

1 MARK BRNOVICH
Attorney General
2 (Firm State Bar No. 14000)
John C. Gray (State Bar No. 028454)
3 Office of the Attorney General
2005 North Central Avenue
4 Phoenix, AZ 85004
Telephone: (602) 542-3725
5 Facsimile: (602) 542-4377
Email: consumer@azag.gov

6 Attorneys for Plaintiff
7

8 **IN THE SUPERIOR COURT OF THE STATE OF ARIZONA**

9 **IN AND FOR THE COUNTY OF MARICOPA**

10
11 STATE OF ARIZONA, *ex rel.* MARK
BRNOVICH, Attorney General,

12 Plaintiff,

13 v.

14 EQUIFAX INC., a corporation,

15 Defendant.
16
17

Case No.

CONSENT JUDGMENT

18

19

20

21

1 Plaintiff State of Arizona, *ex rel.* Mark Brnovich, Attorney General (“the State” or
2 “Plaintiff”), and defendant Equifax Inc., a corporation (“Defendant”) having stipulated to
3 the entry of this Consent Judgment (“Judgment”) by the Court without the taking of proof
4 and without trial, without this Judgment constituting evidence of or an admission by
5 Equifax Inc. regarding any issue of law or fact alleged in the Complaint on file, and
6 without Equifax Inc. admitting any liability, and with all parties having waived their right
7 to appeal, and the Court having considered the matter and good cause appearing:

8 IT IS HEREBY ORDERED, ADJUDGED, AND DECREED THAT:

9 **I. PARTIES AND JURISDICTION**

10 1. Plaintiff is the State of Arizona, *ex rel.* Mark Brnovich, Attorney General.

11 2. Defendant Equifax Inc. is the parent of Equifax Information Services LLC
12 (“EIS”), a CONSUMER REPORTING AGENCY, with its principal office located at
13 1550 Peachtree St. NW, Atlanta, Georgia 30309.

14 3. The Court has jurisdiction over the subject matter of this action and
15 jurisdiction over the parties to this action, and venue is proper in this Court pursuant to
16 A.R.S. § 12-401(17).

17 4. Defendant, at all relevant times, has transacted business in the State of
18 Arizona, including but not limited to business in the County of Maricopa.

19 5. This Judgment is entered pursuant to and subject to the Arizona Consumer
20 Fraud Act (“CFA”), A.R.S. § 44-1521 *et seq.*

21 **II. DEFINITIONS**

22 6. For the purposes of this Judgment, the following definitions shall apply:

1 a. "2017 DATA BREACH" shall mean the data breach, first publicly
2 announced by EQUIFAX on September 7, 2017, in which a person or persons gained
3 unauthorized access to portions of the EQUIFAX NETWORK.

4 b. "2017 BREACH RESPONSE SERVICES AND PRODUCTS" shall
5 mean the following complimentary support services and/or products provided by
6 EQUIFAX, its affiliates, or third parties retained by EQUIFAX or its affiliates, in
7 response to the 2017 DATA BREACH: TrustedID Premier; Equifax Credit Watch Gold
8 with 3 in 1 Monitoring (offered to consumers as a print alternative to TrustedID Premier);
9 the IDNotify product offered for free through Experian; Lock & Alert; and the credit
10 protection services required by Paragraph 42.

11 c. "AFFECTED CONSUMERS" shall mean all consumers residing in
12 Arizona who had their PERSONAL INFORMATION accessed by unauthorized
13 individuals in connection with the 2017 DATA BREACH.

14 d. "ATTORNEYS GENERAL" shall mean the Attorneys General of
15 the states and commonwealths of: Alabama, Alaska, Arizona, Arkansas, California,
16 Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii,¹ Idaho, Illinois, Iowa,
17 Kansas, Kentucky, Louisiana, Maine, Maryland, Michigan, Minnesota, Mississippi,
18 Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New
19 York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Puerto

20
21 ¹ Hawaii is represented by its Office of Consumer Protection. For simplicity
22 purposes, the entire group will be referred to as the "Attorneys General," or individually
as "Attorney General." Such designations, however, as they pertain to Hawaii, shall refer
to the Executive Director of the State of Hawaii Office of Consumer Protection.

1 Rico, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Utah,² Vermont,
2 Virginia, Washington, West Virginia, Wisconsin, and Wyoming, and the District of
3 Columbia.

4 e. “CLEARLY AND CONSPICUOUSLY” shall mean that such
5 statement, disclosure, or other information, by whatever medium communicated,
6 including all electronic devices, is (a) in readily understandable language and syntax, and
7 (b) in a type size, font, color, appearance, and location sufficiently noticeable for a
8 consumer to read and comprehend it, in a print that contrasts with the background against
9 which it appears.

10 i. If such statement, disclosure, or other information is
11 necessary as a modification, explanation, or clarification to other information with which
12 it is presented, it must be presented in proximity to the information it modifies in a
13 manner that is readily noticeable and understandable; and

14 ii. In any communication using an interactive electronic
15 medium, such as the internet or software, the disclosure must be obvious.

16 f. “COMPENSATING CONTROLS” shall mean alternative
17 mechanisms that are put in place to satisfy the requirement for a security measure that is
18 determined by the Chief Information Security Officer or his or her designee to be
19 impractical to implement at the present time due to legitimate technical or business

20 ² Claims pursuant to the Utah Protection of Personal Information Act are brought
21 under the direct enforcement authority of the Attorney General. Utah Code § 13-44-
22 301(1). Claims pursuant to the Utah Consumer Sales Practices Act are brought by the
Attorney General as counsel for the Utah Division of Consumer Protection, pursuant to
the Division's enforcement authority. Utah Code §§ 13-2-1 and 6.

1 constraints. Such alternative mechanisms must: (1) meet the intent and rigor of the
2 original stated requirement; (2) provide a similar level of security as the original stated
3 requirement; (3) be up-to-date with current industry accepted security protocols; and (4)
4 be commensurate with the additional risk imposed by not adhering to the original stated
5 requirement. The determination to implement such alternative mechanisms must be
6 accompanied by written documentation demonstrating that a risk analysis was performed
7 indicating the gap between the original security measure and the proposed alternative
8 measure, that the risk was determined to be acceptable, and that the Chief Information
9 Security Officer or his or her designee agrees with both the risk analysis and the
10 determination that the risk is acceptable.

11 g. “CONSUMER REPORTING AGENCY” shall mean any person as
12 defined by 15 U.S.C. § 1681a(p), and any amendments thereto.

13 h. “CREDIT FILE” shall mean a file as defined in 15 U.S.C. §
14 1681a(g), and any amendments thereto.

15 i. “CREDIT REPORT” shall mean a consumer report as defined in 15
16 U.S.C. § 1681a(d), and any amendments thereto.

17 j. “EFFECTIVE DATE” shall be August 22, 2019 except as otherwise
18 noted in the Judgment.

19 k. “ENCRYPT,” “ENCRYPTED,” or “ENCRYPTION” shall mean
20 rendering data—at rest or in transit—unusable, unreadable, or indecipherable through a
21 security technology or methodology generally accepted in the field of information
22 security commensurate with the sensitivity of the data at issue.

1 l. “EQUIFAX” shall mean Equifax Inc., its affiliates, directors,
2 officers, subsidiaries and divisions, successors and assigns doing business in the United
3 States.

4 m. “EQUIFAX NETWORK” shall mean all networking equipment,
5 databases or data stores, applications, servers, and endpoints that: (1) are capable of
6 using and sharing software, data, and hardware resources; (2) are owned, operated, and/or
7 controlled by EQUIFAX; and (3) collect, process, store, or have access to PERSONAL
8 INFORMATION of consumers who reside in the United States. For purposes of this
9 Judgment, EQUIFAX NETWORK shall not include networking equipment, databases or
10 data stores, applications, servers, or endpoints outside of the United States, which are not
11 used to collect, process, or store PERSONAL INFORMATION, and where access to
12 PERSONAL INFORMATION is restricted using a risk-based control. For purposes of
13 this definition, a risk-based control shall, at a minimum, include: (i) web-application-,
14 network-, or host-based firewalls, or ENCRYPTION of the PERSONAL
15 INFORMATION; and (ii) preadmission identification and/or access management
16 controls, including, for example, multi-factor authentication.

17 n. “FCRA” shall mean the Fair Credit Reporting Act, 15 U.S.C. § 1681
18 et seq., and any amendments thereto.

19 o. “FEE-BASED PRODUCTS OR SERVICES” shall mean any
20 product or service that EQUIFAX sells or charges any amount of money for United
21 States consumers to use or obtain.

1 p. "FURNISHER" or "FURNISHERS" shall mean a person or entity
2 that meets the definition of furnisher set forth in 16 C.F.R. § 660.2(c), and any
3 amendments thereto.

4 q. "GOVERNANCE PROCESS" shall mean any written policy,
5 standard, procedure, or process (or any combination thereof) designed to achieve a
6 control objective with respect to the EQUIFAX NETWORK.

7 r. "MULTI-DISTRICT LITIGATION" shall mean those actions filed
8 against Equifax Inc. and/or its subsidiaries asserting claims related to the 2017 DATA
9 BREACH by or on behalf of one or more consumers that have been or will be transferred
10 to the federal proceedings styled In re Equifax Inc. Customer Data Security Breach
11 Litigation, MDL 1:17-md-2800 (N.D. Ga.) (Consumer Actions).

12 s. "MULTISTATE LEADERSHIP COMMITTEE" shall mean
13 California, Connecticut, District of Columbia, Florida, Georgia, Illinois, Maryland, New
14 Jersey, New York, Ohio, and Pennsylvania.

15 t. "NON-FCRA INFORMATION" shall mean any information that is
16 collected, stored, or maintained by EQUIFAX and either:

17 i. Does not bear on a consumer's credit worthiness, credit
18 standing, credit capacity, character, general reputation, personal characteristics, or mode
19 of living, or

20 ii. Is not used or expected to be used or collected in whole or in
21 part for any purpose authorized under 15 U.S.C. § 1681b, and any amendments thereto.
22

1 u. “PERSONAL INFORMATION” shall mean information regarding
2 an individual residing in Arizona that falls within one of the following categories:

3 i. A consumer’s first name or first initial and last name in
4 combination with any one or more of the following data elements that relate to such
5 individual: (a) Social Security number; (b) driver’s license number; (c) state- or
6 federally-issued identification card number; or (d) financial account number or credit or
7 debit card number, in combination with any required security code, access code, or
8 password that would permit access to the consumer's financial account;

9 ii. Biometric information, meaning data generated by electronic
10 measurements of an individual’s unique physical characteristics, such as a fingerprint,
11 voice print, retina or iris image, or other unique physical characteristics or digital
12 representation thereof;

13 iii. A user name or e-mail address in combination with a
14 password or security question and answer that would permit access to an online account;
15 or

16 iv. Any category of personal information found in the definition
17 as set forth in A.R.S. § 18-545(L)(6) as of September 7, 2017.

18 v. “PROTECTED INDIVIDUAL” shall mean an individual who meets
19 the definition of protected consumer set forth in 15 U.S.C. § 1681c-1(j)(1)(B), and any
20 amendments thereto.

21 w. “REINVESTIGATION” or “REINVESTIGATE” shall mean the
22 process set forth in 15 U.S.C. § 1681i, and any amendments thereto.

1 x. “SECURITY EVENT” shall mean any compromise, or threat that
2 gives rise to a reasonable likelihood of compromise, by unauthorized access or
3 inadvertent disclosure impacting the confidentiality, integrity, or availability of
4 PERSONAL INFORMATION of at least 500 United States consumers held or stored
5 within the EQUIFAX NETWORK, including but not limited to a data breach. For
6 purposes of this definition, “availability” shall not include an intentional limitation on the
7 availability of PERSONAL INFORMATION, such as for purposes of performing
8 maintenance on the EQUIFAX NETWORK.

9 **III. INJUNCTIVE RELIEF**

10 7. The duties, responsibilities, burdens, and obligations undertaken in
11 connection with this Judgment shall apply to EQUIFAX, and its directors, officers, and
12 employees.

13 8. The injunctive terms contained in this Judgment are being entered pursuant
14 to the CFA, A.R.S. § 44-1528.

15 **COMPLIANCE WITH LAW**

16 9. EQUIFAX shall comply with the CFA in connection with its collection,
17 maintenance, and safeguarding of PERSONAL INFORMATION of consumers in
18 Arizona.

19 10. EQUIFAX shall not make a misrepresentation which is capable of
20 misleading consumers or fail to state a material fact if that failure is capable of
21 misleading consumers regarding the extent to which EQUIFAX maintains and/or protects
22

1 the privacy, security, confidentiality, or integrity of any PERSONAL INFORMATION
2 collected from or about consumers.

3 11. EQUIFAX shall not offer, provide, or sell any good or service in violation
4 of 15 U.S.C. § 1681c-1(i), and any amendments thereto.

5 12. EQUIFAX shall comply with Arizona’s data-breach notification law,
6 A.R.S. §§ 18-551 and 552.

7 **INFORMATION SECURITY PROGRAM**

8 13. Within ninety (90) days after the EFFECTIVE DATE and for a period of
9 seven (7) years, EQUIFAX shall implement, maintain, regularly review and revise, and
10 comply with a comprehensive information security program (“Information Security
11 Program”) the purpose of which shall be to take reasonable steps to protect the
12 confidentiality, integrity, and availability of PERSONAL INFORMATION on the
13 EQUIFAX NETWORK. EQUIFAX’s Information Security Program shall be
14 documented in the GOVERNANCE PROCESSES and shall contain administrative,
15 technical, and physical safeguards appropriate to:

- 16 a. The size and complexity of EQUIFAX’s operations;
- 17 b. The nature and scope of EQUIFAX’s activities; and
- 18 c. The sensitivity of the PERSONAL INFORMATION on the

19 EQUIFAX NETWORK.

20 The Information Security Program required by this Judgment shall include the
21 requirements of Paragraphs 14 through 40 in this Judgment.

1 14. The principles of zero-trust should be considered and, where reasonably
2 feasible, utilized in the design of EQUIFAX’s Information Security Program.

3 15. EQUIFAX may satisfy the implementation and maintenance of the
4 Information Security Program and the safeguards required by this Judgment through
5 review, maintenance, and, if necessary, updating, of an existing information security
6 program or existing safeguards, provided that such existing information security program
7 and existing safeguards meet the requirements set forth in this Judgment.

8 16. EQUIFAX shall employ an executive or officer who shall be responsible
9 for implementing, maintaining, and monitoring the Information Security Program (for
10 ease, hereinafter referred to as the “Chief Information Security Officer”). The Chief
11 Information Security Officer shall have the education, qualifications, and experience
12 appropriate to the level, size, and complexity of her/his role in implementing,
13 maintaining, and monitoring the Information Security Program. This Chief Information
14 Security Officer shall report annually to the EQUIFAX Board of Directors on the
15 adequacy of EQUIFAX’s Information Security Program. The Chief Information Security
16 Officer shall also, at any meeting of the Board of Directors concerning the security
17 posture or security risks faced by EQUIFAX and at each quarterly meeting of the
18 Technology Committee of the Board of Directors, provide reports to EQUIFAX’s Board
19 of Directors, and shall inform, advise, and update the Board of Directors or Technology
20 Committee regarding EQUIFAX’s security posture and the security risks faced by
21 EQUIFAX. The Chief Information Security Officer shall report to the Chief Executive
22 Officer, as well as a member of EQUIFAX’s Board of Directors, in the event that the

1 Chief Executive Officer is not a member of the Board of Directors, (i) any unauthorized
2 intrusion to the EQUIFAX NETWORK within forty-eight (48) hours of discovery that it
3 is a SECURITY EVENT and (ii) any “THIRD-PARTY REPORTED EVENT” as defined
4 in Paragraph 23 within forty-eight (48) hours of receipt of the report from the third-party
5 vendor. The quarterly reports to the Technology Committee shall also include all
6 SECURITY EVENTS or THIRD-PARTY REPORTED EVENTS that were reported to
7 the Chief Executive Officer after the previous regular report.

8 17. EQUIFAX shall employ for each of its United States business units an
9 officer who shall be responsible for implementing, maintaining, and monitoring the
10 Information Security Program for that business unit (for ease, hereinafter referred to as a
11 “Business Information Security Officer”). Each Business Information Security Officer
12 shall have the education, qualifications, and experience appropriate to the level, size, and
13 complexity of the Business Information Security Officer’s role in implementing,
14 maintaining and monitoring the Information Security Program. Each Business
15 Information Security Officer shall be responsible for regularly informing, advising, and
16 updating the Chief Information Security Officer or his/her designee regarding the security
17 posture of the business unit for which he/she is responsible, the security risks faced by the
18 relevant business units, and the implications of any decision the Business Information
19 Security Officer makes that may materially impact the security posture of the business
20 unit.

21 18. EQUIFAX shall ensure that the Chief Information Security Officer,
22 Business Information Security Officers, and Information Security Program receive the

1 resources and support reasonably necessary to ensure that the Information Security
2 Program functions as required by this Judgment.

3 19. Employees who are responsible for implementing, maintaining, or
4 monitoring the Information Security Program, including but not limited to the Chief
5 Information Security Officer and Business Information Security Officers, must have
6 sufficient knowledge of the requirements of this Judgment and receive specialized
7 training on safeguarding and protecting consumer PERSONAL INFORMATION to help
8 effectuate EQUIFAX's compliance with the terms of this Judgment. EQUIFAX shall
9 provide the training required under this paragraph to all employees within sixty (60) days
10 of the EFFECTIVE DATE of this Judgment or prior to an employee starting their
11 responsibilities for implementing, maintaining, or monitoring the Information Security
12 Program. On an annual basis, or more frequently if appropriate, EQUIFAX shall provide
13 training on safeguarding and protecting PERSONAL INFORMATION to its employees
14 who handle PERSONAL INFORMATION, and its employees responsible for
15 implementing, maintaining, or monitoring the Information Security Program.

16 20. EQUIFAX's Information Security Program shall be designed and
17 implemented to ensure the appropriate identification, investigation of, and response to
18 SECURITY EVENTS.

19 21. EQUIFAX shall implement and maintain a written incident response plan
20 to prepare for and respond to SECURITY EVENTS. EQUIFAX shall revise and update
21 this response plan, as necessary, to adapt to any changes to the EQUIFAX NETWORK.
22 Such a plan shall, at a minimum, identify and describe the following phases:

- 1 I. Preparation;
- 2 II. Detection and Analysis;
- 3 III. Containment;
- 4 IV. Notification and Coordination with Law Enforcement;
- 5 V. Eradication;
- 6 VI. Recovery;
- 7 VII. Consumer Response (including consideration of appropriate staffing levels,
- 8 training, and written materials), and Consumer and Regulator Notification and
- 9 Remediation; and
- 10 VIII. Post-Incident Analysis.

11 22. EQUIFAX shall conduct, at a minimum, biannual incident response plan

12 exercises (“table-top exercises”) to test and assess its preparedness to respond to a

13 SECURITY EVENT. These exercises shall include the following, as appropriate:

14 a. Planning for sufficient staffing levels to handle a high volume of

15 potential consumer traffic and provide consumers access to live agents in a reasonable

16 amount of time;

17 b. Planning employee training to provide relevant, useful, and accurate

18 information to consumers, including how to place fraud alerts or security freezes;

19 c. Preparing written materials to provide to consumers that CLEARLY

20 AND CONSPICUOUSLY disclose relevant information;

21 d. Planning for any necessary online resources to be compliant with the

22 Americans with Disabilities Act (ADA);

1 e. Planning for oral and written consumer communications in multiple
2 languages depending on the nature of the table-top exercise; and

3 f. Considering the translation of state-required data breach
4 notifications to consumers into multiple languages including Spanish, Chinese, Tagalog,
5 Vietnamese, Arabic, French, and Korean depending on the nature of the table-top
6 exercise.

7 23. EQUIFAX shall oversee its third-party vendors who have access to the
8 EQUIFAX NETWORK or who hold or store PERSONAL INFORMATION on
9 EQUIFAX's behalf by maintaining and periodically reviewing and revising, as needed, a
10 GOVERNANCE PROCESS for assessing vendor compliance in accordance with
11 EQUIFAX'S Information Security Program including whether the vendor's security
12 safeguards are appropriate for that business. That GOVERNANCE PROCESS shall
13 require vendors by contract to implement and maintain such safeguards and to notify
14 EQUIFAX within seventy-two (72) hours of discovering a SECURITY EVENT (a
15 "THIRD-PARTY REPORTED EVENT").

16 **PERSONAL INFORMATION SAFEGUARDS AND CONTROLS**

17 24. EQUIFAX shall maintain and comply with a GOVERNANCE PROCESS
18 establishing that PERSONAL INFORMATION will be collected, processed, or stored to
19 the minimum extent necessary to accomplish the intended legitimate business purpose(s)
20 in using such information.

21 25. EQUIFAX shall maintain, regularly review, revise, and comply with a
22 GOVERNANCE PROCESS requiring EQUIFAX to either ENCRYPT PERSONAL

1 INFORMATION or otherwise implement COMPENSATING CONTROLS to protect
2 PERSONAL INFORMATION from unauthorized access, whether the information is
3 transmitted electronically from the EQUIFAX NETWORK or is stored in the EQUIFAX
4 NETWORK.

5 26. EQUIFAX shall make reasonable efforts to reduce its use and storage of
6 consumer Social Security numbers. It shall:

7 a. Actively seek to and, where possible, participate in an external
8 organization or working group focused on the development and implementation of
9 alternative means of identity authentication with a goal of identifying options for
10 minimizing its use of Social Security numbers for identity authentication purposes, to the
11 extent that any such group exists;

12 b. Conduct an internal study of the primary instances in which Social
13 Security numbers are collected, maintained, or used on the EQUIFAX NETWORK,
14 including for consumer authentication purposes, and evaluate potential alternatives to
15 such collection, maintenance, or use. In evaluating such alternatives, EQUIFAX may
16 consider, among other things, the impact on privacy, security, reducing identity theft and
17 fraud, and ease of incorporation into EQUIFAX's business processes. Upon the
18 conclusion of this study, or within one year of the EFFECTIVE DATE, whichever is
19 sooner, the study shall be provided to the Chief Executive Officer, who shall establish a
20 working group to implement identified alternatives, where feasible. EQUIFAX shall also
21 provide a copy of the study to the California Attorney General's Office.
22

1 i. The California Attorney General’s Office may provide a copy
2 of the study received from EQUIFAX to the Arizona Attorney General upon request.

3 ii. The study and all information contained therein, to the extent
4 permitted by the laws of the State of Arizona: shall be treated by the Arizona Attorney
5 General’s Office as confidential; shall not be shared or disclosed except as described in
6 subsection (i); and shall be treated by the Arizona Attorney General’s Office as exempt
7 from disclosure under the relevant public records laws of the State of Arizona. In the
8 event that the Arizona Attorney General’s Office receives any request from the public for
9 the study or other confidential documents under this Judgment and believes that such
10 information is subject to disclosure under the relevant public records laws, the Arizona
11 Attorney General’s Office agrees to provide EQUIFAX with at least ten (10) days
12 advance notice before producing the information, to the extent permitted by state law
13 (and with any required lesser advance notice), so that EQUIFAX may take appropriate
14 action to defend against the disclosure of such information. The notice under this
15 paragraph shall be provided consistent with the notice requirements contained in
16 Paragraph 81. Nothing contained in this subparagraph shall alter or limit the obligations
17 of the Arizona Attorney General that may be imposed by the relevant public records laws
18 of the State of Arizona, or by order of any court, regarding the maintenance or disclosure
19 of documents and information supplied to the Arizona Attorney General except with
20 respect to the obligation to notify EQUIFAX of any potential disclosure.

21 c. Maintain authentication protocols that do not allow
22 consumers to access PERSONAL INFORMATION from EQUIFAX in connection with

1 direct-to-consumer products and services, such as credit monitoring and CREDIT
2 REPORTS, using only a name in combination with a Social Security number; and

3 d. Implement a GOVERNANCE PROCESS that contractually
4 requires EQUIFAX reseller customers who receive consumer PERSONAL
5 INFORMATION from EQUIFAX to maintain authentication protocols that do not allow
6 consumers to access PERSONAL INFORMATION from EQUIFAX in connection with
7 direct-to-consumer products and services, such as credit monitoring and CREDIT
8 REPORTS using only a name in combination with a Social Security number.

9 27. EQUIFAX shall ENCRYPT Social Security numbers when they are stored
10 in the EQUIFAX NETWORK or transmitted electronically from the EQUIFAX
11 NETWORK, or otherwise implement COMPENSATING CONTROLS to protect Social
12 Security numbers from unauthorized access.

13 28. EQUIFAX shall maintain, regularly review and revise as necessary, and
14 comply with a GOVERNANCE PROCESS that provides for the secure disposal, on a
15 periodic basis, of PERSONAL INFORMATION that is no longer necessary for the
16 legitimate business purpose for which the PERSONAL INFORMATION was collected,
17 processed, or stored, except where such information is otherwise required to be
18 maintained by law.

19 **SPECIFIC TECHNICAL SAFEGUARDS AND CONTROLS**

20 29. **Managing Critical Assets:** EQUIFAX shall rate all software and hardware
21 within the EQUIFAX NETWORK based on criticality, factoring in whether such assets
22 are used to collect, process, or store PERSONAL INFORMATION.

1 30. Segmentation:

2 a. EQUIFAX shall maintain, regularly review and revise as necessary,
3 and comply with its segmentation protocols and related policies that are reasonably
4 designed to properly segment the EQUIFAX NETWORK, which shall, at a minimum,
5 ensure that systems communicate with each other in a secure manner and only to the
6 extent necessary to perform their business and/or operational functions, and that
7 databases are segmented except from systems with which they are required to interact.

8 b. EQUIFAX shall regularly evaluate, and, as appropriate, restrict
9 and/or disable any unnecessary ports on the EQUIFAX NETWORK.

10 c. EQUIFAX shall logically separate its production and non-production
11 environments in the EQUIFAX NETWORK, including the use of appropriate
12 technological safeguards to protect PERSONAL INFORMATION within non-production
13 environments.

14 31. Penetration Testing/Risk Assessment:

15 a. EQUIFAX shall maintain and regularly review and revise as
16 necessary a risk-assessment program designed to continually identify and assess risks to
17 the EQUIFAX NETWORK. In cases where EQUIFAX deems a risk to be acceptable,
18 EQUIFAX shall generate and retain a report demonstrating how such risk is to be
19 managed in consideration of cost or difficulty in implementing effective
20 countermeasures. All reports shall be maintained by the Chief Information Security
21 Officer or his or her designee and be available for inspection by the Third-Party Assessor
22 described in Paragraph 61 of this Judgment.

1 b. EQUIFAX shall implement and maintain a risk-based penetration-
2 testing program reasonably designed to identify, assess, and remediate security
3 vulnerabilities within the EQUIFAX NETWORK. This program shall include at least
4 one annual penetration test of all externally-facing applications within the EQUIFAX
5 NETWORK and at least one weekly vulnerability scan of all systems within the
6 EQUIFAX NETWORK.

7 c. EQUIFAX shall rate and rank the criticality of all vulnerabilities
8 identified as a result of any vulnerability scanning or penetration testing that it performs
9 on the EQUIFAX NETWORK in alignment with an established industry-standard
10 framework (e.g., NVD, CVSS, or equivalent standard). For each vulnerability that is
11 ranked as most critical, EQUIFAX shall commence remediation planning within twenty-
12 four (24) hours after the vulnerability has been rated as critical and shall apply the
13 remediation within one (1) week after the vulnerability has received a critical rating. If
14 the remediation cannot be applied within one (1) week after the vulnerability has received
15 a critical rating, EQUIFAX shall identify existing or implement new COMPENSATING
16 CONTROLS designed to protect PERSONAL INFORMATION as soon as practicable
17 but no later than one (1) week after the vulnerability received a critical rating.

18 32. Access Control and Account Management:

19 a. EQUIFAX shall implement and maintain appropriate controls to
20 manage access to, and use of, all EQUIFAX NETWORK accounts with access to
21 PERSONAL INFORMATION, including, without limitation, individual accounts,
22

1 administrator accounts, service accounts, and vendor accounts. To the extent that
2 EQUIFAX maintains accounts requiring passwords:

3 i. Such controls shall include strong passwords, password
4 confidentiality policies, password-rotation policies, and two-factor authentication or any
5 other equal or greater authentication protocol, where technically feasible. For purposes
6 of this paragraph, any administrative-level passwords shall be ENCRYPTED or secured
7 using a password vault, privilege access monitoring, or an equal or greater security tool
8 that is generally accepted by the security industry.

9 ii. EQUIFAX shall implement and maintain appropriate policies
10 for the secure storage of EQUIFAX NETWORK account passwords based on industry
11 best practices; for example, hashing passwords stored online using an appropriate hashing
12 algorithm that is not vulnerable to a collision attack together with an appropriate salting
13 policy, or other equivalent or stronger protections.

14 b. EQUIFAX shall implement and maintain adequate access controls,
15 processes, and procedures, the purpose of which shall be to grant access to the EQUIFAX
16 NETWORK only after the user has been properly identified, authenticated, reviewed, and
17 approved.

18 c. EQUIFAX shall as soon as practicable, and within forty-eight (48)
19 hours, terminate access privileges for all persons whose access to the EQUIFAX
20 NETWORK is no longer required or appropriate.

21 d. EQUIFAX shall limit access to PERSONAL INFORMATION by
22 persons accessing the EQUIFAX NETWORK on a least-privileged basis.

1 e. EQUIFAX shall regularly inventory the users who have access to the
2 EQUIFAX NETWORK in order to review and determine whether or not such access
3 remains necessary or appropriate. EQUIFAX shall regularly compare termination lists to
4 user accounts to ensure access privileges have been appropriately terminated. At a
5 minimum, such review shall be performed on a quarterly basis.

6 f. EQUIFAX shall implement and maintain adequate administration
7 processes and procedures to store and monitor the account credentials and access
8 privileges of employees who have privileges to design, maintain, operate, and update the
9 EQUIFAX NETWORK.

10 g. EQUIFAX shall implement and maintain controls to identify and
11 prevent unauthorized devices from accessing the EQUIFAX NETWORK such as a
12 network access controller or similar or more advanced technology.

13 33. **File Integrity Monitoring:** EQUIFAX shall maintain controls designed to
14 provide near real-time notification of unauthorized modifications to the EQUIFAX
15 NETWORK. The notification shall include information available about the modification
16 including, where available, the date of the modification, the source of the modification,
17 the type of modification, and the method used to make the modification.

18 34. **Unauthorized Applications:** EQUIFAX shall maintain controls designed
19 to identify and protect against the execution or installation of unauthorized applications
20 on the EQUIFAX NETWORK.

21 35. **Logging and Monitoring:**
22

1 a. EQUIFAX shall implement controls the purposes of which shall be
2 to monitor and log material security and operational activities on the EQUIFAX
3 NETWORK, to report anomalous activity through the use of appropriate platforms, and
4 to require that tools used to perform these tasks be appropriately monitored and tested to
5 assess proper configuration and maintenance.

6 b. All SECURITY EVENTS shall immediately be reported to the Chief
7 Information Security Officer and appropriate Business Information Security Officer, and
8 in no event more than eight (8) hours from the identification of the SECURITY EVENT.
9 Any vulnerability that is associated with a SECURITY EVENT shall be remediated
10 within twenty-four (24) hours of the identification of the vulnerability. If that
11 vulnerability cannot be remediated within twenty-four (24) hours of its identification,
12 then EQUIFAX shall implement COMPENSATING CONTROLS or decommission the
13 system within twenty-four (24) hours of the identification of the vulnerability.

14 c. EQUIFAX shall monitor on a daily basis, and shall test on at least a
15 monthly basis, any tool used pursuant to this paragraph, to properly configure, regularly
16 update, and maintain the tool, to ensure that the EQUIFAX NETWORK is adequately
17 monitored.

18 36. **Change Control:** EQUIFAX shall maintain, regularly review and revise as
19 necessary, and comply with a GOVERNANCE PROCESS established to manage and
20 document changes to the EQUIFAX NETWORK. At a minimum:

21 a. EQUIFAX shall define the roles and responsibilities for those
22 involved in the change control process, including a board responsible for reviewing

1 changes (for ease, hereinafter referred to as the “Change Advisory Board”). The Change
2 Advisory Board shall include stakeholders from the appropriate business and
3 informational technology units. The Change Advisory Board’s responsibilities shall
4 include: managing overall change control policies and procedures; providing guidance
5 regarding the overall change control policies and procedures; conducting an annual audit
6 of change requests to ensure that changes to the EQUIFAX NETWORK are properly
7 analyzed and prioritized; and reviewing, approving, evaluating, and scheduling requests
8 for changes to the EQUIFAX NETWORK.

9 b. The change control policies and procedures shall address the process
10 to: request a change to the EQUIFAX NETWORK; determine the priority of the change;
11 determine the change’s impact on the EQUIFAX NETWORK, the security of
12 PERSONAL INFORMATION, and EQUIFAX’s ongoing business operations; obtain the
13 appropriate approvals from required personnel (e.g., change requester, business unit,
14 Business Information Security Officer, Change Advisory Board); develop, test, and
15 implement the change; and review and test the impact of the change on the EQUIFAX
16 NETWORK and the security of PERSONAL INFORMATION after the change has been
17 made. The change control policies and procedures required by this paragraph shall
18 require that any changes to the EQUIFAX NETWORK be evaluated regarding potential
19 risks, and that all changes receive appropriate additional or heightened (i) analysis, (ii)
20 approvals from required personnel, and (iii) testing.

21 c. Any action with respect to any changes to the EQUIFAX
22 NETWORK (requesting, analyzing, approving, developing, implementing, and

1 reviewing) shall be documented and retained, with the documentation appropriately
2 secured and stored in repositories that are scoped to an application, business unit, and/or
3 geography and are accessible to appropriate security personnel.

4 **37. Asset Inventory:** EQUIFAX shall utilize manual processes and, where
5 practicable, automated tool(s) to regularly inventory and classify, and issue reports on, all
6 assets that comprise the EQUIFAX NETWORK, including but not limited to all software,
7 applications, network components, databases, data stores, tools, technology, and systems.
8 The asset inventory as well as applicable configuration and change management systems
9 shall, at a minimum, collectively identify: (a) the name of the asset; (b) the version of the
10 asset; (c) the owner of the asset; (d) the asset's location within the EQUIFAX
11 NETWORK; (e) the asset's criticality rating; (f) whether the asset collects, processes, or
12 stores PERSONAL INFORMATION; and (g) each security update and security patch
13 applied or installed during the preceding period.

14 **38. Digital Certificates:** EQUIFAX shall implement and maintain a digital
15 certificate management tool or service the purpose of which shall be to inventory digital
16 certificates that expire longer than a week after their creation and that are used to
17 authenticate servers and systems in the EQUIFAX NETWORK. The system or tool
18 required by this paragraph shall manage the life cycle of all such digital certificates,
19 including whether to issue, cancel, renew, reissue, or revoke a digital certificate. The
20 system or tool required by this paragraph shall track the expiration date of any such
21 digital certificate and provide notification of such expiration to the custodian of the
22 certificate key thirty days (30) prior to expiration, ten days (10) prior to expiration, and

1 on the date the digital certificate expires. Digital certificate for purposes of this
2 paragraph shall include a security token, biometric identifier, or a cryptographic key used
3 to protect externally-facing systems and applications.

4 **39. Threat Management:** EQUIFAX shall establish a threat management
5 program which shall include the use of automated tools to continuously monitor the
6 EQUIFAX NETWORK for active threats. EQUIFAX shall monitor on a daily basis, and
7 shall test on at least a monthly basis, any tool used pursuant to this paragraph, to assess
8 whether the monitoring tool is regularly configured, tested, and updated.

9 **40. Updates/Patch Management:** EQUIFAX shall maintain, keep updated,
10 and support the software on the EQUIFAX NETWORK, taking into consideration the
11 impact a software update will have on data security in the context of the EQUIFAX
12 NETWORK and its ongoing business and network operations, and the scope of the
13 resources required to maintain, update, and support the software. At a minimum,
14 EQUIFAX shall also do the following:

15 a. For any software that will no longer be supported by its
16 manufacturer or a third party, EQUIFAX shall commence the evaluation and planning to
17 replace the software or to maintain the software with appropriate COMPENSATING
18 CONTROLS at least two (2) years prior to the date on which the manufacturer's or third
19 party's support will cease, or from the date the manufacturer or third party announces that
20 it is no longer supporting the software if such period is less than two (2) years. If
21 EQUIFAX is unable to commence the evaluation and planning in the timeframe required
22 by this subparagraph, it shall prepare and maintain a written exception that shall include:

1 i. A description of why the exception is appropriate, e.g., what
2 business need or circumstance supports the exception;

3 ii. An assessment of the potential risk posed by the exception;
4 and

5 iii. A description of the schedule that will be used to evaluate and
6 plan for the replacement of the software or addition of any COMPENSATING
7 CONTROLS.

8 b. EQUIFAX shall maintain reasonable controls to address the
9 potential impact security updates and security patches may have on the EQUIFAX
10 NETWORK and shall:

11 i. Maintain a patch management solution(s) to manage software
12 patches that includes the use of automated, standardized patch management distribution
13 tool(s), whenever technically feasible, to: maintain a database of patches; deploy patches
14 to endpoints; verify patch installation; and retain patch history. The patch management
15 program must also have a dashboard or otherwise report on the success, failure, or other
16 status of any security update or security patch; and

17 ii. Maintain a tool that includes an automated Common
18 Vulnerabilities and Exposures (CVE) feed. The CVE tool required by this subparagraph
19 shall provide EQUIFAX regular updates throughout each day regarding known CVEs for
20 vendor-purchased software applications in use within the EQUIFAX NETWORK.
21 EQUIFAX may satisfy its obligations under this subparagraph by using an industry-

1 standard vulnerability scanning tool. The CVE tool required by this subparagraph shall
2 also:

3 (a) Identify, confirm, and enhance discovery of the parts
4 of the EQUIFAX NETWORK that may be subject to CVE events and/or incidents;

5 (b) Scan the EQUIFAX NETWORK for CVEs; and

6 (c) Scan the EQUIFAX NETWORK to determine whether
7 scheduled security updates and patches have been successfully installed, including
8 whether any security updates or patches rated as critical have been installed consistent
9 with the requirement of this Judgment.

10 c. EQUIFAX shall appoint an individual (“Patch Supervisor”) who
11 shall report up to the Chief Technology Officer and shall be responsible for overseeing a
12 team (“Patch Management Group”) of other individuals responsible for regularly
13 reviewing and maintaining the requirements set forth in this paragraph. The Patch
14 Supervisor and the members of the Patch Management Group shall include persons with
15 appropriate experience and qualifications.

16 d. The Patch Management Group shall be responsible for:

17 i. Monitoring software and application security updates and
18 security patch management, including but not limited to, receiving notifications from the
19 tools installed pursuant to subparagraph (b) and ensuring the appropriate and timely
20 application of all security updates and/or security patches;

21 ii. Monitoring compliance with policies and procedures
22 regarding ownership, supervision, evaluation, and coordination of the maintenance,

1 management, and application of all security patches and software and application security
2 updates by appropriate information technology (IT) application and system owners;

3 iii. Supervising, evaluating, and coordinating any system patch
4 management tool(s) such as those identified in subparagraph (b); and

5 iv. A training requirement for individuals responsible for
6 implementing and maintaining EQUIFAX's patch management policies.

7 e. EQUIFAX shall use the inventory created pursuant to Paragraph 37
8 in its regular operations to assist in identifying assets within the EQUIFAX NETWORK
9 for purposes of applying security updates or security patches that have been released.

10 f. EQUIFAX shall employ processes and procedures to ensure the
11 timely scheduling and installation of any security update and security patch, considering
12 (without limitation) the severity of the vulnerability for which the update or patch has
13 been released to address, the severity of the issue in the context of the EQUIFAX
14 NETWORK, the impact on EQUIFAX's ongoing business and network operations, and
15 the risk ratings articulated by the relevant software and application vendors or
16 disseminated by the United States Computer Emergency Readiness Team (US-CERT).
17 Such patch management policies shall require EQUIFAX to rate as critical, high,
18 medium, or low all patches and/or updates, rating as "critical" all patches or updates
19 intended to prevent any vulnerability that threatens the safeguarding or security of any
20 PERSONAL INFORMATION maintained on the EQUIFAX NETWORK. If EQUIFAX
21 does not accept or increase the risk ratings disseminated by either a software or
22 application vendor or US-CERT for externally-facing applications on the EQUIFAX

1 NETWORK, EQUIFAX shall identify for any update or patch for which it is attaching
2 the lower risk rating, the assets to which it applies, and create a written explanation that
3 shall include:

4 i. A description of why the lowered risk rating is appropriate,
5 e.g., what business need or circumstance exists that supports the rating;

6 ii. A description of the alternatives that were considered, and
7 why they were not appropriate;

8 iii. An assessment of the potential risks posed by the revised risk
9 rating;

10 iv. The anticipated length of time for the rating, if the revised
11 risk rating is temporary; and

12 v. To the extent applicable, a plan for managing or mitigating
13 those risks identified in subparagraph (iii) (e.g. COMPENSATING CONTROLS,
14 alternative approaches, methods).

15 The written explanation required by this subparagraph shall be prepared within
16 twenty-four (24) hours of its determination to apply a lower rating, and upon revising the
17 rating, the update or patch shall be treated under EQUIFAX's applicable patch
18 management policies, standards, or procedures in accordance with its revised rating.

19 g. EQUIFAX shall, within twenty-four (24) hours, if feasible, but not
20 later than forty-eight (48) hours of rating any security update or patch as critical, either
21 apply the update or patch to the EQUIFAX NETWORK or take the identified application
22 offline until the update or patch has been successfully applied. If EQUIFAX is not able

1 to, within forty-eight (48) hours of rating any security update or patch as critical, either
2 apply the update or patch to the EQUIFAX NETWORK or take the identified application
3 offline, then EQUIFAX shall apply COMPENSATING CONTROLS as appropriate.

4 h. In connection with the scheduling and installation of any critical
5 patch and/or update, EQUIFAX shall verify that the patch and/or update was applied and
6 installed successfully throughout the EQUIFAX NETWORK. For each security update
7 or security patch rated as critical, EQUIFAX shall maintain records identifying: (1) each
8 critical patch or update that has been applied; (2) the date(s) each patch or update was
9 applied; (3) the assets to which each patch or update was applied; and (4) whether each
10 patch or update was applied and installed successfully (the “Critical Patch Management
11 Records”). The Critical Patch Management Records shall be reviewed on a weekly basis
12 by the Patch Management Group.

13 i. On at least a biannual basis, EQUIFAX shall perform an internal
14 assessment of its management and implementation of security updates and patches for the
15 EQUIFAX NETWORK. This assessment shall identify (i) all known vulnerabilities to
16 the EQUIFAX NETWORK and (ii) the updates or patches applied to address each
17 vulnerability. The assessment will be formally identified, documented, and reviewed by
18 the Patch Management Group.

19 **41. Information Security Program Implementation:** EQUIFAX represents
20 that it has worked and will continue to work in good faith to comply with the
21 requirements of the Information Security Program set forth in this Judgment. As to
22 Paragraphs 24, 25, 26(c), 26(d), 27, 34, 37, and 59, only, the Arizona Attorney General

1 agrees that it shall not commence any action, the purpose of which would be to establish
2 a violation of this order or a finding of contempt until on or after December 31, 2019,
3 subject also to the requirements of Paragraph 82, and that it shall not commence any
4 action, the purpose of which would be to establish a violation of Paragraph 30 or a
5 finding of contempt with respect to that paragraph, until on or after December 31, 2020,
6 subject also to the requirements of Paragraph 82.

7 **CONSUMER-RELATED RELIEF**

8 42. **Extended Credit Monitoring Services:** EQUIFAX shall offer
9 AFFECTED CONSUMERS the opportunity to enroll in credit monitoring services to be
10 provided at no cost for an aggregate of ten (10) years which may be satisfied either
11 through a court-approved settlement in the MULTI-DISTRICT LITIGATION or
12 pursuant to the Federal Trade Commission (FTC) Stipulated Order For Permanent
13 Injunction and Monetary Judgment and the Consumer Financial Protection Bureau
14 (CFPB) Stipulated Order For Permanent Injunction and Monetary Judgment. These
15 credit monitoring services shall consist of the Three-Bureau Credit Monitoring Services
16 set forth in Paragraph 43 and One-Bureau Credit Monitoring Services set forth in
17 Paragraph 44.

18 43. **Three-Bureau Credit Monitoring Services:** AFFECTED CONSUMERS
19 who file valid claims shall be eligible for at least four (4) years of a free Three-Bureau
20 Credit Monitoring Service. These four (4) years shall be provided in addition to any free
21 credit monitoring services EQUIFAX is currently providing or has previously offered as
22 a result of the 2017 DATA BREACH. The Three-Bureau Credit Monitoring Services

1 will be provided and maintained by an independent third party. The Three-Bureau Credit
2 Monitoring Services shall include:

3 a. Daily consumer CREDIT REPORT monitoring from each of the
4 three nationwide CONSUMER REPORTING AGENCIES (EIS, Experian, TransUnion)
5 showing key changes to one or more of an AFFECTED CONSUMER's CREDIT
6 REPORTS, including automated alerts when the following occur: new accounts are
7 opened; inquiries or requests for an AFFECTED CONSUMER's CREDIT REPORT for
8 the purpose of obtaining credit; changes to an AFFECTED CONSUMER's address; and
9 negative information, including delinquencies or bankruptcies.

10 b. On-demand online access to a free copy of an AFFECTED
11 CONSUMER's Experian CREDIT REPORT, updated on a monthly basis;

12 c. Automated alerts, using public or proprietary data sources, when
13 data elements submitted by an AFFECTED CONSUMER for monitoring, such as Social
14 Security number, email addresses, or credit card numbers, appear on suspicious websites,
15 including websites on the "dark web; and

16 d. One Million Dollars (\$1,000,000) in identity theft insurance to cover
17 costs related to incidents of identity theft or identity fraud, with coverage prior to the
18 AFFECTED CONSUMER's enrollment in the Three-Bureau Credit Monitoring Service,
19 provided the costs result from a stolen identity event first discovered during the policy
20 period and subject to the terms of the insurance policy.

21 44. **One-Bureau Credit Monitoring Services:** AFFECTED CONSUMERS
22 who file valid claims and enroll in Three-Bureau Credit Monitoring Services shall be

1 eligible for single-bureau credit monitoring services (“One-Bureau Credit Monitoring
2 Services”). EQUIFAX shall provide One-Bureau Credit Monitoring Services upon
3 expiration of the Three-Bureau Credit Monitoring Services to AFFECTED
4 CONSUMERS who enroll in the Three-Bureau Credit Monitoring Services. EQUIFAX
5 shall provide One-Bureau Credit Monitoring Services for the period of time necessary for
6 the aggregate number of years of credit monitoring provided under Paragraphs 43 and 44
7 to equal ten (10) years. The cost of the One-Bureau Credit Monitoring Services shall not
8 be paid from the Consumer Restitution Fund described in Section V. of this Judgment.

9 One-Bureau Credit Monitoring Services will include the following:

10 a. Daily CREDIT REPORT monitoring from EQUIFAX showing key
11 changes to an AFFECTED CONSUMER’s EIS CREDIT REPORT including automated
12 alerts when the following occur: new accounts are opened; inquiries or requests for an
13 AFFECTED CONSUMER’s CREDIT REPORT for the purpose of obtaining credit;
14 changes to an AFFECTED CONSUMER’s address; and negative information, such as
15 delinquencies or bankruptcies.

16 b. On-demand online access to a free copy of an AFFECTED
17 CONSUMER’s EIS CREDIT REPORT, updated on a monthly basis; and

18 c. Automated alerts using certain available public and proprietary data
19 sources when data elements submitted by an AFFECTED CONSUMER for monitoring,
20 such as Social Security numbers, email addresses, or credit card numbers, appear on
21 suspicious websites, including websites on the “dark web.”

1 45. For any AFFECTED CONSUMERS who were under the age of 18 on May
2 13, 2017, EQUIFAX shall offer these consumers who make valid claims the opportunity
3 to enroll in credit monitoring to achieve an aggregate of eighteen (18) years of continuous
4 credit monitoring at no cost which may be satisfied either through a court-approved
5 settlement in the MULTI-DISTRICT LITIGATION or pursuant to the FTC Stipulated
6 Order For Permanent Injunction and Monetary Judgment and the CFPB Stipulated Order
7 For Permanent Injunction and Monetary Judgment. These services shall include:

8 a. At least four (4) years of Three-Bureau Credit Monitoring Services,
9 except that during the period when an AFFECTED CONSUMER is under the age of 18,
10 the services provided will be child monitoring services where the parent or guardian can
11 enroll the AFFECTED CONSUMER under the age of 18 to receive the following
12 services: alerts when data elements submitted for monitoring appear on suspicious
13 websites, such as websites on the “dark web;” and alerts when the Social Security
14 number of an AFFECTED CONSUMER under the age of 18 is associated with new
15 names or addresses or the creation of a CREDIT REPORT at one or more of the three
16 nationwide CREDIT REPORTING AGENCIES.

17 b. Followed by no more than fourteen (14) years of One-Bureau Credit
18 Monitoring Services, except that during the period when an AFFECTED CONSUMER is
19 under the age of 18, EQUIFAX will provide child monitoring services where the parent
20 or guardian can enroll the AFFECTED CONSUMER under the age of 18 in these
21 services and must validate their status as guardian. These child monitoring services
22 include: alerts when data elements such as a Social Security number submitted for

1 monitoring appear on suspicious websites, including websites on the “dark web;” for
2 minors who do not have an EIS CREDIT REPORT, an EIS CREDIT REPORT is created,
3 locked, and then monitored, and for minors with an EIS CREDIT REPORT, their EIS
4 CREDIT REPORT is locked and then monitored.

5 46. EIS shall offer all United States consumers two free copies of their EIS
6 CREDIT REPORT every 12 months, for at least five (5) years from the implementation
7 of this paragraph. EQUIFAX shall implement this paragraph by December 31, 2019.

8 47. Consistent with, and as required by federal law, EIS shall not collect any
9 fees for creating an EIS CREDIT FILE in connection with a request from a
10 PROTECTED INDIVIDUAL to place a security freeze on his/her EIS CREDIT FILE.
11 Additionally, EIS shall not collect any fees for placing, temporarily lifting, or removing a
12 security freeze on an EIS CREDIT FILE.

13 48. EQUIFAX shall continue to refrain from charging consumers any fees for
14 any 2017 BREACH RESPONSE SERVICES AND PRODUCTS.

15 49. EQUIFAX shall not request or collect payment information (such as
16 payment card information or financial account information) from consumers during their
17 enrollment process for any 2017 BREACH RESPONSE SERVICES AND PRODUCTS
18 regardless of whether such enrollment is or was ultimately completed. This paragraph
19 shall have no impact on prior or future collection of such information if collected for
20 EQUIFAX products or services outside of any 2017 BREACH RESPONSE SERVICES
21 AND PRODUCTS.

1 50. EQUIFAX, including by or through any partner, affiliate, agent, or third
2 party, shall not use any information provided by consumers (or the fact that the consumer
3 provided information) to enroll, or to attempt to enroll, those consumers in the 2017
4 BREACH RESPONSE SERVICES AND PRODUCTS to sell, upsell, or directly market
5 or advertise its FEE-BASED PRODUCTS OR SERVICES. Nothing in this paragraph, or
6 in this Judgment, shall relieve EQUIFAX of any obligation, or prevent EQUIFAX from
7 complying with its obligations, under federal and/or state law to offer and/or advertise
8 security freezes.

9 51. Consistent with, and as required by federal law, EQUIFAX shall provide
10 information regarding security freezes on its website. EQUIFAX shall not dissuade
11 consumers from placing or choosing to place a security freeze. Should EQUIFAX offer
12 any standalone product or service as an alternative with substantially similar features as a
13 security freeze (e.g., Lock & Alert), it shall not seek to influence or persuade consumers
14 to choose the alternative product or service instead of a security freeze.

15 52. EQUIFAX shall not require consumers to agree to arbitrate disputes with
16 EQUIFAX or waive class action rights or any other private right of action against
17 EQUIFAX when receiving or enrolling in any 2017 BREACH RESPONSE SERVICES
18 AND PRODUCTS.

19 53. **Dedicated Resources for Continued 2017 BREACH RESPONSE:** For a
20 period of three (3) years from the EFFECTIVE DATE, EQUIFAX shall devote
21 reasonable and sufficient resources focused on administering its efforts to support
22

1 consumers related to the 2017 DATA BREACH (“2017 BREACH RESPONSE”),
2 including but not limited to:

3 a. Maintaining all consumer-facing internet tools and applications in
4 such a manner that they work reliably and quickly;

5 b. Establishing and maintaining sufficient staffing levels to handle the
6 volume of consumer traffic;

7 c. Training employees to provide relevant, useful, and accurate
8 information to consumers who contact EQUIFAX regarding the 2017 DATA BREACH;

9 d. Promptly handling requests by consumers to place fraud alerts or
10 security freezes consistent with, and as required by, federal law; and

11 e. Ensuring that the online resources are compliant with the Americans
12 with Disabilities Act (ADA).

13 54. EQUIFAX shall make the following digital communications available in
14 Spanish, Chinese, Tagalog, Vietnamese, Arabic, French, and Korean: (1) within sixty
15 (60) days of content being finalized, all webpages that EQUIFAX makes available on its
16 website, or on any website that it operates or controls that are dedicated to describing the
17 terms of this Judgment and any benefits available under the Judgment; (2) all legally-
18 required consumer notices regarding any future data breach that are made available on its
19 website, or on any website that it operates or controls; and (3) all notices and claim forms
20 that are made available on any website operated by the settlement administrator.
21 EQUIFAX may satisfy its obligation under this paragraph by providing an automated
22 translation function on the applicable web page(s) which automatically translates all

1 content capable of being translated by the selected translation tool, which, at a minimum,
2 shall translate text appearing directly on the website.

3 55. Placing Freezes for PROTECTED INDIVIDUALS:

4 a. Pursuant to Paragraph 51 and consistent with, and as required by,
5 federal law, EQUIFAX shall provide information regarding security freezes on its
6 webpage, including information on placing a security freeze on behalf of PROTECTED
7 INDIVIDUALS.

8 b. EIS shall place, temporarily lift, and remove a security freeze for a
9 PROTECTED INDIVIDUAL consistent with and as required by federal law.

10 c. EIS shall make good faith efforts to evaluate methods by which
11 representatives of PROTECTED INDIVIDUALS may place, temporarily lift, or remove
12 freezes on behalf of PROTECTED INDIVIDUALS and submit any required
13 documentation via a secure online connection on EQUIFAX's website and take steps to
14 implement such method(s) to the extent they are reasonably feasible and can be
15 accomplished in a manner that complies with federal law.

16 56. **Consumer Assistance Process:** As part of or in addition to that which is
17 required by federal and state law, EIS shall continue to offer direct assistance, processes,
18 and informational resources to United States consumers who have questions about their
19 EIS CREDIT FILE, who wish to place a fraud alert and/or security freeze on their EIS
20 CREDIT FILE, or who have or may have been the victim of fraud or identity theft.
21 These processes shall include the ability for consumers to contact EIS online, by toll-free
22

1 phone numbers, and by United States mail, or any other reasonably accessible means
2 established by EIS to communicate directly with consumers.

3 a. At a minimum, EIS shall:

4 i. Handle consumer complaints regarding identity theft or
5 fraudulent activity, which may include dedicated teams to review and handle referred
6 complaints by the Consumer Financial Protection Bureau, Federal Trade Commission, or
7 other equivalent federal agency, and the Arizona Attorney General;

8 ii. Provide direct assistance and informational resources,
9 including, for example, sample template letters and checklists, to help consumers
10 understand their EIS CREDIT FILES and submit disputes related to their EIS CREDIT
11 FILES;

12 iii. Assist consumers in fulfilling requests for fraud alerts and
13 placing, temporarily lifting, or removing a security freeze on their EIS CREDIT FILE, as
14 well as provide information on how to contact the other CONSUMER REPORTING
15 AGENCIES to place, temporarily lift, or remove a security freeze;

16 iv. Fulfill its responsibilities to REINVESTIGATE consumers'
17 disputes that information on their EIS CREDIT FILE is inaccurate or incomplete
18 including, as appropriate, escalating disputes for fraud and identity theft to agents
19 specially trained in fraud and identity theft protection;

20 v. Maintain enhanced consumer dispute results letters to assist
21 consumers in understanding the basis and results of EIS's REINVESTIGATION process,
22 including the actions taken by EIS as a result of the consumer's dispute, the role of the

1 FURNISHER in the REINVESTIGATION process, the results of the dispute including
2 any modified or deleted information, and the options the consumer may take if
3 dissatisfied with the results of the REINVESTIGATION;

4 vi. Provide informational resources on what supporting and
5 relevant consumer documents may assist a consumer in disputing information on his/her
6 EIS CREDIT FILE and the methods available for consumers to submit documents;

7 vii. Assist consumers who contact EIS in understanding the basis
8 for when EIS declines to block or rescinds a block of information previously disputed as
9 a result of an alleged identity theft;

10 viii. Assist consumers disputing inaccurate or fraudulent
11 information and/or accounts by facilitating dispute or REINVESTIGATION requests
12 with FURNISHERS via the Automated Consumer Dispute Verification (ACDV) process;

13 and

14 ix. Refer consumers to available federal, state, and/or local
15 resources for additional information about consumer rights and identity theft protection
16 measures, such as the sources found at <https://www.identitytheft.gov>.

17 b. EIS shall provide direct assistance to members of the United States armed
18 forces, including without limitation members of the National Guard and military reserve,
19 (collectively “Service Members”), or their spouses or other dependents (collectively
20 “Military Families”). At a minimum, EIS shall train a department or group to: help
21 Service Members and Military Families review their EIS CREDIT FILES; review
22 complaints regarding identity theft or fraudulent activity; and help Service Members and

1 Military Families place a security freeze on their EIS CREDIT FILES and implement
2 active duty alerts.

3 c. EQUIFAX shall designate a department or group to act as the point
4 of contact for the Arizona Attorney General to directly contact and which will provide
5 assistance to consumers who have submitted complaints to the Arizona Attorney
6 General's Office. This department or group shall be trained in the specific provisions of
7 this paragraph.

8 d. EQUIFAX shall develop a method to identify and track consumer
9 complaints related to the 2017 DATA BREACH and report these metrics to the
10 MULTISTATE LEADERSHIP COMMITTEE as part of the Consumer Remedies
11 Reports required by Paragraph 62 of this Judgment.

12 e. Disclosure of the Consumer Assistance Process

13 i. EQUIFAX shall CLEARLY AND CONSPICUOUSLY
14 disclose on its website the following components of the Consumer Assistance Process:
15 the existence of the processes and informational resources offered by EQUIFAX; the
16 content of and how to access an EIS CREDIT FILE; the methods to request a fraud or
17 active duty alert, or take advantage of any security freeze feature on an EIS CREDIT
18 FILE; the methods to dispute the accuracy or completeness of an item on an EIS
19 CREDIT FILE; and informational materials for Service Members and Military Families.
20 EQUIFAX may comply with this paragraph by: (1) maintaining a dedicated website page
21 that describes or provides the resources set forth above; and (2) providing the consumer
22 with a link to said dedicated website page.

1 ii. For telephone calls with consumers related to the 2017 DATA
2 BREACH, EQUIFAX shall train staff to be prepared to discuss or address in appropriate
3 circumstances: the existence of the processes and informational resources offered by
4 EQUIFAX; the content of and how to access an EIS CREDIT FILE; the methods to
5 request a fraud or active duty alert, or take advantage of any security freeze feature on an
6 EIS CREDIT FILE; the methods to dispute the accuracy or completeness of an item on
7 an EIS CREDIT FILE; and informational materials for Service Members and Military
8 Families. EQUIFAX shall also maintain documentation of this training.

9 f. EQUIFAX shall maintain reasonable and sufficient staffing levels,
10 resources, and support necessary to respond to foreseeable consumer contact volume.

11 g. The Arizona Attorney General agrees that it shall not commence any
12 action, the purpose of which would be to establish a violation of this paragraph or a
13 finding of contempt with respect to this paragraph, until on or after December 31, 2019,
14 subject also to the requirements of Paragraph 82.

15 57. **Declining to Block Information in a CREDIT FILE:** If EIS declines to
16 block, as that term is used in FCRA, or rescinds any block on, the information in a
17 CREDIT FILE that the consumer identifies as information that resulted from an alleged
18 identity theft, EIS shall provide the consumer with additional steps the consumer can take
19 if the REINVESTIGATION of such information results in the information remaining on
20 the consumer's CREDIT FILE, including his/her ability to utilize the Escalated Identity
21 Theft Block Process set forth in Paragraph 58. EIS can choose to satisfy this provision
22 by drafting a form letter to send to consumer that provides this information. This

1 paragraph shall not limit or restrict EIS's ability to designate a dispute filing frivolous or
2 abusive disputes pursuant to 15 U.S.C. § 1681i(a)(3). The Arizona Attorney General
3 agrees that it shall not commence any action, the purpose of which would be to establish
4 a violation of this paragraph or a finding of contempt with respect to this paragraph, until
5 on or after December 31, 2019, subject also to the requirements of Paragraph 82.

6 **58. Escalated Identity Theft Block Process:** If a consumer complains to a
7 State Attorney General that EIS declined to either block information or rescind the block
8 of information, the Arizona Attorney General may send such complaint to the department
9 or group designated pursuant to Paragraph 56(c) of this Judgment. Upon referral, EIS
10 will review and process the consumer's identity theft report and shall take appropriate
11 action to block the noted information or decline to block or rescind a block, as applicable,
12 from the consumer's EIS CREDIT FILE. This paragraph shall not limit or restrict EIS's
13 ability to designate a dispute filing frivolous or abusive disputes pursuant to 15 U.S.C. §
14 1681i(a)(3).

15 **59. Consumer Transparency:** EQUIFAX shall post on the homepage of any
16 website owned or controlled by EQUIFAX: a notice that details categories of the
17 PERSONAL INFORMATION EQUIFAX collects and maintains, including NON-FCRA
18 INFORMATION; how EQUIFAX collects the PERSONAL INFORMATION; how
19 EQUIFAX uses the PERSONAL INFORMATION; how EQUIFAX protects the
20 PERSONAL INFORMATION; whether EQUIFAX shares the PERSONAL
21 INFORMATION with others, and if so, what PERSONAL INFORMATION is shared
22 and the categories of persons or entities with whom the PERSONAL INFORMATION is

1 shared; and whether consumers have control over their PERSONAL INFORMATION,
2 and if so, what kind of control they have and how to exercise the control. If EQUIFAX's
3 PERSONAL INFORMATION practices change, the notice shall be updated to reflect
4 those changes. EQUIFAX may comply with this paragraph by including this information
5 in its online privacy notices.

6 60. Unless otherwise specified herein, Paragraphs 42 through 59 shall apply for
7 seven (7) years from the EFFECTIVE DATE.

8 **ASSESSMENT AND REPORTING REQUIREMENTS TO THE**
9 **ATTORNEY GENERAL**

10 61. **Third-Party Assessment:** During the time period established in
11 Paragraph 13, EQUIFAX shall obtain from an independent third party an initial
12 assessment, followed by biennial assessments of the Information Security Program
13 required under the terms of this Judgment (the "Third-Party Assessments"). The Third-
14 Party Assessments required by this paragraph shall be conducted by a third-party (the
15 "Third-Party Assessor").

16 a. The findings of each of the Third-Party Assessments shall be
17 documented in individual reports (the "Third-Party Assessor's Reports") that shall:

18 i. Identify the specific administrative, technical, and physical
19 safeguards maintained by EQUIFAX's Information Security Program;

20 ii. Document the extent to which the identified administrative,
21 technical and physical safeguards are appropriate considering EQUIFAX's size and
22

1 complexity, the nature and scope of EQUIFAX’s activities, and the sensitivity of the
2 PERSONAL INFORMATION maintained on the EQUIFAX NETWORK; and

3 iii. Assess the extent to which the administrative, technical, and
4 physical safeguards that have been implemented by EQUIFAX meet the requirements of
5 the Information Security Program.

6 b. EQUIFAX may fulfill its assessment and reporting obligations under
7 this paragraph by providing a copy of the Third Party Assessor’s Report required under
8 the FTC Stipulated Order For Permanent Injunction and Monetary Judgment and the
9 CFPB Stipulated Order For Permanent Injunction and Monetary Judgment (the “Federal
10 Security Assessment Report”) to the California Attorney General’s Office during the time
11 period set forth in Paragraph 13. The California Attorney General’s Office may provide
12 a copy of the Federal Security Assessment Report received from EQUIFAX to the
13 Arizona Attorney General’s Office upon request.

14 c. Any Third Party Assessor’s Report provided pursuant to this
15 paragraph and all information contained therein, to the extent permitted by the laws of the
16 State of Arizona shall be treated by the Arizona Attorney General’s Office as
17 confidential; shall not be shared or disclosed except as described in subsection b; and
18 shall be treated by the Arizona Attorney General’s Office as exempt from disclosure
19 under the relevant public records laws of the State of Arizona. In the event that the
20 Arizona Attorney General’s Office receives any request from the public to inspect any
21 Third Party Assessor’s Report provided pursuant to this paragraph or other confidential
22 documents under this Judgment and believes that such information is subject to

1 disclosure under the relevant public records laws, the Attorney General’s Office agrees to
2 provide EQUIFAX with at least ten (10) days advance notice before producing the
3 information, to the extent permitted by state law (and with any required lesser advance
4 notice), so that EQUIFAX may take appropriate action to defend against the disclosure of
5 such information. The notice under this paragraph shall be provided consistent with the
6 notice requirements contained in Paragraph 81. Nothing contained in this subparagraph
7 shall alter or limit the obligations of the Arizona Attorney General that may be imposed
8 by the relevant public records laws of the State of Arizona, or by order of any court,
9 regarding the maintenance or disclosure of documents and information supplied to the
10 Arizona Attorney General except with respect to the obligation to notify EQUIFAX of
11 any potential disclosure.

12 62. Consumer Relief and Internal Metrics Report: EQUIFAX shall prepare a
13 report regarding its compliance with Paragraphs 53, 55, and 56 (“Consumer Remedies
14 Report”) as outlined below.

15 a. The reporting periods for the Consumer Remedies Reports must
16 cover: (1) the first one-hundred and eighty (180) days after the EFFECTIVE DATE for
17 the initial Consumer Remedies Report; and (2) each one-year period thereafter for the
18 following five (5) years.

19 b. The Consumer Remedies Reports shall include the following
20 information and metrics:

21 i. An organizational chart identifying the individuals employed
22 or contracted by EQUIFAX to respond to consumer complaints related to the 2017

1 DATA BREACH as specified in Paragraph 56(d) and complaints submitted through a
2 State Attorney General as specified in Paragraph 56(c), identified by their titles with a
3 number designating how many staff are assigned to each position;

4 ii. A description of the training EQUIFAX provides to first-line
5 employees or contractors responsible for directly responding to consumers;

6 iii. A count of the number of complaints EQUIFAX received,
7 broken down by telephone, email, or regular mail, in which the consumer's complaint
8 relates to the 2017 DATA BREACH as specified in Paragraph 56(d);

9 iv. The number of fraud alerts placed on EIS CREDIT FILES for
10 United States consumers;

11 v. The number of security freezes placed, temporarily lifted, or
12 permanently removed on EIS CREDIT FILES;

13 vi. The number of security freezes placed on behalf of
14 PROTECTED CONSUMERS on EIS CREDIT FILES;

15 vii. The number of complaints received by EQUIFAX from the
16 Arizona Attorney General's Office pursuant to Paragraph 56(c); and

17 viii. For the complaints listed in subsection vii EQUIFAX shall
18 indicate whether they were resolved within fifteen (15) business days.

19 c. Each Consumer Remedies Report must be completed within sixty
20 (60) days after the end of the reporting period to which the Consumer Remedies Report
21 applies. EQUIFAX shall provide a copy of the Consumer Remedies Report to the
22

1 California Attorney General's Office within ten (10) business days of the completion of
2 the Consumer Remedies Report.

3 d. The California Attorney General's Office may provide a copy of the
4 Consumer Remedies Reports received from EQUIFAX to the Arizona Attorney General
5 upon request.

6 e. The Consumer Remedies Reports and all information contained
7 therein, to the extent permitted by the laws of the State of Arizona: shall be treated by
8 the Arizona Attorney General's Office as confidential; shall not be shared or disclosed
9 except as described in subsection (d); and shall be treated by the Arizona Attorney
10 General's Office as exempt from disclosure under the relevant public records laws of the
11 State of Arizona. In the event that the Arizona Attorney General's Office receives any
12 request from the public for a Consumer Remedies Report or other confidential documents
13 under this Judgment and believes that such information is subject to disclosure under the
14 relevant public records laws, the Arizona Attorney General's Office agrees to provide
15 EQUIFAX with at least ten (10) days advance notice before producing the information, to
16 the extent permitted by state law (and with any required lesser advance notice), so that
17 EQUIFAX may take appropriate action to defend against the disclosure of such
18 information. The notice under this paragraph shall be provided consistent with the notice
19 requirements contained in Paragraph 81. Nothing contained in this subparagraph shall
20 alter or limit the obligations of the Arizona Attorney General that may be imposed by the
21 relevant public records laws of the State of Arizona, or by order of any court, regarding
22 the maintenance or disclosure of documents and information supplied to Arizona

1 Attorney General except with respect to the obligation to notify EQUIFAX of any
2 potential disclosure.

3 **IV. DOCUMENT RETENTION**

4 63. EQUIFAX shall retain and maintain the reports, records, exceptions,
5 information and other documentation required by Paragraphs 31(a), 36(c), 37, 40(a),
6 40(f), 40(h), 40(i), 61, and 62 for a period of no less than seven (7) years.

7 **V. CONSUMER RESTITUTION**

8 64. Consumer Restitution Fund:

9 a. EQUIFAX shall pay the ATTORNEYS GENERAL an amount of at
10 least Three Hundred Million Dollars (\$300,000,000), and no more than Four Hundred
11 and Twenty-Five Million (\$425,000,000), for the purpose of providing restitution to
12 AFFECTED CONSUMERS, including the cost of the Three-Bureau Credit Monitoring
13 Services set forth in Paragraph 43 and the monitoring for minors set forth in Paragraph
14 45(a).

15 b. The payment/s required by this paragraph may be satisfied in its or
16 their entirety by Equifax Inc. making the payments described in subsection (a) into a fund
17 (the "Consumer Restitution Fund") established pursuant to a court-approved settlement in
18 the MULTI-DISTRICT LITIGATION that pays for restitution and redress to
19 AFFECTED CONSUMERS that includes the Three-Bureau Credit Monitoring Services
20 set forth in Paragraph 43 and the monitoring for minors set forth in Paragraph 45(a) and
21 may also include other restitution and redress to AFFECTED CONSUMERS provided
22 through the MULTI-DISTRICT LITIGATION.

1 c. The Consumer Restitution Fund shall be established and
2 administered, payments shall be made by Equifax Inc., and consumer restitution shall be
3 disbursed from the Consumer Restitution Fund in accordance with the terms of the court-
4 approved settlement in the MULTI-DISTRICT LITIGATION.

5 d. If the FTC and the CFPB jointly issue a written notice of termination
6 pursuant Section XI(A) of the FTC Stipulated Order For Permanent Injunction and
7 Monetary Judgment and Section XI.I of the CFPB Stipulated Order For Permanent
8 Injunction and Monetary Judgment, the Arizona Attorney General and EQUIFAX agree
9 that the payment/s required by this paragraph may instead be satisfied in its or their
10 entirety by:

11 i. EQUIFAX making payments in accordance with the terms of
12 the FTC and CFPB Stipulated Orders For Permanent Injunction and Monetary Judgment.
13 Such amounts shall be deposited into a fund and administered by the FTC or its designee
14 in accordance with the terms of the FTC and CFPB Stipulated Orders for Permanent
15 Injunction and Monetary Judgment to be used for consumer restitution and redress on
16 behalf of the FTC, CFPB, and ATTORNEYS GENERAL; and

17 ii. The MULTISTATE LEADERSHIP COMMITTEE and
18 EQUIFAX will coordinate with the FTC and/or CFPB so that AFFECTED
19 CONSUMERS receive materially similar restitution as that set forth in Paragraphs 43 and
20 45(a) of this Judgment.

1 **VI. MONETARY PAYMENT**

2 65. No later than thirty (30) days after the EFFECTIVE DATE, Equifax, Inc.
3 shall pay a total of One Hundred and Seventy Five Million Dollars (\$175,000,000.00) to
4 the ATTORNEYS GENERAL, which is to be divided amongst the ATTORNEYS
5 GENERAL. The amount apportioned to the Arizona Attorney General is to be paid by
6 Equifax Inc. directly to the Arizona Attorney General in an amount to be designated by
7 and in the sole discretion of the MULTISTATE LEADERSHIP COMMITTEE. The
8 amounts and wiring instructions shall be provided to Equifax Inc. no later than seven (7)
9 days after the EFFECTIVE DATE. If the Court has not entered this Judgment by the
10 EFFECTIVE DATE, Equifax Inc. shall make the payment within thirty (30) days of the
11 EFFECTIVE DATE or within fourteen (14) days of the entry of the Judgment, whichever
12 is later. Said payment shall be used for additional consumer relief; reimbursement of
13 attorney fees and other costs of investigation and litigation; distribution or application to
14 any applicable consumer protection enforcement funds, including future consumer
15 protection enforcement, consumer education, litigation or local consumer aid, or
16 revolving funds; defraying the costs of the inquiry leading hereto; or any other lawful
17 purpose, at the sole discretion of the Arizona Attorney General.

18 **VII. RELEASE**

19 66. Following full payment of the amounts due under this Judgment, the
20 Arizona Attorney General shall release and discharge EQUIFAX and its directors,
21 officers, and employees from all civil claims alleged in the Complaint, and any civil
22 claims that it could have brought based on EQUIFAX's conduct related to the 2017

1 DATA BREACH under the CFA, A.R.S. § 18-545, A.R.S. § 18-552, the Fair Credit
2 Reporting Act, 15 U.S.C. § 1681 *et seq.*, and any state credit reporting law, or common
3 law claims, including those concerning unfair, deceptive, or fraudulent trade practices.
4 Nothing contained in this paragraph shall be construed to limit the ability of the Arizona
5 Attorney General to enforce the obligations that EQUIFAX has under this Judgment.

6 67. Notwithstanding any term of this Judgment, any and all of the following
7 forms of liability are specifically reserved and excluded from the release in Paragraph 66
8 as to any entity or person, including EQUIFAX:

9 a. Any criminal liability that any person or entity, including
10 EQUIFAX, has or may have to the States.

11 b. Any civil or administrative liability that any person or entity,
12 including EQUIFAX, has or may have to the States under any statute, regulation or rule
13 giving rise to, any and all of the following claims:

14 i. State or federal antitrust violations;

15 ii. State or federal securities violations; or

16 iii. State or federal tax claims.

17 68. Nothing in this Judgment shall be construed as excusing or exempting
18 EQUIFAX from complying with any state or federal law, rule, or regulation, nor shall
19 any of the provisions of this Judgment be deemed to authorize or require EQUIFAX to
20 engage in any acts or practices prohibited by any law, rule, or regulation.

1 **VIII. NO ADMISSION OF LIABILITY**

2 69. **Violations of Law:** In stipulating to the entry of this Judgment, EQUIFAX
3 does not admit to any violation of or liability arising from any state, federal, or local law.

4 70. **Admissions of Fact:** EQUIFAX does not admit to any fact alleged in the
5 Complaint, except admits that on March 8, 2017, it received notification of a
6 vulnerability in Apache Struts open-source software (CVE-2017-5638) prior to the 2017
7 DATA BREACH.

8 71. Nothing contained in this Judgment shall be construed as an admission or
9 concession of liability by EQUIFAX, or create any third-party beneficiary rights or give
10 rise to or support any right of action in favor of any consumer or group of consumers, or
11 confer upon any person other than the parties hereto any rights or remedies. By entering
12 into this Judgment, EQUIFAX does not intend to create any legal or voluntary standard
13 of care and expressly denies that any practices, policies, or procedures inconsistent with
14 those set forth in this Judgment violate any applicable legal standard. This Judgment is
15 not intended to be and shall not be construed as, deemed to be, represented as, or relied
16 upon in any manner by any party in any civil, criminal, or administrative proceeding
17 before any court, administrative agency, arbitration, or other tribunal as an admission,
18 concession, or evidence that EQUIFAX has violated any federal, state, or local law, or
19 that EQUIFAX's current or prior practices related to the 2017 DATA BREACH or its
20 information security program is or was not in accordance with any federal, state, or local
21 law.

1 **IX. GENERAL PROVISIONS**

2 72. Nothing herein shall be construed to exonerate any failure to comply with
3 any provision of this Judgment after the EFFECTIVE DATE, or to compromise the
4 authority of the Arizona Attorney General to initiate a proceeding for any failure to
5 comply with this Judgment.

6 73. Nothing in this Judgment shall be construed to limit the authority or ability
7 of the Arizona Attorney General to protect the interests of Arizona or the people of
8 Arizona. This Judgment shall not bar the Arizona Attorney General or any other
9 governmental entity from enforcing laws, regulations, or rules against EQUIFAX for
10 conduct subsequent to or otherwise not covered by this Judgment. Further, nothing in
11 this Judgment shall be construed to limit the ability of the Arizona Attorney General to
12 enforce the obligations that EQUIFAX has under this Judgment.

13 74. Nothing in this Judgment shall be construed as relieving EQUIFAX of the
14 obligation to comply with all state and federal laws, regulations, and rules, nor shall any
15 of the provisions of this Judgment be deemed to be permission to engage in any acts or
16 practices prohibited by such laws, regulations, and rules.

17 75. EQUIFAX shall deliver a copy of this Judgment to, and otherwise fully
18 apprise, its Chief Executive Officer, Chief Technology Officer, Chief Information
19 Security Officer, each of its Business Information Security Officers, Patch Supervisor
20 designated pursuant to this Judgment, General Counsel, and Board of Directors within
21 ninety (90) days of the EFFECTIVE DATE. To the extent EQUIFAX replaces any of the
22 above listed officers, counsel, or Directors, EQUIFAX shall deliver a copy of this

1 Judgment to their replacements within ninety (90) days from the date on which such
2 person assumes his/her position with EQUIFAX.

3 76. EQUIFAX shall pay all court costs associated with the filing of this
4 Judgment.

5 77. EQUIFAX shall not participate in any activity or form a separate entity or
6 corporation for the purpose of engaging in acts or practices in whole or in part that are
7 prohibited by this Judgment or for any other purpose that would otherwise circumvent
8 any term of this Judgment. EQUIFAX shall not knowingly cause, permit, or encourage
9 any other persons or entities acting on its behalf, to engage in practices prohibited by this
10 Judgment.

11 78. EQUIFAX agrees that this Judgment does not entitle it to seek or to obtain
12 attorneys' fees as a prevailing party under any statute, regulation, or rule, and EQUIFAX
13 further waives any right to attorneys' fees that may arise under such statute, regulation, or
14 rule.

15 79. This Judgment shall not be construed to waive any claims of sovereign
16 immunity Arizona may have in any action or proceeding.

17 80. If any portion of this Judgment is held invalid or unenforceable, the
18 remaining terms of this Judgment shall not be affected and shall remain in full force and
19 effect.

20 81. Whenever EQUIFAX shall provide notice to the Arizona Attorney General
21 under this Judgment, that requirement shall be satisfied by sending notice to: John C.
22 Gray, Senior Litigation Counsel, Office of the Arizona Attorney General, 2005 N.

1 Central Ave., Phoenix, AZ 85004. Any notices or other documents sent to EQUIFAX
2 pursuant to this Judgment shall be sent to the following address: Chief Legal Officer,
3 Equifax Inc., 1550 Peachtree Street, N.W., Atlanta, GA 30309; Phyllis Sumner, King &
4 Spalding LLP, 1180 Peachtree Street, N.E., Suite 1600, Atlanta, GA 30309; and Zachary
5 Fardon, King & Spalding LLP, 444 West Lake Street, Suite 1650, Chicago, IL 60606.
6 All notices or other documents to be provided under this Judgment shall be sent by
7 United States mail, certified mail return receipt requested, or other nationally recognized
8 courier service that provides for tracking services and identification of the person signing
9 for the notice or document, and shall have been deemed to be sent upon mailing. Any
10 party may update its designee or address by sending written notice to the other party
11 informing them of the change.

12 82. If the Arizona Attorney General reasonably believes that EQUIFAX has
13 failed to comply with any of Paragraphs 9 through 63 of this Judgment, and if in the
14 Arizona Attorney General's sole discretion the failure to comply does not threaten the
15 health or safety of the citizens of the State of Arizona and/or does not create an
16 emergency requiring immediate action, the Arizona Attorney General shall provide
17 notice to EQUIFAX of such alleged failure to comply and EQUIFAX shall have thirty
18 (30) days from receipt of such notice to provide a good faith written response, including
19 either a statement that EQUIFAX believes it is in full compliance with the relevant
20 provision or a statement explaining how the violation occurred, how it has been
21 addressed or when it will be addressed, and what EQUIFAX will do to make sure the
22 violation does not occur again. The Arizona Attorney General may agree to provide

1 EQUIFAX with more than thirty (30) days to respond. The Arizona Attorney General
2 shall receive and consider the response from EQUIFAX prior to initiating any proceeding
3 for any alleged failure to comply with this Judgment.

4 83. In the event that technological or industry developments or other
5 intervening changes in law or fact cause EQUIFAX to believe that elimination or
6 modification of this Judgment is warranted or appropriate, EQUIFAX will provide notice
7 to the Arizona Attorney General. If the Parties reach a mutual agreement that elimination
8 or modification of a provision is appropriate, they may jointly petition the Court to
9 eliminate or modify such provision. If the Parties fail to reach an agreement, EQUIFAX
10 may petition the Court to eliminate or modify such provision.

11 84. Jurisdiction is retained by the Court for the purpose of enabling any party to
12 the Judgment to apply to the Court at any time for such further orders and directions as
13 may be necessary or appropriate for the construction or the carrying out of this Judgment,
14 for the modification of any of the injunctive provisions hereof, for enforcement of
15 compliance herewith, and for the punishment of violations hereof, if any.

16 85. The clerk is ordered to enter this Judgment forthwith.

17 **X. FINAL JUDGMENT**

18 86. No further matters remain pending, and this final CONSENT JUDGMENT
19 is entered under Arizona Rule of Civil Procedure 54(c).
20

21 DATED: _____

JUDGE OF THE SUPERIOR COURT

1 **CONSENT TO JUDGMENT**

2 1. Defendant acknowledges that it has waived service of the Complaint in this
3 matter, is aware of its right to a trial in this matter, and has waived the same.

4 2. Defendant admits the jurisdiction of this Court and consents to the entry of
5 the foregoing Consent Judgment.

6 3. Except as expressly set forth in this Consent Judgment, Defendant states
7 that no promise of any kind or nature whatsoever was made to induce it to enter into this
8 Consent Judgment and declares that it has entered into this Consent Judgment
9 voluntarily.

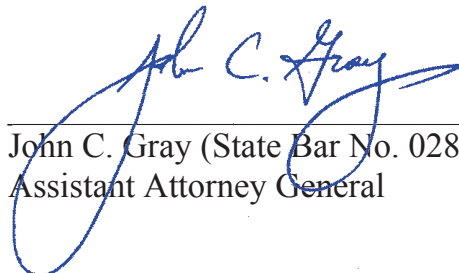
10 4. This Consent Judgment is entered as a result of a compromise and a
11 settlement agreement between the parties. Only the parties to this action may seek
12 enforcement of this Consent Judgment. Nothing herein is intended to create a private
13 right of action by other parties.

14 5. Defendant represents and warrants that the person signing below on its
15 behalf is duly appointed and authorized to do so.

16
17 DATED this 19th day of July 2019.

18
19 STATE OF ARIZONA, *ex rel.* MARK BRNOVICH,
20 ATTORNEY GENERAL

21 By:



22 John C. Gray (State Bar No. 028454)
Assistant Attorney General

1 Office of the Attorney General
2 2005 North Central Avenue
3 Phoenix, AZ 85004
4 Telephone: (602) 542-3725
5 Facsimile: (602) 542-4377
6 Email: consumer@azag.gov

7 DEFENDANT EQUIFAX INC.

8 By:


9 Whitney DuPree

10 Local Counsel for Equifax Inc.
11 Arizona Bar No. 035061
12 King & Spalding LLP
13 1180 Peachtree Street NE
14 Suite 1600
15 Atlanta, GA 30309
16 Tel.: (404) 215-5755
17 wdupree@kslaw.com

18 By:


19 PHYLLIS B. SUMNER

20 CHRISTOPHER C. BURRIS
21 SHANNON F. COX
22 STEPHEN P. CUMMINGS
KING & SPALDING LLP
1180 Peachtree Street, N.E.
Atlanta, Georgia 30309
Tel.: (404) 572-4600
Fax: (404) 572-5140

and

ZACHARY FARDON
KING & SPALDING LLP
444 W. Lake Street
Suite 1650
Chicago, Illinois 60606
Tel.: (312) 995-6333
Fax: (312) 995-6330

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22

psumner@kslaw.com
zfardon@kslaw.com
cburris@kslaw.com
scox@kslaw.com
scummings@kslaw.com