.15. The activities leading up to the Incident began on 10 March 2017 when intruders electronically scanned Equifax Inc's computer systems to determine whether the firm had closed a known software vulnerability. The vulnerability was known because, on 8 March 2017, two days before the attack, US-CERT published an alert about the vulnerability. Apache Struts, the software provider, also warned firms about the problem and provided a software patch to fix the problem. Equifax Inc received the notice of the Apache Struts vulnerability from the US-CERT on 8 March

2017 and circulated the notice to their systems administrators on 9 March 2017. The recipient list for the notice was not up to date so some of the individuals who were responsible for installing the patch did not receive it. Further, the employee who oversaw the team responsible for patching software supporting the sub-directory on which the Apache Struts vulnerability was located did not identify the vulnerability after receiving the notice and thus did not ensure the appropriate personnel applied the patch. An expired certificate prevented a security rule from blocking the attackers from exploiting the Apache Struts vulnerability. Further, vulnerability manager software scanned only root directories, bypassing the sub-directory on which the Apache Struts vulnerability was located. Although Equifax Inc closed the vulnerability in some areas it did not do so entirely. This left Equifax Inc and individuals across the US, the UK, and Canada whose data was stored on its US servers exposed to unauthorised access.

4.16. The actual cyber-attack began on 13 May 2017 and continued, undetected by Equifax Inc, until 29 July 2017. The information about US, UK, and Canadian citizens on Equifax Inc's servers accessed in the attack included consumers' names, dates of birth, email addresses, drivers' licence numbers, partial credit card details and, in the case of US and Canadian citizens, Social Security numbers. Equifax Ltd would not know about the Incident until the night of 7 September 2017, approximately five minutes before Equifax Inc made a market announcement to the general public.

30 July 2017 – 6 September 2017

Equifax Inc investigates the suspicious activity

4.17. On 30 July 2017, Equifax Inc security notified its senior management that it had observed suspicious activity on the firm's US Online Disputes Portal. Equifax Inc instructed lawyers and, on 2 August 2017, they instructed a cybersecurity firm to investigate the suspicious activity, and reported the matter to the FBI.

4.18. Equifax Inc security personnel, lawyers, and other advisers mobilised a "War Room" to coordinate its operations. The War Room controlled the dissemination of information about the Incident, which constituted inside information, and brought individuals inside the information barrier consistent with its global policy, on a "*need to know*" basis. Equifax Ltd was not informed about the incident until 7 September 2017 (see below).

4.19. During the first two weeks of August 2017, the cybersecurity firm and Equifax Inc's security department investigated the incident to identify what had happened and the impact. They determined that cyber-attackers had accessed large volumes of personal data residing on Equifax Inc's servers in Alpharetta, Georgia. By 11 August 2017, the cybersecurity firm had determined that the personal identifying information of consumers may have been accessed. Equifax Inc should have been aware from the outset that there was a risk to UK consumers' data as a result of the Incident, and from 11 August 2017 Equifax Inc should have been aware of the risk that UK consumers' data could have been accessed without authorisation.

4.20. On 23 August 2017, Equifax Inc became aware that a database containing UK consumer data could have been exposed during the Incident. On or about 29 August 2017, Equifax Inc determined that UK consumer data may have been accessed during the Incident. Equifax Inc and Equifax Ltd had entered into a Data Processing Agreement which, among other things, required Equifax Inc to inform Equifax Ltd if it suspected a security breach involving UK data serious enough to require notification to the Authority or ICO. Equifax Inc did not seek advice as to whether such an obligation to notify had arisen until 4 September 2017. It was

advised by external counsel on 5 September 2017 that a requirement to notify the ICO had arisen and it informed Equifax Ltd about the Incident on 7 September 2017 (see below).

4.21. The Security Executive told the Authority that on 1 September 2017 Equifax Inc's global security executive asked him to step into a side room. The Security Executive, an Equifax Ltd employee who reported to Equifax Inc, was responsible for data security in a number of Equifax's international jurisdictions, including the UK. Although the Security Executive had a "hard" reporting line to the global security executive, he had a "*dotted*" reporting line to a senior executive leader of Equifax Ltd. The Security Executive was in Alpharetta for an annual "*ISO summit*". He arrived on 28 August 2017, expected to leave on 1 September 2017, but, in the end, stayed until 15 September 2017.

4.22. The Security Executive told the Authority that the global security executive told him that there was an "*ongoing investigation about an incident, that it was potentially one of the largest incidents on record*". The Security Executive said that he asked the global security executive whether "*it would be safe to conclude that it was solely affecting the US*". The global security executive replied that it was "*not necessarily safe to assume*" that. However, the Security Executive told the Authority "*at no point was I suspicious that the UK was part of it*". The Security Executive said that the global security executive explained that, "*If you ask any further questions then you will be walked off site. And if you tell anyone about the incident then you will be walked off site.*" The Security Executive understood that "*walked off site*" meant that he would be "*terminated, walked off immediately by security.*" The Security Executive did not ask any further questions and joined Equifax Inc security personnel, lawyers, and other advisers in the War Room. The Security Executive told the Authority that he first learnt UK data had been impacted when it was announced publicly on 7 September 2017. If that is true, he was kept in ignorance of this matter despite his role in addressing the Incident and being an employee of Equifax Ltd.

Equifax Inc prepares itself before making the public announcement

4.23. During the period between 29 July 2017 (when Equifax Inc became aware of the suspicious activity) and 7 September 2017 (when Equifax Inc publicly announced the fact of the Incident) besides instructing US lawyers and the cybersecurity firm, Equifax Inc contacted the FBI; identified the US citizens whose data was compromised; formulated a communication and remediation strategy for the affected US citizens; constructed a dedicated website to help US citizens determine whether their information was accessed in the attack; organised a call centre to assist US citizens; and prepared written notifications to all US state attorneys general identifying the approximate number of affected US residents in each state. To the list of consumer protections it originally offered to US citizens, Equifax Inc subsequently gave the ability to lock and unlock their credit files, at will, for life. The Authority does not suggest that Equifax Ltd could or should have taken all of these steps if it had been aware of the Incident during this time, but it is clear given the actions taken by Equifax Inc that Equifax Ltd could have taken significant steps to seek to understand and mitigate the harm of the Incident if it had been given notice at an earlier stage.

7 September 2017 – "A bad surprise"

4.24. On 7 September 2017 between 21:00 and 21:30 BST, Equifax Inc convened a conference call with, among others, a senior executive leader from Equifax Ltd. During the call and minutes before Equifax Inc publicly announced the breach, Equifax Inc informed the participants that Equifax Inc had been the subject of a

cybersecurity breach affecting millions of US citizens and that "*limited*" personal information of UK and Canadian residents had also been exposed.

4.25. This was the first time the Equifax Ltd senior executive leader had heard about the Incident and, in his words, it came as a "*bad surprise*". Equifax Inc could and should have informed Equifax Ltd further in advance of its announcement about the Incident. Advance notice, in turn, would have allowed Equifax Ltd's senior executive team time to take steps to seek to identify the data that was subject to unauthorised access, notify the Authority, prepare informative announcements to the affected UK public as it understood them, and consider an appropriate remediation plan. In the words of an Equifax Ltd communications executive, the fact that Equifax Ltd only found out about the Incident shortly before the public announcement put Equifax Ltd "*on the ropes*" by which he meant, that Equifax Ltd was not able "*to be fully transparent and say precisely what data had been accessed*".

8 September 2017 – The Authority learns about the Incident through a press report

4.26. On 8 September 2017 at 08:32 BST, Equifax Ltd Compliance emailed a proposed notification to the Authority to Equifax Inc asking it to review and approve so that it could notify the Authority.

4.27. Before Equifax Ltd Compliance received a response, the Authority learned about the Incident through a press report and, at approximately 09:45 BST on 8 September 2017, the Authority telephoned Equifax Ltd Compliance.

4.28. Following the Authority's telephone call, Equifax Ltd Compliance sent an email and a copy of Equifax Inc's 7 September 2017 market announcement to the Authority.

4.29. Concerned that Equifax Ltd Compliance was unable to provide basic information, (the number of UK individuals affected, kinds of data accessed, consumer notification plan), the Authority organised a series of discussions with Equifax Ltd.

4.30. At the time the cybersecurity firm's investigations were ongoing and Equifax Ltd had little information about the Incident's effect on UK consumers because its information was limited to that which Equifax Inc provided to it. At that point, the information was limited to the fact that the Incident had occurred and information suggesting that the Incident affected millions of UK consumers. Equifax Inc did not provide Equifax Ltd with a copy of the UK data which had been accessed (some of which had still not been identified by the cybersecurity firm).

4.31. Equifax Ltd needed information about the subset of UK data residing on Equifax Inc's US servers which had been accessed in the Incident to enable it to identify the affected UK consumers. This included copies of the unstructured data and also the queries run by the attackers ("SQL queries"). It had not kept its own records of the data it had transferred to Equifax Inc because it wrongly believed that the data had been deleted. Ordinarily, Equifax Ltd had remote access to UK data residing on Equifax Inc's US servers. During the post-breach detection period, however, Equifax Inc, as a security measure, restricted Equifax Ltd's access to the UK data.

4.32. Having to ask Equifax Inc for access to the UK data delayed Equifax Ltd from identifying the categories of data accessed, the numbers of affected individuals as well as their identities and contact details. In the words of an Equifax Ltd communications executive, it was "*deeply frustrating*" for Equifax Ltd not to have access to the impacted UK data, it was frustrating because until Equifax Ltd had "*accurate data*" it was unable to respond to anxious consumers who wished to know

the extent to which they were affected by the Incident and the extent to which their personal information like credit card numbers was exposed. To begin identifying individuals, Equifax Ltd asked Equifax Inc for additional information and by 13 September 2017 Equifax Ltd was aware that the UK data known to have been impacted at the time related to its EIV product.

4.33. On 13 September 2017, Equifax Ltd asked Equifax Inc to transfer the affected UK EIV data to it to analyse. Equifax Ltd also subsequently requested additional data which had not been impacted in order to support efforts to identify affected UK consumers. Equifax Ltd received an initial copy of the affected UK EIV data on 15 September 2017. However, due to the complexity of the exercise and technical problems, Equifax Ltd did not receive the data requested in the form required until 21 September 2017.

4.34. The delays in identifying and remediating the UK individuals affected by the Incident were attributable, in part, to the fact that Equifax Ltd was subject to Equifax Inc's US crisis management framework. The SIHPP was the underlying policy document. The SIHPP gave Equifax Inc's Security Incident Reponses Team ("SIRT") responsibility to analyse and respond to security incidents and it restricted the dissemination of information in critical incidents to a "*need to know*" basis. Therefore, the centralised SIRT team had the authority to decide who needed to know what, based on whether it was relevant for the performance of "*officially sanctioned duties*".

4.35. Equifax Ltd's risk register identified the SIRT as a control for data breaches without recognising the limitations this could have on its ability to respond to a security incident involving UK consumers whose data had been transferred to Equifax Inc.

Information provided to UK consumers

15 September 2017 – Equifax Ltd's first notification to the public

4.36. Equifax Ltd originally posted information about the Incident on its website and in a press release on 15 September 2017. The information was also included in the material provided to Equifax Ltd's call handlers. Website viewers had to overcome two barriers to reach the Incident page containing the notice.

4.37. The first barrier was a "*cookies*" banner on the Home Page. The cookies banner obscured the sentence inviting readers to click a link to "*learn more about the cybersecurity incident in the United States*". Unless readers clicked the "*continue*" button and consented to cookies, the second barrier, they would not have seen that sentence or the link to the Incident page. Equifax Ltd rectified this on 20 September 2017 after the issue was raised by the Authority. Even then, the underlying sentence did not alert readers to the fact that the Incident affected *UK consumers*.

4.38. Finally, the information Equifax Ltd provided on the Incident page said that:

(1) "*a file containing UK consumer information may potentially have been accessed*." At the point the notice was published, Equifax Ltd was aware that UK consumer data relating to its EIV product resided on Equifax Inc's servers and had been accessed;

(2) "*This was due to a process failure, corrected in 2016, which led to a limited amount of UK data being stored in the US between 2011 and 2016*." The storing of UK data in the US was not the result of a process failure but was the way that Equifax Ltd had, as part of its usual business processes, operated the EIV product. It ceased transferring UK consumer data relating

to the EIV product to Equifax Inc in 2016, but, as discussed below, it failed to ensure that all UK consumer data relating to the EIV product had been removed from Equifax Inc's servers; and

(3) that "*having concluded the initial assessment Equifax has established that it is likely to need to contact fewer than 400,000 UK consumers*". By referring only to the number of individuals whom it had planned to contact, the notice implied that the Incident affected only 400,000 UK consumers. In fact, Equifax Ltd understood at the time that it published the notice that the Incident potentially affected over 15.1 million UK consumers. Multiple news outlets relied on the notice to report that the Incident affected "up to" 400,000 individuals. The reasons for including this language are set out in paragraph 4.40 below, and the Authority considers that there was no intention to mislead by including it. However, when it became apparent that the language was interpreted in an inaccurate way, Equifax Ltd did not take steps to clarify the position until 10 October 2017, as described below.

19 September 2017

4.39. By 19 September 2017, Equifax Ltd had determined, from analysis of the data transferred by Equifax Inc on 15 September 2017, along with a copy of the SQL queries used by the attackers that Equifax Inc provided, that the effect of the Incident was significantly different from its earlier understanding. Based on earlier information from Equifax Inc, Equifax Ltd had thought that:

(1) Data relating to approximately 300,000 consumers whose name, DOB, email address, telephone number and country of residence had been accessed ("Group A").

(2) Data relating to approximately 1.5 million consumers whose name, DOB and either email address or telephone number had been accessed ("Group B").

(3) Approximately 15.1 million name and DOB records had been accessed ("Group C").

4.40. Equifax Ltd had decided to say that it expected to contact up to 400,000 consumers in the notice it published on 15 September 2017 on the basis that it would write to the consumers in Group A. It chose to give a figure of 400,000 rather than 300,000 to allow a margin for error.

4.41. However, by 19 September 2017, Equifax Ltd had discovered via its own analysis that there were actually no consumers who fell into Group A, and the number in Group B was at most approximately 1.25 million. Separately, it had also discovered a new group, consisting of approximately 35,000 individuals whose driving licence information had been accessed. This was a smaller number of affected consumers than had been identified as "Group A" but the data that had been accessed was more sensitive and exposed them to higher risk. This group was thereafter referred to as a new "Group A" and the need to notify them was made a priority. Equifax Ltd took no steps at that time to make this information public in light of the fact that its investigations were still ongoing and previous information that it had received had been incorrect.

21 September 2017

4.42. The Authority contacted Equifax Ltd on 20 September 2017 highlighting the potential unintended consequence of Equifax Ltd's use of the 400,000 figure in its 15 September 2017 press release and website update and asked for a timescale

within which Equifax Ltd would clarify the nature and scale of the affected UK consumer population.

4.43. Equifax Ltd responded that it had "*no plans*" to issue any further press releases at that time; that the Authority had wanted the press release; that at the time Equifax Ltd's investigations had not concluded; that the 400,000 number had been included in "*good faith*"; that the figure was still accurate; and it did not think that issuing a further clarification would further the protection of consumers. In a call held later that day, the Authority stated that it was not asking Equifax Ltd to take any steps at that time. It was agreed that a further call would be scheduled for Monday 25 September 2017, given that Equifax Ltd was still analysing the impacted UK data. As noted above, Equifax Inc did not complete the transfer of data until 21 September 2017.

22 September 2017

4.44. On 22 September 2017, the Authority provided the agenda for the call on 25 September 2017, which included confirmation of figures following work over the weekend and "*The firm's revised proposals for web-site content and re-consideration of an updated press release to ensure any misleading "un-intended consequences" of the initial press-release are addressed and [Group C] customers are made appropriately aware of the loss of their data*."

25 September 2017

4.45. On 25 September 2017, Equifax Ltd provided to the Authority a table which recorded that: the number of consumers in "Group A" (those whose driving licence details had been accessed) was 29,188; those in "Group B" (those whose name, DOB, and phone number had been accessed) was 283,198 and that there were 15,322,230 records of names and dates of birth that had been accessed, but the number of consumers within these records was to be confirmed. It was stated that Equifax Ltd's Analytics team would walk the FCA through those numbers on a call later that afternoon. The figure given for the number of consumers in Group B excluded at least 520,871 other individuals who fell into this group. These individuals fell into two groups: the BT OSIS group comprising (166,741 individuals) and the ConnectSelect group comprising (354,130 individuals). The groups were excluded on the basis that these records were in the public domain and therefore Equifax Ltd did not plan to write to them at the time. Equifax Ltd subsequently conducted contact exercises in respect of the BT OSIS group and ConnectSelect group.

4.46. On the scheduled call with the Authority on 25 September 2017, Equifax Ltd declined to correct the statements that had been published by UK media outlets. Equifax Ltd considered that it should not be "*held responsible for journalists who misinterpret the information*". Separately, it considered that publication of the total number of consumers in the name and DOB data (then thought to be about 15.1 million) was not justified on the basis that this: would alarm consumers in circumstances where no call-to-action would be given; that its call centre and website would be overwhelmed by consumers' inquiries which would cause further distress to consumers; that such an announcement would increase the risk by inviting hackers to search online for the accessed data; and that it would not be able to control journalists' use of that information which would lead to further inaccurate reporting. It also noted that, in the event of publication this could affect Equifax Inc's share price which would require appropriate processes to be followed in relation to NYSE rules in advance of any such publication.

1 October 2017

4.47. During the weekend of 30 September and 1 October 2017, the cybersecurity firm identified that another UK dataset had also been accessed during the Incident (the GCS Direct data). Equifax Inc informed Equifax Ltd about this on 1 October 2017. This data included password details, email addresses and residential addresses relating to thousands of Equifax Ltd's customers. The consumers falling into this category were exposed to the greatest risk of any UK consumers. Equifax Inc provided a copy of the dataset to Equifax Ltd on 2 October 2017.

4.48. This information meant that information in Equifax Ltd's previous press release and website update, which said that the data had not included residential addresses or password information, was no longer correct. Equifax Ltd planned to issue an updated press release to explain these developments, to coincide with it commencing its consumer mailing campaign and produced a draft for discussion with the FCA, although it did not inform the FCA about the discovery that the further dataset had been accessed until 4 October 2017.

4 October 2017

4.49. The Authority was so concerned about Equifax Ltd's communication strategy that it invited a senior executive leader from Equifax Ltd to a meeting to discuss the situation. Equifax Ltd informed the FCA about the discovery of the GCS Direct data at this meeting on 4 October 2017. Following the meeting, Equifax Ltd agreed to issue additional press releases explaining that it would soon begin writing to affected individuals and providing confirmation of the total impact of the Incident.

6 October 2017

4.50. Equifax Ltd provided a draft "*interim press release*" to the Authority on 6 October 2017, along with the draft of a materially similar update for Equifax Ltd's website.

4.51. The Authority had a number of concerns about the content. In particular:

(1) Equifax Ltd's assertion in both documents that it proposed to write to "*all impacted consumers with immediate effect to notify them of the nature of the breach and offer them advice and a range of services to safeguard themselves*"; and

(2) a statement suggesting that Equifax Ltd would be "*contacting every individual".*

4.52. These statements did not provide an accurate picture of the position. Equifax Ltd only planned to write to approximately 5.3% of UK individuals whose data was accessed. Equifax Ltd only planned to contact all UK individuals from within the accessed dataset who it identified and verified at a given address according to its own validation thresholds. The Authority told Equifax Ltd (via written comments on the draft) during the evening of Friday 6 October 2017 that these statements did not appear to be true and suggested deleting or amending them.

4.53. Equifax Ltd replied the same evening and said it would review the FCA's comments over the weekend. It repeated this statement at 07:42 on Saturday 7 October 2017. Equifax Ltd subsequently published the unchanged statements on its website on 7 October 2017.

7 October 2017

4.54. Equifax Ltd then sent the "*interim press release*" to at least one journalist (Equifax Ltd has not been able to confirm how many) as well as public relations firms. The firm realised that the press release was not helpful to UK consumers as revealed in a comment by a senior Equifax Ltd executive who commented to a colleague in an internal email, that "*We have to balance keeping the FCA happy with recognising this release says next to nothing*".

8 October 2017

4.55. On 8 October 2017, the Authority told Equifax Ltd that the information it had published was misleading and explained that it expected Equifax Ltd to clarify the total affected customer population and explaining the different groups of affected consumers in the press release scheduled for the following day. In the end, this press release was published on 10 October 2017. Equifax Ltd did not, during this time, remove from its website the statement published on 7 October.

10 October 2017

4.56. On 10 October 2017, Equifax Ltd published a further press release and website update. This stated, amongst other things, that:

(1) Equifax Ltd would be writing to *"637,430 consumers who had their phone numbers accessed".*

(2) *"a file containing 15.2m UK records dating from between 2011 and 2016 was attacked in the incident".*

4.57. The press release did not:

(1) refer to a further population of 166,741 consumers who had their phone numbers accessed. These consumers had already made their phone number available in a public directory (the BT OSIS group) and, on the basis that their information was already in the public domain and therefore they were not considered to be at risk, Equifax Ltd did not intend to write to them at the time of this press release.

(2) reference a population of potentially up to 512,416 further individuals that may have had their phone number accessed, but whom Equifax Ltd could not identify/verify as living at a given address without undertaking further checks (and therefore did not intend to write to). Equifax did not apply these checks because it considered the relevant process too *"resource intensive"*. Equifax had however applied the same process to the data which applied to thousands of other affected individuals.

(3) make clear that the 15.2 million affected records referenced, excluded: the 693,665 individuals to whom the firm proposed to write, the BT OSIS group and the additional 512,416 unvalidated individuals.

(4) disclose the fact that the residential addresses of some consumers had been accessed in the Incident (although affected individuals were informed of this in the letter that they subsequently received (see below)).

Further updates

4.58. Equifax Ltd issued a further update on 18 January 2018 in which it confirmed that it would be writing to a further 167,431 UK consumers who comprised the BT OSIS group and for whom Equifax Ltd had verified an address.

4.59. In October 2018, at the request of the Authority, Equifax Ltd performed further analysis on name and DOB records and determined that these equated to approximately 12.3m consumers. This information was included in an update published following the issuance of a statement by the US Department of Justice on 10 February 2020 concerning the indictment of individuals responsible for the cyber-attack.

The Incident affected UK consumers

GCS product data

4.60. Equifax Ltd has sold the GCS product in the UK since 18 September 2003. Equifax Ltd started transferring UK GCS Direct product data to Equifax Inc to process shortly after that date. Equifax Ltd had intended to cease transferring UK data to the US by the end of 2019, but due to the launch of a new platform and delays created by COVID it did not complete the transfer of the UK data to Equifax Ltd until July 2021. Equifax Inc continued to process the UK GCS Direct product data until then.

4.61. At the time of the Incident, approximately 290,000 UK consumers had GCS Direct subscriptions and, during the period between January 2014 and December 2017, Equifax Inc generated 7,942,586 credit reports on behalf of Equifax Ltd's UK customers. Although the UK consumer credit reports themselves were not accessed in the Incident, data underlying the GCS Direct membership was accessed.

EIV product data

4.62. Equifax Ltd has sold the EIV product in the UK since 2000. From 2000 until September 2016, Equifax Ltd transferred EIV product data to Equifax Inc to process. Equifax Ltd ceased transferring UK EIV product data to Equifax Inc in September 2016 when it developed a new version of the EIV product. From October 2015 to September 2016, all Equifax Ltd EIV clients were the subject of a "*repatriation exercise*" designed to transfer all UK data and clients to Equifax Ltd.

4.63. Following the Incident, Equifax Ltd would learn that not all the EIV product UK consumer data residing on Equifax Inc's servers was deleted following the repatriation exercise and that some EIV product data remained on Equifax Inc's servers and was accessed during the Incident. The data was consumer data underlying the verification and authentication phases of the EIV product. It included data that was input by the EIV product service user (i.e. Equifax Ltd's client) at a particular point in time when it sought to verify an individual's identity. The input data could include a variety of data points including names, dates of birth and current addresses including up to two previous addresses, the time in residence at the current address, email addresses, drivers' licences, bank account numbers and sort codes, telephone numbers, and the client's own reference for the transaction.

4.64. Equifax Ltd told the Authority that it understood that Equifax Inc would delete copies of all historic UK EIV product records which resided on Equifax Inc's servers. Equifax Inc and Equifax Ltd had exchanged emails about the deletion, but the email exchange did not provide adequate assurance that the data had, in fact, been deleted. In addition, an individual in the EIV business at Equifax Ltd had examined

the content of the data table where the EIV data had been historically stored and found it to be empty, which he concluded meant it had been deleted. However, Equifax Ltd should have taken further steps to ensure that the data had been deleted from Equifax Inc's servers. Indeed, as Equifax Ltd would learn after the Incident, Equifax Inc had not deleted all of the data.

Equifax Ltd's contact with affected individuals

4.65. Equifax Ltd was able, after 15 September 2017, to begin some initial analysis work to determine the identities and contact details of potentially affected UK consumers. It was able to advance this exercise further following receipt of additional information on 22 September 2017. Such individuals fell into different categories, depending on the type of data accessed. Equifax Ltd contacted all UK individuals that it identified and verified as living at a given address in accordance with its validation criteria by letter.

4.66. The "Incident Table" below identifies the numbers of individuals affected, the types of data accessed, and the number of individuals contacted.

Data accessed	**Number of individuals affected**	**Number of individuals contacted**	**Not notified**
Name, DOB, phone number, Equifax membership login details (username and password) with secret Q&A and partially exposed credit card details, and residential addresses	14,961	14,374	548
Name, DOB, Phone number, and Driving Licence number	28,649	24,788	3,701
Name, DOB, email address and phone number	12,086	6,591	5,483
Name, DOB, phone number	1,218,909	628,270	583,478
Name, DOB, mobile and/or landline phone number in BT OSIS database	166,741	166,675	66
Name and DOB	12,322,945	0	12,322,945
TOTALS	**13,749,330**	**840,698**	**12,916,472**

4.67. Consumers who were contacted were provided with particulars regarding their data that had been accessed and offered identity protection products, free of charge.

Governance and risk management

4.68. As a regulated firm, Equifax Ltd retains full accountability for discharging its responsibilities under the regulatory system and cannot delegate responsibility for the functions it outsourced to Equifax Inc. Those responsibilities included the duty to:

(1) Identify and mitigate the risks outsourcing poses.

(2) Oversee and monitor service providers.

(3) Ensure the firm's on-going functioning if outsourced services are interrupted.

2014

4.69. In 2014, Equifax Ltd's primary mechanism for managing the risk of outsourcing data to Equifax Inc was the DPA 2014. The DPA 2014 required Equifax Inc to disclose to Equifax Ltd any accidental or unauthorised access; to keep information relating to Equifax Ltd and its customers confidential; and to provide services to maintain consistent services if Equifax Inc's infrastructure became unavailable. The DPA 2014 itself only contained a short summary of Equifax Inc's security arrangements. The DPA 2014 was supposed to contain a "*Security Annex*" describing Equifax Inc's security arrangements, but Equifax Ltd was unable to provide the Authority with a copy of the agreement containing the annex. It is noted that a new annex was produced in 2016 which was agreed between Equifax Ltd and Equifax Inc to have retrospective effect such that it was incorporated into the terms of the DPA 2014

2015

4.70. Although Equifax Ltd received interim permission on 1 April 2014, it did not have in place an adequate risk management framework that identified and mitigated the risks inherent in the outsourcing and processing of data to Equifax Inc at this time.

4.71. In September 2015, the Board considered the quality of Equifax Ltd's systems and controls for overseeing third party outsourcers when a security incident involving one of the outsourcers occurred. At a Board meeting on 2 November 2015, Equifax Ltd Compliance outlined its concerns about its oversight of third party security standards and noted that "*the firm's existing contractual audit rights were not exercised to an extent that was considered sufficient."* The Board agreed to allocate budget in 2015 to maintain adequate oversight of third parties.

4.72. The oversight concerns were referred for discussion at a Board meeting on 30 November 2015 where the Board noted the "*need to reduce the risk exposure arising from the use of data by third parties. Contractual audit rights were to be reviewed by the Heads of Audit and Security*."

4.73. Equifax Ltd's Board started using its own risk registers in 2015. Prior to this, the Equifax group managed risk on an enterprise basis through its Enterprise Risk Management Framework, which had been in place since 2006. In respect of "*Lack of Supplier Management*", Equifax Ltd's 2015 Risk Register identified some risks related to data theft and attack. The controls that mitigated the risk were stated to be the security policies from the supplier and Equifax (adherence to which was referred to in annual contract agreements); annual site visits performed by Equifax Ltd Security to the third party data centre; and bi-weekly security meetings held with the third party and Equifax Ltd Security.

4.74. Notwithstanding that it had not articulated its risk appetite in 2015 (it was not adopted before September 2016), the Risk Office said that the Risk Appetite Check for "*Lack of Supplier Management*" was "*below*" the Risk Appetite, that the Score Check was "*Much Lower*", and that the Control Check was "*not assessed*". Given there was no documented risk appetite statement at this time to provide the basis for those conclusions, it is unclear how they were formed. The following examples demonstrate the firm's poor understanding of the identification and mitigation of the *"Lack of Supplier Management"* risk:

(1) The 2015 risk register does not indicate that any adequate consideration was given to whether the "*Lack of Supplier Management*" risk applied to Equifax Inc. To the contrary, it appears that there was no consideration of the risks of outsourcing to Equifax Inc, or understanding that the arrangements with Equifax Inc involved outsourcing.

(2) The "*Owner*" of the *"Lack of Supplier Management"* risk was the Security Executive from Equifax Ltd who visited Equifax Inc's data centres in Alpharetta and whose role involved a "hard" reporting line to Equifax Inc. The Security Executive took no steps specifically to manage the risk of outsourcing to Equifax Inc, relying instead on the fact that Equifax Inc had achieved ISO accreditation.

(3) Although the 2015 Risk Register identified the risk of "*Data Breach Investigation*" and noted that "*There is a risk that EFX would struggle with determining the extent of a data breach*", it had no controls in place time to mitigate the risk by the end of that year.

4.75. Equifax Ltd's Risk Management Policy, first approved in November 2015, made the Board ultimately responsible for risk governance throughout the firm. The Board's responsibilities included the duty to review and confirm the suitability of the risk management framework and its underlying policy; to determine the nature and extent of the significant risks it is willing to take; and to review and approve the risk appetite and top risks as needed and at least annually.

Equifax Ltd's Outsourcing Policy introduced on 30 November 2015

4.76. Equifax Ltd's Board approved its original Outsourcing Policy on 30 November 2015. The policy did not specify whether it applied to arrangements with intra-group entities including Equifax Inc. Instead, it referred explicitly to third party outsourcers ("TPOs"). The policy identified the duties of, among others:

(1) The Board (to ensure that Operational Management understands its obligations in relation to outsourcing, to receive regular reports on outsourcing risks, and to take appropriate action to define and implement remedial activity to mitigate outsourcing risks that have moved out of risk appetite).

(2) Operational Management (to assess the risk that Equifax strategies, processes, finance and employees may be exposed to risks arising from TPOs and, as necessary, take steps to reduce those risks).

(3) The Security function (to conduct due diligence checks on prospective "*outsource partners*").

(4) Relationship Management (to understand the risks inherent in the TPO arrangement and the controls that need to be in place to mitigate them).

4.77. Equifax Ltd did not apply the requirements in the Outsourcing Policy to its relationship with Equifax Inc in the same way that it applied them to other third party relationships. The Security Executive accepted in interview that "*I think looking back from a security perspective I think, I don't think we treat Equifax Inc in the same way as we treated a data processor in the UK, so, a traditional business partner. That said, we did have sight of the ISO 270001 certification so the independent audit results and the PCI DSS certification so we took assurance from those two independent audit processes*." This difference in treatment of Equifax Inc is an example of the specific risk that can arise when outsourcing intra-group. The Outsourcing Policy did not identify any risks relating to intra-group outsourcing.

The 2015 patch audit

4.78. Had the Security Executive or Equifax Ltd's Board required Equifax Inc to produce copies of its security audits, they would have become aware of the 2015 Patch Audit, conducted by Equifax Inc's internal audit team. The audit contained information which related directly to the underlying vulnerability which exposed Equifax Ltd's consumer data to the cyber-attack.

4.79. The 2015 Patch Audit identified "*over 1000 known critical/high/medium vulnerabilities on externally facing systems*" and over 7500 critical/high vulnerabilities on internal systems and warned Equifax Inc that its "*patch and configuration management controls were not adequately designed to ensure Equifax systems are securely configured and patched in a timely manner*". Of those known vulnerabilities, approximately 75% of the external, and 93% of the internal, vulnerabilities were over 90 days old.

Development of Risk Management Policy

4.80. By the end of 2015, Equifax Ltd's Board took steps to address its risk management weaknesses. The most significant step was the development of its Risk Management Policy. The Risk Management Policy defined the firm's approach for managing risk, identified the parties responsible for executing the policy, established the risk management cycle, including the use of a risk register, procedures for incident management, and criteria for reporting and governance. The Equifax Ltd Board started using its own risk register and adopted policies, including the Outsourcing Policy.

2016

Equifax Ltd Board meeting – 12 February 2016

4.81. At its 12 February 2016 Board meeting, a senior adviser to the Equifax Ltd Board noted the absence of a formal process for receiving security updates and proposed that the Security Executive should provide at least quarterly security updates. The Board approved this suggestion, but instead of quarterly security updates, it asked for monthly updates. It had been receiving monthly updates since at least November 2015.

4.82. The Security Executive provided his first security update under the new process to the Equifax Ltd Board at its 12 April 2016 meeting. The update consisted of a two-slide power-point presentation about malware and a ransomware infection in Equifax's Spanish business. The subsequent security updates were similarly high-level, unstructured, and gave the Board no real oversight of security matters.

Risk Appetite Statement Approved – September 2016

4.83. The Board approved its first Risk Appetite Statement in September 2016. The 2016 Risk Appetite Statement broadly articulated the level of risk the Board was willing to take to achieve its objectives. Among other risk appetites, the Board articulated the following for consumer data and treatment of consumers:

(1) *"As guardians of consumer data, we will embed and maintain a positive security culture. Through implementation of appropriate controls, we aim to* ***avoid*** *security incidents or data losses involving sensitive data"*.

(2) "*We aim to have fair consumer outcomes and no material compliance failures. We have no appetite for regulatory breach, censure or fine and will* ***avoid*** *any action that could increase the likelihood of these outcomes*".

4.84. The 2016 Risk Appetite Statement defined "avoid" as the strongest measure on its risk appetite scale definition. According to the scale, "***avoid***" meant: "*We have minimal tolerance for uncertainty. We do not anticipate tangible rewards from taking risk. We choose options that are expected to strongly protect our vital objectives*".

4.85. The Security Executive also updated the Board on the progress Equifax Inc was making on patching vulnerabilities. He explained that, "*Progress had been made in the remediation of high risk vulnerabilities and the quantum of patching requirements was reducing*." There is no indication that the Board asked any questions about the nature of the vulnerabilities or the "*quantum*" of patches to be remediated. Instead, according to the minutes, the "*Board were satisfied with the progress being made in all these respects*."

Risk register

4.86. The Board developed its identification of risks and controls. The relevant risks and controls Equifax Ltd identified are set out in *italics* and discussed below:

(1) *Third Party Reliance Risk* (the risk that, "*third parties do not deliver their service to the level of our operational expectations*"). The suppliers listed did not include Equifax Inc. The controls were monitoring plans and site audits. As discussed above, Equifax Ltd did not consider Equifax Inc an outsourced service provider. Equifax Ltd never conducted site audits of Equifax Inc's servers and senior Equifax Ltd representatives explained, at interview, that they considered that it would have been inappropriate even to raise the possibility of undertaking an audit of its parent.

(2) *Data Breach Management* (the risk that "*EFX may not respond to a data breach in a timely, appropriate or thorough manner*"). The control was the SIRT Plan (Security Incident Reponses Team) which fell under the US crisis management program. The plan was kept separate from the normal CAT (Crisis Action Team) plans because, the register explained, "*it is very specific and the activities and communications within it would be covered under Client/Attorney Privilege*".

(3) *Data Breach* (the risk that "*Equifax's systems suffer a security breach by internal or external individuals or customers allowing unauthorised access to our data*"). The controls included monthly vulnerability scans performed by Global Security which "*feeds into a working group between UK Security and IT Operations*".

(4) *Hacking – Equifax Applications* (the risk that "*Equifax data or consumer credit data is compromised/stolen when a successful cyber-attack enables a hacker to exploit a vulnerability from poor software development, gaining access to internal systems*"). The controls section explained that the US Chief Information Security Officer had conducted a review of the US security engineering process to determine whether it remained "US led" or whether it should be devolved to regional teams. The controls included the UK Security team's development of risk assessment and security plans which were to be completed for high risk applications first and then "*rolled out to all applications*".

6 October 2016 Equifax Ltd Board meeting

4.87. At the 6 October 2016 Board meeting, prompted by Equifax Ltd's Compliance function, the directors held a closed session where they "*considered the specific issue of potential influence of the firm's US parent upon the decision making process within the UK Board and governance structures*". Equifax Ltd Compliance raised the question "*solely to ensure that the Board were satisfied it was able to exercise autonomy in its decision making process*". The directors concluded, following a "*detailed discussion*" that they, "*were satisfied that, in relation to directions that the firm received from time to time in the normal course from the Corporation, it had appropriate autonomy to exercise its discretion, oversight and decision making in the interests of the firm*".

2017

4.88. The Equifax Ltd Board approved its "Risk Management Framework Standard" on 3 January 2017 and it continued to develop its risk register and to receive monthly security updates. However, these continued to be *ad hoc* in nature, without a set structure and without regular management information that would have enabled the Board to oversee data security risks effectively.

4.89. In February 2017, Equifax Ltd and Equifax Inc signed the DPA 2017 replacing the DPA 2014. The DPA 2017 contained a clause allowing Equifax Ltd to carry out audits of Equifax Inc. However, Equifax Ltd never carried out any such audits.

4.90. At an Equifax Ltd Board meeting on 7 June 2017, the Security Executive provided the Board with an update on the patch audit explaining that, "*Remedial patching activity had materially reduced the vulnerability of the firm's workstations and servers."* There is no evidence that the Board asked any questions about the length of time the patching exercise was taking, the volume of patching required, or the nature of the risks the unpatched areas created to UK consumers whose data was stored on Equifax Inc's servers.

4.91. As a result of failing adequately to consider the risks of intra-group outsourcing in the Outsourcing Policy or otherwise, the Board created a situation in which the only controls in place for the oversight and management of outsourcing UK consumer data to Equifax Inc were those provided under the Data Protection Agreements, global policies and Equifax Ltd's security function, which included the Security Executive who had a hard reporting line to Equifax Inc. This meant that no specific consideration was given to the appropriateness of the arrangements from an outsourcing perspective.

4.92. The Security Executive explained that he took assurance about security arrangements from Equifax Inc's ISO 27001 certificates. An ISO certificate is a short document which certifies the auditor's findings. The auditor's findings are contained in a separate audit report which underlies the certificate. The Security Executive

only saw copies of the ISO 27001 certificates, not the underlying audits. The certificates provide verification that the auditor certified Equifax Inc (page one) and identify the scope and boundaries of the audit (page two). The appendix to the certificate identifies the geographical territories covered in the audit.

4.93. Equifax Ltd provided substantial amounts of UK personal data to Equifax Inc to process. It took no steps to obtain assurance that the data could safely reside on those servers and instead relied upon Equifax Inc's ISO certificates. It was not sufficient to do so. It was not consistent with Equifax Ltd's Outsourcing Policy. In addition, the Security Executive was aware of specific concerns, such as those identified in Equifax Inc's Patch Audit which should have alerted him to the likelihood that relying on industry standard accreditations was not sufficient.

4.94. The Security Executive believed that Equifax Ltd's security team's oversight of the security controls in place for the GCS application was adequate and that its two main options were to rely on the ISO 27001 certificate or to instruct an Equifax Ltd security employee to audit Equifax Inc.

4.95. Although the DPA 2014 gave Equifax Ltd the power to audit Equifax Inc and Equifax Ltd regularly appointed independent auditors to review other third parties to whom they outsourced services, Equifax Ltd never exercised its power to audit Equifax Inc. A senior individual with responsibility for data protection explained that, because of the relationship between Equifax Ltd and Equifax Inc, it would not have been possible for Equifax Ltd to audit Equifax Inc. Equifax Inc's "*what's it got to do with you… You are not going to come along and audit your parent*" attitude led the individual to resign. The senior individual said, "*There are definitely changes now in the way the US are viewing things but I have to say that I have only seen those changes as a consequence of the breach and I think the very fact that they have hired for the first time, the position of a global chief privacy and data governance office in itself reflects the fact that, that they're taking the matter seriously…"*. Equifax Ltd's Board never discussed the possibility of auditing Equifax Inc's cyber security controls.

2018

4.96. Following the Incident, Equifax Ltd took steps to identify and address the problems which left UK consumers vulnerable to the data breach. The problems, rooted in its approach to intra-group outsourcing, continued into 2018 and 2019 and are the subject of independent reports and evaluations.

4.97. In particular, The British Standards Institute evaluated Equifax Ltd's compliance with the ISO 27001 standard in both 2018 and 2019 and was unable to close Equifax Ltd's non-conformity with the oversight requirement because, *"[t]he UK&I [Equifax Ltd] does not have sufficient visibility of results from Global monitoring, measurement, analysis and evaluation results of UK&I data and there is very little evidence that information security performance in areas 'outsourced' to a Global level are regularly reviewed and monitored on a local level*". Whilst there was evidence the non-conformity had been actioned and of a review in January 2019, there was no record of root cause analysis and corrective action.

Treatment of Complainants

4.98. The regulatory system requires firms to establish processes and procedures to ensure appropriate handling of consumer complaints. Following the public announcements, Equifax Ltd received complaints from consumers about the exposure of their data to cyber-crime. Equifax Ltd used the designation "*Sierra*"

complaints to distinguish those complaints from its "*business as usual"* ("BAU") complaints.

Equifax Ltd outsourced its contact centre services

4.99. Equifax Ltd outsourced its contact centre services to Firm A, a global services firm. 90% of consumer contacts originated with Firm A. As part of their contact centre services, Firm A's agents were authorised to attempt to resolve consumer complaints raised during the first interaction between Firm A's agents and the consumer. If they were unable to do so, Firm A's escalation team sent the complaint to Equifax Ltd's GCS Ops team.

4.100. Equifax Ltd was required to ensure that Firm A complied with the Authority's complaints handling rules. As part of this, Equifax Ltd required Firm A to carry out QA checks of 2% of the forecasted monthly contacts (with a minimum of 12 quality checks per agent, per month) using processes Equifax Ltd designed. QA checks play a vital role in mitigating the risk that complaints will not be handled fairly.

4.101. Firm A retained records of the QA work in order to assess its performance. Firm A's records did not distinguish between Sierra (complaints arising from the Incident) and BAU complaints (complaints arising from Equifax Ltd's business). The Authority asked Equifax Ltd how many unfair outcomes Firm A's complaints QA had identified in the period after the Incident was announced on 7 September 2017. Equifax Ltd said that the data recorded by Firm A about unfair outcomes prior to April 2019 could not be relied upon and contained "*obvious anomalies*", such as a higher number of unfair outcomes than the total number of complaints assessed. Accordingly, Equifax Ltd could not reliably state how many complaints (Sierra or BAU) handled by Firm A resulted in unfair outcomes before April 2019.

4.102. Equifax Ltd did not realise until December 2020 that the contemporaneous information provided to it by Firm A was unreliable.

GCS Ops

4.103. As well as dealing with complaints escalated by Firm A, GCS Ops handled the 10% of consumer contacts, including complaints, which did not originate with Firm A.

4.104. GCS Ops also performed QA on Firm A, including on Firm A's escalation team. This activity was called "*check the checker*". Additionally, as at 7 September 2017, a part-time team in GCS Ops caried out QA on the complaints handled by GCS Ops and *"check the checker"* activity to verify the output of QA on GCS Ops' own complaints handling. Monthly QA work on the end to end customer journey was also performed by GCS Ops' *"Complaints Specialist Team".* Further, Equifax Ltd's Compliance function also monitored GCS Ops' complaints handling.

4.105. The Authority asked Equifax Ltd how many unfair outcomes GCS Ops had identified in the period after the announcement of the Incident. Equifax Ltd informed the Authority that, whilst it assessed whether complaints received a fair outcome prior to September 2018, GCS Ops did not track this by way of management information. Consequently, Equifax Ltd was unable to explain how many complaints received unfair outcomes.

Suspension of QA after 7 September 2017

4.106. Circumstances after the announcement of the Incident on 7 September 2017 presented a particular risk that Equifax Ltd might fail to handle complaints fairly and in accordance with the Authority's rules. These included that Equifax Ltd was

likely to experience a significant rise in non BAU complaints in a scenario where it had no time to adapt its processes. Additionally, Equifax Ltd's Complaints function was operating against a background of an internal report prepared earlier in 2017 which had been highly critical of its complaints handling and QA processes.

4.107. Equifax Ltd did not take sufficient steps until December 2017 to mitigate the risks arising from its QA function by, for example, bringing in additional QA resource or taking other steps to augment or even maintain its current QA function. Instead, Equifax Ltd largely ceased QA oversight of its complaints handling as follows:

(1) the "check the checker" activity conducted by GCS Ops' in relation to Firm A ceased between 28 September 2017 and 12 February 2018, as Equifax Ltd chose to allocate the resources to the handling of Sierra complaints and other consumer remediation activity, such as the consumer mailing exercise. In the intervening period, Equifax Ltd relied on the management information generated by Firm A's own QA work. As noted above, this was not reliable. Though "check the checker" activity resumed after 12 February 2018, a report provided to the Board shortly after that date noted that "*Quality checking… is not of sufficient standard.*"

(2) After 7 September 2017, the monthly end-to-end QA work performed by GCS Ops' "*Complaints Specialist Team*" was ceased. On 12 October 2017, Equifax Ltd ceased the other QA work carried out by GCS Ops. This activity resumed in May 2018.

(3) The effect of the above was that, between October 2017 and February 2018, Equifax Ltd's only QA of complaints handling was that provided by its Compliance team. However, this was carried out for a period of only 4 weeks, between 23 October 2017 and 17 November 2017 and consisted of the review of only 33 complaints. The findings of that exercise were stark: 94% of the assessed complaints failed to meet the required standards. The QA found significant problems with the identification and investigation of complaints and the communication with complainants. Despite these findings, Equifax Ltd did not immediately reinstate and augment its full suite of QA for complaints handling.

4.108. The findings of the Compliance QA work which took place in October 2017 and November 2017 suggested that there had been a crystallisation of the risk that complaints would not be handled fairly in the aftermath of the announcement of the Incident. Further evidence of this emerged over the following months.

4.109. A backlog of 970 complaints had accumulated by 20 November 2017, with the average acknowledgement time standing at 9.07 days. On 23 November 2017, Equifax Ltd decided to engage a compliance consultancy firm to clear the backlog of outstanding Sierra complaints. Following an intensive training period for its complaints handlers, the compliance consultancy firm commenced work on 22 January 2018. By this time Equifax Ltd had closed 1,870 Sierra complaints. The compliance consultancy firm worked on the backlog until 27 April 2018, at which time it was cleared. The effect of the backlog was that, of the 4,211 Sierra complaints recorded by Equifax Ltd, 1027 took longer than 8 weeks to resolve and, of these, 185 were not provided with a communication specified by DISP 1.6.2R(2), which requires firms to notify complainants if their complaint will take more than 8 weeks to resolve and informs them of their right to refer the matter to the Financial Ombudsman service.

4.110. The information from Firm A about the number of unfair outcomes it had identified was concerning (although that information has since been found to be unreliable).

It suggested it was failing to carry out the required number of QA checks on telephone calls between November 2017 and February 2018 and also failing as regards QA checks of written responses from January 2018 until the end of the Relevant Period.

4.111. QA work in early 2018 determined that Equifax Ltd had wrongly informed 1193 Sierra complainants that their complaints had not been upheld (or only "*partly upheld"* in 69 cases). These individuals had complained of the distress caused to them by the Incident. Whilst the individuals received an apology and were offered the free products, Equifax Ltd had incorrectly categorised their complaints as 'not upheld' or 'partially upheld' because of erroneous internal guidance. Equifax Ltd later stated to the Authority that it was not of consequence because the individuals were offered the same free products as they would have been had their complaints been correctly categorised.

Reports into Equifax Ltd's Complaints Handling

4.112. Equifax Ltd Compliance compiled a report into Equifax Ltd's complaints handling which was published internally on 18 June 2018 ("2018 Compliance Report"). Sierra complaints were said to be "*out of scope*" because they would be subject to a separate review. However, the conclusions of the report apply to Sierra and BAU complaints because, except where a Sierra complaint was handled by the compliance consultant, both types of complaint were handled via the same channels, policies and processes. The 2018 Compliance Report was highly critical, with failings spanning the whole customer journey from Firm A through to GCS Ops. Findings included that Equifax Ltd's QA arrangements and approach to MI were *"insufficient"* and that the reduction in QA work for BAU complaints after 7 September 2017 carried a *"significant risk of potential or actual detriment, which is exacerbated by the fact that new complaint handlers were trained and began managing complaints during that time"*. Further, amongst the BAU complaints sampled (which had been handled between November 2017 and February 2018), the report "*did not identify any instances where a fair outcome was delivered at every stage in the process*" from initial identification through to the communication of a final outcome. The 2018 Compliance Report found significant weaknesses and instances of material non-compliance in the complaints operating framework which impacted Equifax Ltd's ability to deliver fair outcomes.

4.113. In February and March 2018, the compliance consultant compiled a report known as the "*GCS Ops Model Review"* (published internally on 18 July 2018). It was highly critical of Equifax Ltd's complaints handling and highlighted a "*risk of customer detriment*". Particular areas of concern included that Equifax Ltd's QA processes were not appropriate and that there was insufficient oversight or review of MI provided by Firm A, despite significant reliance being put upon it.

Reviews resulting from the reports into Equifax Ltd's lack of QA

4.114. As a result of these findings, Equifax Ltd commissioned a Past Business Review, known as the "*GCS Ops Service Review".* The purpose of the review was to understand whether the suspension of QA had affected "BAU" complainants and whether remediation was required as a result. While Equifax Ltd has told the Authority that the GCS Ops Service Review focused on "BAU" contacts, the review itself also refers to "*Sierra data breach queries*", though these are distinguished from complaints about the Incident.

4.115. The GCS Ops Service Review final report only reached the draft stage. The conclusion of that draft document was that 46% of the 238 customer journeys reviewed resulted in an unfair outcome. In 11% of cases, insufficient information

had been captured to make a determination. Unfair outcomes were "*more prevalent for certain contact types, for example…complaints* [and] *Sierra data breach queries".* Of the 110 customers in the sample who were treated unfairly, the draft GCS Ops Service review concluded that 107 suffered some form of detriment, including financial loss and distress.

4.116. Equifax Ltd brought the GCS Ops Service Review to an end before the draft document could be finalised. Equifax Ltd later conducted an analysis of the same 238 customer journeys sample, concluding that, of the 110 unfair outcomes identified, 95 were "unfair" and 15 were not "fair", but had in Equifax Ltd's view resulted in only minor detriment. Due to the small number of cases involving financial detriment, and because Equifax Ltd considered that not all of the 110 unfair outcome cases could be classified as complaints, Equifax Ltd decided not to carry out a further redress or remediation exercise.

4.117. Further, as part of the preparation of the GCS Ops Service Review, a team from Equifax Ltd visited Firm A's facilities. The team found that complaints procedures were not operating properly, including that QA was "*not being undertaken to the required standard"*.

Reviews resulting from the reports into Equifax Ltd's Complaints Handling: Sierra complaints

4.118. Equifax Ltd's Compliance team also considered a small number of complaints handled by the compliance consultant as part of a separate review, which generally concluded that complaints handled by the compliance consultant had been handled appropriately and that remediation had taken place where unfair outcomes were identified.

4.119. Despite multiple indicators that Sierra complainants had been exposed to the risk of unfair outcomes after 7 September 2017, Equifax Ltd has informed the Authority that it does not consider that the scope and severity of potential consumer detriment or harm that may have arisen justifies undertaking a comprehensive review, redress or remediation exercise in relation to those complaints. Further, given the time that Equifax Ltd has allowed to elapse Equifax Ltd no longer holds sufficient records to carry out such an exercise.

4.120. From September 2018 onwards, Equifax Ltd sought to remedy some of the identified issues with its complaints handling and QA functions. The Authority makes no findings in this notice about the adequacy of the steps that Equifax Ltd took at that time and since.

5. FAILINGS

5.1. The regulatory provisions relevant to this Notice are referred to in Annex A.

Principle breaches

Principle 3 breaches

5.2. Principle 3 requires a firm to take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems. Equifax Ltd breached Principle 3 because:

(1) Equifax Ltd failed to put in place, approve, and operate an appropriate risk management framework that allowed it to identify, manage, monitor, and

mitigate the risks inherent in outsourcing the processing of data to its parent, Equifax Inc. Most significantly:

(a) Equifax Ltd failed to put in place an appropriate risk management framework at the point Equifax Ltd came within the Authority's regulation on 1 April 2014. Instead, Equifax Ltd relied on Equifax Inc's risk management arrangements without properly considering whether they satisfied Equifax Ltd's regulatory obligations.

(b) Equifax Ltd approved a risk management framework in November 2015, 19 months after it had become an FCA authorised firm. The risk management framework was deficient because it failed to identify the risks inherent in the transfer, processing and storage of UK consumer data to Equifax Inc, an intra-group outsourced service provider. Its Outsourcing Policy, approved on 30 November 2015, also failed to address these risks. Specific risks arose from this intra-group outsourcing arrangement that Equifax Ltd should have identified and sought to mitigate. In particular:

    (i) Equifax Ltd was subject to Equifax Inc's SIHPP which, in turn, gave Equifax Inc's SIRT group-wide responsibility to analyse and respond to security incidents. This meant that, in the event of a security breach affecting data processed and stored by an intra-group company, there was a risk that the interests of other parts of the Equifax group could be placed above the interests of Equifax Ltd.

    (ii) The Security Executive that was responsible for Equifax Ltd's security function reported to Equifax Inc's global security executive, further contributing to the risk in (i) above.

    (iii) There were also risks common in many cases of intra-group outsourcing, including that known weaknesses at the group entity would not be treated by Equifax Ltd with the same degree of seriousness as would be the case if the outsourcing had been to a third party, and that the risks associated with the outsourced processing of data by Equifax Inc would not be managed with the degree of rigour required notwithstanding its volume and sensitivity.

(c) All of these risks crystallised:

    (i) Prior to the Incident, Equifax Ltd was aware of serious security patching problems at Equifax Inc. Had Equifax Ltd treated the arrangements as outsourcing, it would have been required under its Outsourcing Policy and risk management framework to take responsive action.

    (ii) Equifax Ltd had not kept records of the data it had sent to Equifax Inc because it wrongly believed that the data had been deleted. Ordinarily Equifax Ltd had remote access to its data which was restricted when the Incident was discovered as a security measure. The need to obtain the subset of UK data residing on Equifax Inc's servers which had been accessed in the Incident caused delay in identifying and notifying consumers.

(iii) Equifax Ltd also failed to properly ensure that millions of data records were deleted from Equifax Inc's servers when it substantially ceased outsourcing its EIV product to Equifax Inc in September 2016.

(iv) When the Incident occurred, the way that Equifax Ltd had managed the outsourcing arrangements meant that it was not made aware in a timely manner by Equifax Inc that UK consumer data had been accessed. This contributed to delay in contacting UK consumers and Equifax Ltd's inability to cope with the complaints it received when the Incident was announced.

(d) As a result of failing to identify the risks, the risk management framework failed to identify a risk appetite for the level of risk it was willing to accept when it outsourced critical or important functions to Equifax Inc. The result was that Equifax Ltd did not have a standard against which to measure its appetite for the risks associated with intra-group outsourcing and, consequently, it did not identify the steps it should take to mitigate those risks.

(2) Equifax Ltd failed to put in place adequate systems and controls for ensuring the security of UK consumer data processed by Equifax Inc and stored on its US servers. More specifically:

(a) Equifax Ltd entered into two separate data protection agreements with Equifax Inc, one in 2014 and another in 2017. Equifax Ltd relied upon the "security" annexes in the agreements for assurance that Equifax Inc's security arrangements were adequate. Equifax Ltd was unable to provide a copy of the security annex to the 2014 agreement and the 2017 agreement only contained a short summary of security arrangements.

(b) Although the data protection agreements explicitly gave Equifax Ltd the power to audit Equifax Inc, Equifax Ltd did not exercise that power.

(c) Equifax Ltd relied upon its Security function for assurance that Equifax Inc's security arrangements were appropriate. However, in circumstances where it was subject to a global security policy and the Security function ultimately reported to Equifax Inc, and no consideration was given to the risks of outsourcing the processing of data to Equifax Inc, this gave rise to risks that Equifax Ltd failed to identify or manage. More specifically:

(i) The Security Executive did not take sufficient steps to inspect Equifax Inc's security arrangements and neither did anyone else do so on behalf of Equifax Ltd.

(ii) The Security Executive admitted that Equifax Ltd did not treat Equifax Inc as it did other third-party outsourced providers.

(iii) The Security Executive relied upon Equifax Inc's ISO 27001 certificates for assurance that Equifax Inc's US servers were secure. Nobody, including the Security Executive, took sufficient steps to assess whether Equifax Inc's US servers were sufficiently secure for nature of the outsourcing from

Equifax Ltd, even after becoming aware of the substantial patching backlog.

(iv) The Security Executive provided unstructured *ad hoc* Board reports which were not capable of enabling the Board to exercise appropriate oversight.

Principle 6 breaches

5.3. Principle 6 requires a firm to pay due regard to the interests of its customers and treat them fairly. When a firm becomes aware of a data breach, it is essential that it promptly notifies affected individuals and informs them of the steps that they can take to protect themselves. Equifax Ltd breached Principle 6 because:

(1) It failed to properly manage its outsourcing arrangements with Equifax Inc which meant that it did not promptly identify and notify individuals:

(a) Equifax Inc did not inform Equifax Ltd of the Incident until 7 September 2017. It did not provide Equifax Ltd with the underlying affected EIV data until 15 September 2017 and only provided a fully readable copy of the EIV data on 21 September 2017. Similarly, Equifax Inc did not identify and inform Equifax Ltd of the affected GCS data until 1 October 2017, providing a copy on 2 October 2017. These delays left Equifax Ltd unable to begin to:

(i) identify the UK consumers whom the Incident affected;

(ii) identify the categories of UK consumer data accessed;

(iii) notify the UK consumers whom the Incident affected;

(iv) explain to UK consumers the actions they should take to protect their data; and

(v) design and execute a remediation plan.

(b) Equifax Ltd did not keep proper records of the data it had supplied to Equifax Inc, with the result that, even when it finally did become aware of the Incident, it was hampered in the steps it could take to identify and therefore notify consumers.

(2) It exposed a sub-group of 512,416 individuals (whose names, DOBs, and telephone numbers were accessed without authorisation from the server) to the risk of identity and other theft by failing to inform them that their data had been accessed. Although Equifax Ltd contacted the other individuals who fell into this category, it declined to inform this subgroup because it could not confirm their addresses without applying a special process to the data, a process it considered too "*resource intensive*". Equifax Ltd had, however, applied those processes to the data which applied to thousands of other affected individuals.

(3) Equifax Ltd exposed consumers who complained to the risk of unfair outcomes by:

(a) Ceasing to exercise QA checks over complaints processed by a third party between September 2017 and February 2018.

(b) Removing most QA oversight of GCS Ops' complaint handling function in different stages between September 2017 and May 2018.

(c) Failing to immediately reinstate QA following concerns raised in October and November 2017 by Equifax Ltd's compliance team.

(d) Relying on complaints handling MI from a third party that contained "*obvious anomalies*" and was otherwise inaccurate and insufficient.

Principle 7 breaches

5.4. Principle 7 requires a firm to pay due regard to the information needs of its clients and communicate information to them in a way which is clear, fair and not misleading. Equifax Ltd breached Principle 7 because it:

(1) Published on 15 September 2017, a press release and website update (which also formed the basis of the FAQ it provided to its call centres). The information in this press release:

(a) stated that "*a file containing UK consumer information may potentially have been accessed*." At the point the notice was published, Equifax Ltd was aware that UK consumer data relating to its EIV product resided on Equifax Inc's servers and had been accessed;

(b) stated that it intended to contact 400,000 individuals. At the time, Equifax Ltd was aware that potentially 15.1 million individuals were affected. As a result of this press release, UK national news outlets reported that the Incident affected "up to" 400,000 UK consumers, which Equifax Ltd failed to take timely steps to correct.; and

(c) stated that the UK data had been stored in the US because of a process failure. That was not correct. In fact, the data had been stored there as a result of BAU processes, and when it ceased such processes, Equifax Ltd failed to ensure that all UK consumer data had been removed.

(2) Published, on 7 October 2017, a further website update which said that the firm intended to write to "*all impacted consumers*". At the time it published this statement, Equifax Ltd only intended to contact all UK individuals who it could identify and verify at a given address according to its validation criteria. This constituted approximately 690,000 individuals.

(3) Published, on 10 October 2017, a further press release and website update which continued to give an inaccurate impression about the number of individuals the Incident affected.

(4) Equifax Ltd did not reveal that 15.2 million records equated to 12.3 million unique name and DOB combinations which represented the maximum number of individuals within this group potentially affected by the Incident, until more than two years after the Incident.

6. SANCTION

Financial penalty

6.1. The Authority's policy for imposing a financial penalty is set out in chapter 6 of DEPP. In respect of conduct occurring on or after 6 March 2010, the Authority applies a five-step framework to determine the appropriate level of financial penalty. DEPP 6.5A sets out the details of the five-step framework that applies in respect of financial penalties imposed on firms.

6.2. For the purposes of applying the Authority's financial penalty policy, it is appropriate to separate the analysis into two separate relevant periods:

(1) **Element A** relates to the failings that led to the Incident and the immediate handling of the Incident. The relevant period for these failings commences on 1 April 2014 (the date Equifax Ltd became subject to FCA regulation) and ends on 31 December 2017 (the date by which a data security transformation programme at Equifax Inc was underway).

(2) **Element B** relates to the failings relating to complaints handling. The relevant period for these failings commences on 7 September 2017 (the date when Equifax Ltd ceased monthly QA work on GCS Ops' own complaints handling performed by GSC Ops' Complaints Specialist Team) and ends on 1 September 2018 (the date by which Equifax Ltd started to address the underlying complaints handling problems).

ELEMENT A

Step 1: disgorgement

6.3. Pursuant to DEPP 6.5A.1G, at Step 1 the Authority seeks to deprive a firm of the financial benefit derived directly from the breach where it is practicable to quantify this.

6.4. The Authority does not consider it practicable to quantify any financial benefit that Equifax Ltd derived directly from its breach.

6.5. Step 1 is therefore £0.

Step 2: the seriousness of the breach

6.6. Pursuant to DEPP 6.5A.2G, at Step 2 the Authority determines a figure that reflects the seriousness of the breach. Where the amount of revenue generated by a firm from a particular product line or business area is indicative of the harm or potential harm that its breach may cause, that figure will be based on a percentage of the firm's revenue from the relevant products or business area.

6.7. The Authority considers that the revenue derived from the GCS and EIV product lines is the appropriate basis for the Step 2 figure. This is because the breaches concerned Equifax Ltd's outsourcing of these two products only to Equifax Inc. The relevant revenue for Element A is **£105,847,404**. This is the total revenue Equifax Ltd derived from the GCS (Direct and Indirect revenue) and the EIV product during the Element A Relevant Period.

6.8. In deciding the percentage of the relevant revenue that forms the basis of the step 2 figure, the Authority considers the seriousness of the breach and chooses a percentage between 0% and 20%. This range is divided into five fixed levels which

represent, on a sliding scale, the seriousness of the breach, the more serious the breach, the higher the level. For penalties imposed on firms there are five levels:

(1) Level 1 – 0%

(2) Level 2 – 5%

(3) Level 3 – 10%

(4) Level 4 – 15%

(5) Level 5 – 20%

Level 4 or Level 5 factors

6.9. The Authority takes into account various factors which reflect the impact and nature of the breach, and whether it was committed deliberately or recklessly. DEPP 6.5A.2G(11) identifies factors likely to be considered "*level 4 factors' or 'level 5 factors*". The factors outlined below are relevant to the Authority's assessment.

DEPP 6.5A.2G(11)(a) -- Significant loss or risk of loss to individual consumers, investors, or other market users

6.10. The breach exposed a large number of individual consumers to the risk of financial loss if cyber-criminals used their data that was accessed in the Incident to perpetuate financial crime through identity or other theft.

DEPP 6.5A.2G(11)(b) -- Serious or systemic weaknesses in the management systems or internal controls relating to all or part of the firm's business

6.11. The breach revealed serious deficiencies in Equifax Ltd's risk management framework.

DEPP 6.5A.2G(11)(d)—The breach created a significant risk that financial crime would be facilitated, occasioned or otherwise occur

6.12. The breach exposed UK consumers to a risk of identity theft and financial misappropriation and it exposed the UK financial system to financial crime.

Level 1, 2 or 3 factors

6.13. DEPP 6.5A.2G (12) identifies factors likely to be considered "level 1 factors" or "level 2 factors" or "level 3 factors". The factor outlined below is relevant to the Authority's assessment.

DEPP 6.5A (12)(e) – The breach was committed negligently or inadvertently

6.14. The breach was committed negligently.

6.15. The Authority has taken these factors into account and considers the seriousness of Equifax Ltd's Element A breaches to be level 4. The Element A revenue is **£105,847,404**. The relevant percentage of revenue is 15%. The Step 2 Element A figure is therefore **£15,877,111.**

Step 3: mitigating and aggravating factors

6.16. Pursuant to DEPP 6.5A.3G, at Step 3 the Authority may increase or decrease the amount of the financial penalty arrived at after Step 2 to take into account factors which aggravate or mitigate the breach. The factors outlined below are relevant in this matter.

DEPP 6.5A.3G(2)(b) Degree of cooperation by the firm

6.17. Equifax Ltd displayed a high level of cooperation during the investigation.

DEPP 6.5A.3G(2)(d) Remedial steps taken since the breach

6.18. Equifax Inc instituted a global transformation programme.

6.19. Equifax Ltd implemented a voluntary redress programme. Consumers were offered identity protection products free of charge. Equifax Ltd estimates that it would have cost consumers in the region of £324,509,428 if all redress products offered had been taken up and purchased on the open market.

6.20. Taking all of these matters into account, the Authority considers that a reduction of 15% should be applied to the figure at Step 2.

6.21. The Step 3 figure is therefore **£13,495,544**.

Step 4: adjustment for deterrence

6.22. Pursuant to DEPP 6.5A.4G if the Authority considers the figure arrived at after Step 3 is insufficient to deter the firm who committed the breach, or others, from committing further or similar breaches, then the Authority may increase the penalty.

6.23. The Authority considers that the Step 3 figure of **£13,495,544** represents a sufficient deterrent to Equifax Ltd and others, and so has not increased the penalty at Step 4.

6.24. The Step 4 figure is therefore **£13,495,544**.

Step 5: settlement discount

6.25. Pursuant to DEPP 6.5A.5G, if the Authority and the firm on whom a penalty is to be imposed agree the amount of the financial penalty and other terms, DEPP 6.7 provides that the amount of the financial penalty which might otherwise have been payable will be reduced to reflect the stage at which the Authority and the firm reached agreement.

6.26. The Authority and Equifax Ltd reached agreement at Stage 1 and so a 30% discount applies to the Step 4 figure.

6.27. The Step 5 figure is therefore **£9,446,881**.

ELEMENT B – Complaints handling

Step 1: disgorgement

6.28. Pursuant to DEPP 6.5A.1G at Step 1 the Authority seeks to deprive a firm of the financial benefit derived directly from the breach where it is practicable to quantify this.

6.29. The Authority has not identified any financial benefit that Equifax ltd derived from its breach.

6.30. Step 1 is therefore £0.

Step 2: the seriousness of the breach

6.31. Pursuant to DEPP 6.5A.2G, at Step 2 the Authority determines a figure that reflects the seriousness of the breach. Where the amount of revenue generated by a firm from a particular product line or business area is indicative of the harm or potential harm that its breach may cause, that figure will be based on a percentage of the firm's revenue from the relevant products or business area.

6.32. The Authority considers that the revenue derived from the GCS and EIV product lines is the appropriate basis for the Step 2 figure. This is because the breaches concerned Equifax Ltd's outsourcing of these two products only to Equifax Inc. The relevant revenue for Element B is **£24,537,241**. This is the total revenue Equifax Ltd derived from the GCS (Direct and Indirect revenue) and the EIV product during the Element B relevant period.

6.33. In deciding the percentage of the relevant revenue that forms the basis of the step 2 figure, the Authority considers the seriousness of the breach and chooses a percentage between 0% and 20%. This range is divided into five fixed levels which represent, on a sliding scale, the seriousness of the breach, the more serious the breach, the higher the level. For penalties imposed on firms there are five levels:

(1) Level 1 – 0%

(2) Level 2 – 5%

(3) Level 3 – 10%

(4) Level 4 – 15%

(5) Level 5 – 20%

Level 4 or Level 5 factors

6.34. The Authority takes into account various factors which reflect the impact and nature of the breach, and whether it was committed deliberately or recklessly. DEPP 6.5A.2G(11) identifies factors likely to be considered "level 4 factors' or 'level 5 factors". The Authority considers that no level 4 or level 5 factors apply.

Level 1, 2 or 3 factors

6.35. DEPP 6.5A.2G (12) identifies factors likely to be considered "level 1 factors" or "level 2 factors" or "level 3 factors". The factors outlined below are relevant to the Authority's assessment.

DEPP 6.5A (12)(a) – little, or no, profits were made or losses avoided as a result of the breach, either directly or indirectly

6.36. Equifax Ltd made no profits nor avoided losses as a result of the breach, either directly or indirectly.

DEPP 6.5A.2G(b) – there was no, or little loss or risk of loss to consumers, investors or other market users individually and in general

6.37. The Authority considers that there was loss or risk of loss to consumers whose complaints had been mishandled, but accepts that this risk was limited.

DEPP 6.5A (12)(e) – The breach was committed negligently or inadvertently

6.38. The breach was committed negligently.

6.39. The Authority has taken these factors into account and considers the seriousness of Equifax Ltd's Element B breaches to be level 3. The Element B revenue is £24,537,241. The relevant percentage of revenue is 10%. The Step 2 Element B figure is therefore **£2,453,724**.

Step 3: mitigating and aggravating factors

6.40. Pursuant to DEPP 6.5A.3G, at Step 3 the Authority may increase or decrease the amount of the financial penalty arrived at after Step 2 to take into account factors which aggravate or mitigate the breach.

6.41. Equifax Ltd commissioned a past business review of its complaints handling failings, but did not implement the report's findings.

6.42. The Step 3 Element B figure therefore remains **£2,453,724**.

Step 4: adjustment for deterrence

6.43. Pursuant to DEPP 6.5A.4G if the Authority considers the figure arrived at after Step 3 is insufficient to deter the firm who committed the breach, or others, from committing further or similar breaches, then the Authority may increase the penalty.

6.44. The Authority considers that the Step 3 figure of **£2,453,724** represents a sufficient deterrent to Equifax Ltd and others, and so has not increased the penalty at Step 4.

Step 5: settlement discount

6.45. Pursuant to DEPP 6.5A.5G, if the Authority and the firm on whom a penalty is to be imposed agree the amount of the financial penalty and other terms, DEPP 6.7 provides that the amount of the financial penalty which might otherwise have been payable will be reduced to reflect the stage at which the Authority and the firm reached agreement.

6.46. The Authority and Equifax Ltd reached agreement at Stage 1 and so a 30% discount applies to the Step 4 figure.

6.47. The Step 5 figure is therefore **£1,717,607**.

Total penalty

6.48. The Authority hereby imposes a total financial penalty of **£11,164,400** (**£15,949,200** before Stage 1 discount) on Equifax Ltd for breaching Principles 3, 6, and 7.

7. PROCEDURAL MATTERS

7.1. This Notice is given to Equifax Ltd under and in accordance with section 390 of the Act.

7.2. The following statutory rights are important.

Decision maker

7.3. The decision which gave rise to the obligation to give this Notice was made by the Settlement Decision Makers.

Manner and time for payment

7.4. The financial penalty must be paid in full by Equifax Ltd to the Authority no later than 17 October 2023.

If the financial penalty is not paid

7.5. If all or any of the financial penalty is outstanding on 18 October 2023, the Authority may recover the outstanding amount as a debt owed by Equifax Ltd and due to the Authority.

Publicity

7.6. Sections 391(4), 391(6) and 391(7) of the Act apply to the publication of information about the matter to which this notice relates. Under those provisions, the Authority must publish such information about the matter to which this notice relates as the Authority considers appropriate. The information may be published in such manner as the Authority considers appropriate. However, the Authority may not publish information if such publication would, in the opinion of the Authority, be unfair to you or prejudicial to the interests of consumers or detrimental to the stability of the UK financial system.

7.7. The Authority intends to publish such information about the matter to which this Final Notice relates as it considers appropriate.

Authority contacts

7.8. For more information concerning this matter generally, contact Adil Rana at the Authority (direct line: 020 7066 5800/email: Adil.Rana@fca.org.uk).

Nicholas Hills

Head of Department

Financial Conduct Authority, Enforcement and Market Oversight Division

ANNEX A

RELEVANT STATUTORY AND REGULATORY PROVISIONS

1. RELEVANT STATUTORY PROVISIONS

1.1 The Authority has the power to impose an appropriate penalty on an authorised person if the Authority considers that an authorised person has contravened a relevant requirement (section 206 of the Act).

1.2 In discharging its general functions, the Authority must, so far as reasonably possible, act in a way which is compatible with its strategic objective and advances one or more of its operational objectives (section 1B (1) of the Act). The Authority's strategic objective is ensuring that the relevant markets function well (section 1B (2) of the Act). The Authority has three operational objectives (section 1B (3) of the Act).

1.3 Two of the Authority's operational objectives, the consumer protection objective (section 1C of the Act) and the integrity objective (section 1D of the Act), are relevant to this matter.

2. RELEVANT REGULATORY PROVISIONS

2.1 In exercising its powers to impose a financial penalty, the Authority has had regard to the relevant regulatory provisions published in the Authority's Handbook. The Handbook provisions relevant in this matter are the Principles, the Decision, Procedures and Penalties Manual ("DEPP") and the Enforcement Guide ("EG").

2.2 The Principles are a general statement of the fundamental obligations of firms under the regulatory system. They derive their authority from the Authority's rule-making powers set out in the Act. The relevant Principles in this matter are Principles 3, 6, and 7. The relevant rule is SYSC 8.1.6.

2.3 DEPP sets out the Authority's policy for imposing a financial penalty. For conduct occurring on or after 6 March 2010, the Authority applies a five-step framework to determine the appropriate level of financial penalty. DEPP 6.5A sets out the details of the five-step framework that applies to financial penalties imposed on firms. The conduct that is the subject matter of this action took place after 6 March 2010.

2.4 EG sets out the Authority's approach to taking disciplinary action. The Authority's approach to financial penalties is set out in Chapter 7 of the Enforcement Guide.