TIMOTHY C. FOX
Montana Attorney General
MARK W. MATTIOLI
Bureau Chief
Kelley Hubbard
Assistant Attorney General
Montana Office of Consumer Protection
P.O. Box 200151
Helena, MT 59620-0151
(406) 444-2026
mmattioli@mt.gov

MONTANA FIRST JUDICIAL DISTRICT COURT LEWIS & CLARK COUNTY

STATE OF MONTANA, Plaintiff, **v.** **EQUIFAX INC., a corporation,** Defendant.	Case No. **CONSENT JUDGMENT AND PERMANENT INJUNCTION**

Plaintiff, the People of the State of State of Montana ("the People" or "Plaintiff"), appearing through its attorney, Timothy C. Fox, Attorney General of the State of Montana, and Defendant Equifax Inc., a corporation ("Defendant"), appearing through its attorney, Sheldon Bradshaw of King & Spalding LLP, having stipulated to the entry of this Final Judgment and Permanent Injunction ("Judgment") by the Court without the taking of proof and without trial or adjudication of any fact or law, without this Judgment constituting evidence of or an admission by Equifax Inc. regarding any issue of law or fact alleged in the Complaint on file, and without Equifax Inc. admitting any liability, and with all parties having waived their right to appeal, and the Court having considered the matter and good cause appearing:

IT IS HEREBY ORDERED, ADJUDGED, AND DECREED THAT:

I. PARTIES AND JURISDICTION

1. The State of Montana is the Plaintiff in this case.

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

3. The Court has jurisdiction over the subject matter of this action and jurisdiction over the parties to this action, and venue is proper in this Court. Mont. Code Ann. § 30-14-111; Mont. Code Ann. § 30-14-1705.

4. Defendant, at all relevant times, has transacted business in the State of Montana, including, but not limited to, Lewis & Clark County.

5. This Judgment is entered pursuant to and subject to Parts 1 and 17 of the Montana Unfair Trade Practices and Consumer Protection Act, Mont. Code Ann. § 30-14-101 to -144; 30-14-1701 to 1736].

II. DEFINITIONS

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

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

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

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

d. "ATTORNEYS GENERAL" shall mean the Attorneys General of the states and commonwealths of: Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii,[1] Idaho, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Puerto Rico, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Utah,[2] Vermont, Virginia, Washington, West Virginia, Wisconsin, and Wyoming, and the District of Columbia.

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

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

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

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

[1] Hawaii is represented by its Office of Consumer Protection. For simplicity 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.

[2] Claims pursuant to the Utah Protection of Personal Information Act are brought under the direct enforcement authority of the Attorney General. Utah Code § 13-44-301(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.

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

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

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

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

j. "EFFECTIVE DATE" shall be August 22, 2019 except as otherwise noted in the Judgment.

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

l. "EQUIFAX" shall mean Equifax Inc., its affiliates, directors, officers, subsidiaries and divisions, successors and assigns doing business in the United States.

m. "EQUIFAX NETWORK" shall mean all networking equipment, databases or data stores, applications, servers, and endpoints that: (1) are capable of using and sharing software, data, and hardware resources; (2) are owned, operated, and/or controlled by EQUIFAX; and (3) collect, process, store, or have access to PERSONAL INFORMATION of consumers who reside in the United States. For purposes of this Judgment, EQUIFAX

NETWORK shall not include networking equipment, databases or data stores, applications, servers, or endpoints outside of the United States, which are not used to collect, process, or store PERSONAL INFORMATION, and where access to PERSONAL INFORMATION is restricted using a risk-based control. For purposes of this definition, a risk-based control shall, at a minimum, include: (i) web-application-, network-, or host-based firewalls, or ENCRYPTION of the PERSONAL INFORMATION; and (ii) preadmission identification and/or access management controls, including, for example, multi-factor authentication.

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

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

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

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

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

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

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

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

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

u. "PERSONAL INFORMATION" shall mean information regarding an individual residing in Montana that falls within one of the following categories:

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

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

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

iv. Any category of personal information found in the definition as set forth in Mont. Code Ann. § 30-14-1702(7) as of September 7, 2017.

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

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

x. "SECURITY EVENT" shall mean any compromise, or threat that gives rise to a reasonable likelihood of compromise, by unauthorized access or inadvertent disclosure impacting the confidentiality, integrity, or availability of PERSONAL INFORMATION of at

least 500 United States consumers held or stored within the EQUIFAX NETWORK, including but not limited to a data breach. For purposes of this definition, "availability" shall not include an intentional limitation on the availability of PERSONAL INFORMATION, such as for purposes of performing maintenance on the EQUIFAX NETWORK.

III. INJUNCTIVE RELIEF

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

8. The injunctive terms contained in this Judgment are being entered pursuant to Parts 1 and 17 of the Montana Unfair Trade Practices and Consumer Protection Act, including, without limitation, Mont. Code Ann. §§ 30-14-111 and 30-14-1705.

COMPLIANCE WITH LAW

9. EQUIFAX shall comply with the Montana Unfair Trade Practices and Consumer Protection Act, specifically including, without limitation, Part 17, Impediment of Identify Theft in connection with its collection, maintenance, and safeguarding of PERSONAL INFORMATION of consumers in Montana.

10. EQUIFAX shall not make a misrepresentation which is capable of misleading consumers or fail to state a material fact if that failure is capable of misleading consumers regarding the extent to which EQUIFAX maintains and/or protects the privacy, security, confidentiality, or integrity of any PERSONAL INFORMATION collected from or about consumers.

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

12. EQUIFAX shall comply with the Part 17 of the Montana Unfair Trade Practices and Consumer Protection Act, including, without limitation, Mont. Code Ann. § 30-14-1704.

INFORMATION SECURITY PROGRAM

13. Within ninety (90) days after the EFFECTIVE DATE and for a period of seven (7) years, EQUIFAX shall implement, maintain, regularly review and revise, and comply with a comprehensive information security program ("Information Security Program") the purpose of

which shall be to take reasonable steps to protect the confidentiality, integrity, and availability of PERSONAL INFORMATION on the EQUIFAX NETWORK. EQUIFAX's Information Security Program shall be documented in the GOVERNANCE PROCESSES and shall contain administrative, technical, and physical safeguards appropriate to:

a. The size and complexity of EQUIFAX's operations;

b. The nature and scope of EQUIFAX's activities; and

c. The sensitivity of the PERSONAL INFORMATION on the EQUIFAX NETWORK.

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

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

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

16. EQUIFAX shall employ an executive or officer who shall be responsible for implementing, maintaining, and monitoring the Information Security Program (for ease, hereinafter referred to as the "Chief Information Security Officer"). The Chief Information Security Officer shall have the education, qualifications, and experience appropriate to the level, size, and complexity of her/his role in implementing, maintaining, and monitoring the Information Security Program. This Chief Information Security Officer shall report annually to the EQUIFAX Board of Directors on the adequacy of EQUIFAX's Information Security Program. The Chief Information Security Officer shall also, at any meeting of the Board of Directors concerning the security posture or security risks faced by EQUIFAX and at each quarterly meeting of the Technology Committee of the Board of Directors, provide reports to EQUIFAX's Board of Directors, and shall inform, advise, and update the Board of Directors or

Technology Committee regarding EQUIFAX's security posture and the security risks faced by EQUIFAX. The Chief Information Security Officer shall report to the Chief Executive Officer, as well as a member of EQUIFAX's Board of Directors, in the event that the Chief Executive Officer is not a member of the Board of Directors, (i) any unauthorized intrusion to the EQUIFAX NETWORK within forty-eight (48) hours of discovery that it is a SECURITY EVENT and (ii) any "THIRD-PARTY REPORTED EVENT" as defined in Paragraph 23 within forty-eight (48) hours of receipt of the report from the third-party vendor. The quarterly reports to the Technology Committee shall also include all SECURITY EVENTS or THIRD-PARTY REPORTED EVENTS that were reported to the Chief Executive Officer after the previous regular report.

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

18. EQUIFAX shall ensure that the Chief Information Security Officer, Business Information Security Officers, and Information Security Program receive the resources and support reasonably necessary to ensure that the Information Security Program functions as required by this Judgment.

19. Employees who are responsible for implementing, maintaining, or monitoring the Information Security Program, including but not limited to the Chief Information Security

Officer and Business Information Security Officers, must have sufficient knowledge of the requirements of this Judgment and receive specialized training on safeguarding and protecting consumer PERSONAL INFORMATION to help effectuate EQUIFAX's compliance with the terms of this Judgment. EQUIFAX shall provide the training required under this paragraph to all employees within sixty (60) days of the EFFECTIVE DATE of this Judgment or prior to an employee starting their responsibilities for implementing, maintaining, or monitoring the Information Security Program. On an annual basis, or more frequently if appropriate, EQUIFAX shall provide training on safeguarding and protecting PERSONAL INFORMATION to its employees who handle PERSONAL INFORMATION, and its employees responsible for implementing, maintaining, or monitoring the Information Security Program.

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

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

I. Preparation;

II. Detection and Analysis;

III. Containment;

IV. Notification and Coordination with Law Enforcement;

V. Eradication;

VI. Recovery;

VII. Consumer Response (including consideration of appropriate staffing levels, training, and written materials), and Consumer and Regulator Notification and Remediation; and

VIII. Post-Incident Analysis.

22. EQUIFAX shall conduct, at a minimum, biannual incident response plan exercises ("table-top exercises") to test and assess its preparedness to respond to a SECURITY EVENT. These exercises shall include the following, as appropriate:

a. Planning for sufficient staffing levels to handle a high volume of potential consumer traffic and provide consumers access to live agents in a reasonable amount of time;

b. Planning employee training to provide relevant, useful, and accurate information to consumers, including how to place fraud alerts or security freezes;

c. Preparing written materials to provide to consumers that CLEARLY AND CONSPICUOUSLY disclose relevant information;

d. Planning for any necessary online resources to be compliant with the Americans with Disabilities Act (ADA);

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

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

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

PERSONAL INFORMATION SAFEGUARDS AND CONTROLS

24. EQUIFAX shall maintain and comply with a GOVERNANCE PROCESS establishing that PERSONAL INFORMATION will be collected, processed, or stored to the

minimum extent necessary to accomplish the intended legitimate business purpose(s) in using such information.

25. EQUIFAX shall maintain, regularly review, revise, and comply with a GOVERNANCE PROCESS requiring EQUIFAX to either ENCRYPT PERSONAL INFORMATION or otherwise implement COMPENSATING CONTROLS to protect PERSONAL INFORMATION from unauthorized access, whether the information is transmitted electronically from the EQUIFAX NETWORK or is stored in the EQUIFAX NETWORK.

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

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

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

i. The California Attorney General's Office may provide a copy of the study received from EQUIFAX to the Montana Attorney General upon request.

ii. The study and all information contained therein, to the extent permitted by the laws of the State of Montana shall be treated by the Montana Attorney

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

c. Maintain authentication protocols that do not allow consumers to access PERSONAL INFORMATION from EQUIFAX in connection with direct-to-consumer products and services, such as credit monitoring and CREDIT REPORTS, using only a name in combination with a Social Security number; and

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

27. EQUIFAX shall ENCRYPT Social Security numbers when they are stored in the EQUIFAX NETWORK or transmitted electronically from the EQUIFAX NETWORK, or

otherwise implement COMPENSATING CONTROLS to protect Social Security numbers from unauthorized access.

28. EQUIFAX shall maintain, regularly review and revise as necessary, and comply with a GOVERNANCE PROCESS that provides for the secure disposal, using a method that is consistent with Mont Code Ann. § 30-14-1703, on a periodic basis, of PERSONAL INFORMATION that is no longer necessary for the legitimate business purpose for which the PERSONAL INFORMATION was collected, processed, or stored, except where such information is otherwise required to be maintained by law.

SPECIFIC TECHNICAL SAFEGUARDS AND CONTROLS

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

30. **Segmentation:**

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

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

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

31. **Penetration Testing/Risk Assessment:**

a. EQUIFAX shall maintain and regularly review and revise as necessary a risk-assessment program designed to continually identify and assess risks to the EQUIFAX NETWORK. In cases where EQUIFAX deems a risk to be acceptable, EQUIFAX shall generate

and retain a report demonstrating how such risk is to be managed in consideration of cost or difficulty in implementing effective countermeasures. All reports shall be maintained by the Chief Information Security Officer or his or her designee and be available for inspection by the Third-Party Assessor described in Paragraph 61 of this Judgment.

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

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

32. **Access Control and Account Management:**

a. EQUIFAX shall implement and maintain appropriate controls to manage access to, and use of, all EQUIFAX NETWORK accounts with access to PERSONAL INFORMATION, including, without limitation, individual accounts, administrator accounts, service accounts, and vendor accounts. To the extent that EQUIFAX maintains accounts requiring passwords:

i. Such controls shall include strong passwords, password confidentiality policies, password-rotation policies, and two-factor authentication or any other equal or greater authentication protocol, where technically feasible. For purposes of this

paragraph, any administrative-level passwords shall be ENCRYPTED or secured using a password vault, privilege access monitoring, or an equal or greater security tool that is generally accepted by the security industry.

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

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

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

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

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

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

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

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

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

35. **Logging and Monitoring:**

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

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

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

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

a. EQUIFAX shall define the roles and responsibilities for those involved in the change control process, including a board responsible for reviewing changes (for ease, hereinafter referred to as the "Change Advisory Board"). The Change Advisory Board shall include stakeholders from the appropriate business and informational technology units. The Change Advisory Board's responsibilities shall include: managing overall change control policies and procedures; providing guidance regarding the overall change control policies and procedures; conducting an annual audit of change requests to ensure that changes to the EQUIFAX NETWORK are properly analyzed and prioritized; and reviewing, approving, evaluating, and scheduling requests for changes to the EQUIFAX NETWORK.

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

c. Any action with respect to any changes to the EQUIFAX NETWORK (requesting, analyzing, approving, developing, implementing, and reviewing) shall be documented and retained, with the documentation appropriately secured and stored in repositories that are scoped to an application, business unit, and/or geography and are accessible to appropriate security personnel.

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

38. **Digital Certificates:** EQUIFAX shall implement and maintain a digital certificate management tool or service the purpose of which shall be to inventory digital certificates that expire longer than a week after their creation and that are used to authenticate servers and systems in the EQUIFAX NETWORK. The system or tool required by this paragraph shall manage the life cycle of all such digital certificates, including whether to issue, cancel, renew, reissue, or revoke a digital certificate. The system or tool required by this paragraph shall track the expiration date of any such digital certificate and provide notification of such expiration to the custodian of the certificate key thirty days (30) prior to expiration, ten days (10) prior to expiration, and on the date the digital certificate expires. Digital certificate for purposes of this paragraph shall include a security token, biometric identifier, or a cryptographic key used to protect externally-facing systems and applications.

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

40. **Updates/Patch Management:** EQUIFAX shall maintain, keep updated, and support the software on the EQUIFAX NETWORK, taking into consideration the impact a software update will have on data security in the context of the EQUIFAX NETWORK and its

ongoing business and network operations, and the scope of the resources required to maintain, update, and support the software. At a minimum, EQUIFAX shall also do the following:

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

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

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

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

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

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

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

satisfy its obligations under this subparagraph by using an industry-standard vulnerability scanning tool. The CVE tool required by this subparagraph shall also:

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

(b) Scan the EQUIFAX NETWORK for CVEs; and

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

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

d. The Patch Management Group shall be responsible for:

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

ii. Monitoring compliance with policies and procedures regarding ownership, supervision, evaluation, and coordination of the maintenance, management, and application of all security patches and software and application security updates by appropriate information technology (IT) application and system owners;

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

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

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

f. EQUIFAX shall employ processes and procedures to ensure the timely scheduling and installation of any security update and security patch, considering (without limitation) the severity of the vulnerability for which the update or patch has been released to address, the severity of the issue in the context of the EQUIFAX NETWORK, the impact on EQUIFAX's ongoing business and network operations, and the risk ratings articulated by the relevant software and application vendors or disseminated by the United States Computer Emergency Readiness Team (US-CERT). Such patch management policies shall require EQUIFAX to rate as critical, high, medium, or low all patches and/or updates, rating as "critical" all patches or updates intended to prevent any vulnerability that threatens the safeguarding or security of any PERSONAL INFORMATION maintained on the EQUIFAX NETWORK. If EQUIFAX does not accept or increase the risk ratings disseminated by either a software or application vendor or US-CERT for externally-facing applications on the EQUIFAX NETWORK, EQUIFAX shall identify for any update or patch for which it is attaching the lower risk rating, the assets to which it applies, and create a written explanation that shall include:

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

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

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

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

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

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

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

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

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

41. **Information Security Program Implementation:** EQUIFAX represents that it has worked and will continue to work in good faith to comply with the requirements of the Information Security Program set forth in this Judgment. As to Paragraphs 24, 25, 26(c), 26(d),

27, 34, 37, and 59, only, the Montana Attorney General agrees that it shall not commence any action, the purpose of which would be to establish a violation of this order or a finding of contempt until on or after December 31, 2019, subject also to the requirements of Paragraph 82 , and that it shall not commence any action, the purpose of which would be to establish a violation of Paragraph 30 or a finding of contempt with respect to that paragraph, until on or after December 31, 2020, subject also to the requirements of Paragraph 82.

CONSUMER-RELATED RELIEF

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

43. **Three-Bureau Credit Monitoring Services:** AFFECTED CONSUMERS who file valid claims shall be eligible for at least four (4) years of a free Three-Bureau Credit Monitoring Service. These four (4) years shall be provided in addition to any free credit monitoring services EQUIFAX is currently providing or has previously offered as a result of the 2017 DATA BREACH. The Three-Bureau Credit Monitoring Services will be provided and maintained by an independent third party. The Three-Bureau Credit Monitoring Services shall include:

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

to an AFFECTED CONSUMER's address; and negative information, including delinquencies or bankruptcies.

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

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

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

44. **One-Bureau Credit Monitoring Services:** AFFECTED CONSUMERS who file valid claims and enroll in Three-Bureau Credit Monitoring Services shall be eligible for single-bureau credit monitoring services ("One-Bureau Credit Monitoring Services"). EQUIFAX shall provide One-Bureau Credit Monitoring Services upon expiration of the Three-Bureau Credit Monitoring Services to AFFECTED CONSUMERS who enroll in the Three-Bureau Credit Monitoring Services. EQUIFAX shall provide One-Bureau Credit Monitoring Services for the period of time necessary for the aggregate number of years of credit monitoring provided under Paragraphs 43 and 44 to equal ten (10) years. The cost of the One-Bureau Credit Monitoring Services shall not be paid from the Consumer Restitution Fund described in Section V. of this Judgment. One-Bureau Credit Monitoring Services will include the following:

a. Daily CREDIT REPORT monitoring from EQUIFAX showing key changes to an AFFECTED CONSUMER's EIS CREDIT REPORT including automated alerts when the following occur: new accounts are opened; inquiries or requests for an AFFECTED CONSUMER's CREDIT REPORT for the purpose of obtaining credit; changes to an

AFFECTED CONSUMER's address; and negative information, such as delinquencies or bankruptcies.

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

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

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

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

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

such as a Social Security number submitted for monitoring appear on suspicious websites, including websites on the "dark web;" for minors who do not have an EIS CREDIT REPORT, an EIS CREDIT REPORT is created, locked, and then monitored, and for minors with an EIS CREDIT REPORT, their EIS CREDIT REPORT is locked and then monitored.

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

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

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

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

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

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

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

53. **Dedicated Resources for Continued 2017 BREACH RESPONSE:** For a period of three (3) years from the EFFECTIVE DATE, EQUIFAX shall devote reasonable and sufficient resources focused on administering its efforts to support consumers related to the 2017 DATA BREACH ("2017 BREACH RESPONSE"), including but not limited to:

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

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

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

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

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

54. EQUIFAX shall make the following digital communications available in Spanish, Chinese, Tagalog, Vietnamese, Arabic, French, and Korean: (1) within sixty (60) days of content being finalized, all webpages that EQUIFAX makes available on its website, or on any website that it operates or controls that are dedicated to describing the terms of this Judgment and any benefits available under the Judgment; (2) all legally-required consumer notices

regarding any future data breach that are made available on its website, or on any website that it operates or controls; and (3) all notices and claim forms that are made available on any website operated by the settlement administrator. EQUIFAX may satisfy its obligation under this paragraph by providing an automated translation function on the applicable web page(s) which automatically translates all content capable of being translated by the selected translation tool, which, at a minimum, shall translate text appearing directly on the website.

55. **Placing Freezes for PROTECTED INDIVIDUALS:**

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

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

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

56. **Consumer Assistance Process:** As part of or in addition to that which is required by federal and state law, EIS shall continue to offer direct assistance, processes, and informational resources to United States consumers who have questions about their EIS CREDIT FILE, who wish to place a fraud alert and/or security freeze on their EIS CREDIT FILE, or who have or may have been the victim of fraud or identity theft. These processes shall include the ability for consumers to contact EIS online, by toll-free phone numbers, and by United States mail, or any other reasonably accessible means established by EIS to communicate directly with consumers.

a. At a minimum, EIS shall:

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

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

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

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

v. Maintain enhanced consumer dispute results letters to assist consumers in understanding the basis and results of EIS's REINVESTIGATION process, including the actions taken by EIS as a result of the consumer's dispute, the role of the FURNISHER in the REINVESTIGATION process, the results of the dispute including any modified or deleted information, and the options the consumer may take if dissatisfied with the results of the REINVESTIGATION;

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

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

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

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

b. EIS shall provide direct assistance to members of the United States armed forces, including without limitation members of the National Guard and military reserve, (collectively "Service Members"), or their spouses or other dependents (collectively "Military Families"). At a minimum, EIS shall train a department or group to: help Service Members and Military Families review their EIS CREDIT FILES; review complaints regarding identity theft or fraudulent activity; and help Service Members and Military Families place a security freeze on their EIS CREDIT FILES and implement active duty alerts.

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

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

e. Disclosure of the Consumer Assistance Process

i. EQUIFAX shall CLEARLY AND CONSPICUOUSLY disclose on its website the following components of the Consumer Assistance Process: the existence of the processes and informational resources offered by EQUIFAX; the content of and how to access an EIS CREDIT FILE; the methods to request a fraud or active duty alert, or take advantage of any security freeze feature on an EIS CREDIT FILE; the methods to dispute the accuracy or completeness of an item on an EIS CREDIT FILE; and informational materials for

Service Members and Military Families. EQUIFAX may comply with this paragraph by: (1) maintaining a dedicated website page that describes or provides the resources set forth above; and (2) providing the consumer with a link to said dedicated website page.

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

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

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

57. **Declining to Block Information in a CREDIT FILE:** If EIS declines to block, as that term is used in FCRA, or rescinds any block on, the information in a CREDIT FILE that the consumer identifies as information that resulted from an alleged identity theft, EIS shall provide the consumer with additional steps the consumer can take if the REINVESTIGATION of such information results in the information remaining on the consumer's CREDIT FILE, including his/her ability to utilize the Escalated Identity Theft Block Process set forth in Paragraph 58. EIS can choose to satisfy this provision by drafting a form letter to send to consumer that provides this information. This paragraph shall not limit or restrict EIS's ability to designate a dispute filing frivolous or abusive disputes pursuant to 15 U.S.C. § 1681i(a)(3). The Montana Attorney General agrees that it shall not commence any action, the purpose of which

would be to establish a violation of this paragraph or a finding of contempt with respect to this paragraph, until on or after December 31, 2019, subject also to the requirements of Paragraph 82.

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

59. **Consumer Transparency:** EQUIFAX shall post on the homepage of any website owned or controlled by EQUIFAX: a notice that details categories of the PERSONAL INFORMATION EQUIFAX collects and maintains, including NON-FCRA INFORMATION; how EQUIFAX collects the PERSONAL INFORMATION; how EQUIFAX uses the PERSONAL INFORMATION; how EQUIFAX protects the PERSONAL INFORMATION; whether EQUIFAX shares the PERSONAL INFORMATION with others, and if so, what PERSONAL INFORMATION is shared and the categories of persons or entities with whom the PERSONAL INFORMATION is shared; and whether consumers have control over their PERSONAL INFORMATION, and if so, what kind of control they have and how to exercise the control. If EQUIFAX's PERSONAL INFORMATION practices change, the notice shall be updated to reflect those changes. EQUIFAX may comply with this paragraph by including this information in its online privacy notices.

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

ASSESSMENT AND REPORTING REQUIREMENTS TO THE ATTORNEY GENERAL

61. **Third-Party Assessment:** During the time period established in Paragraph 13, EQUIFAX shall obtain from an independent third party an initial assessment, followed by biennial assessments of the Information Security Program required under the terms of this

Judgment (the "Third-Party Assessments"). The Third-Party Assessments required by this paragraph shall be conducted by a third-party (the "Third-Party Assessor").

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

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

ii. Document the extent to which the identified administrative, technical and physical safeguards are appropriate considering EQUIFAX's size and complexity, the nature and scope of EQUIFAX's activities, and the sensitivity of the PERSONAL INFORMATION maintained on the EQUIFAX NETWORK; and

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

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

c. Any Third Party Assessor's Report provided pursuant to this paragraph and all information contained therein, to the extent permitted by the laws of the State of Montana shall be treated by the Montana Attorney General's Office as confidential; shall not be shared or disclosed except as described in subsection b; and shall be treated by the Montana Attorney General's Office as exempt from disclosure under the relevant public records laws of the State of Montana. In the event that the Montana Attorney General's Office receives any request from the public to inspect any Third Party Assessor's Report provided pursuant to this paragraph or other

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

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

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

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

i. An organizational chart identifying the individuals employed or contracted by EQUIFAX to respond to consumer complaints related to the 2017 DATA BREACH as specified in Paragraph 56(d) and complaints submitted through a State Attorney General as specified in Paragraph 56(c), identified by their titles with a number designating how many staff are assigned to each position;

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

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

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

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

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

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

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

c. Each Consumer Remedies Report must be completed within sixty (60) days after the end of the reporting period to which the Consumer Remedies Report applies. EQUIFAX shall provide a copy of the Consumer Remedies Report to the California Attorney General's Office within ten (10) business days of the completion of the Consumer Remedies Report.

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

e. The Consumer Remedies Reports and all information contained therein, to the extent permitted by the laws of the State of Montana: shall be treated by the Montana Attorney General's Office as confidential; shall not be shared or disclosed except as described in subsection (d); and shall be treated by the Montana Attorney General's Office as exempt from disclosure under the relevant public records laws of the State of Montana. In the event that the Montana Attorney General's Office receives any request from the public for a Consumer Remedies Report or other confidential documents under this Judgment and believes that such

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

IV. DOCUMENT RETENTION

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

V. CONSUMER RESTITUTION

64. **Consumer Restitution Fund:**

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

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

restitution and redress to AFFECTED CONSUMERS provided through the MULTI-DISTRICT LITIGATION.

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

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

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

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

VI. MONETARY PAYMENT

65. No later than thirty (30) days after the EFFECTIVE DATE, Equifax Inc. shall pay a total of One Hundred and Seventy Five Million Dollars ($175,000,000.00) to the ATTORNEYS GENERAL, which is to be divided amongst the ATTORNEYS GENERAL. The amount apportioned to Montana is to be paid by Equifax Inc. directly to the Montana Attorney General in an amount to be designated by and in the sole discretion of the MULTISTATE LEADERSHIP COMMITTEE. The amounts and wiring instructions shall be provided to Equifax Inc. no later than seven (7) days after the EFFECTIVE DATE. If the Court has not

entered this Judgment by the EFFECTIVE DATE, Equifax Inc. shall make the payment within thirty (30) days of the EFFECTIVE DATE or within fourteen (14) days of the entry of the Judgment, whichever is later. The money received by the Montana Attorney General pursuant to this paragraph may be used for purposes that may include, but are not limited to, attorneys fees, and other costs of investigation and litigation, or be placed in, or applied to, any consumer protection law enforcement fund, including future consumer protection or privacy enforcement, consumer education, litigation or local consumer aid fund or revolving fund, used to defray the costs of the inquiry leading hereto, or for other uses permitted by state law, at the sole discretion of the Attorney General.

VII. RELEASE

66. Following full payment of the amounts due under this Judgment, the Montana Attorney General shall release and discharge EQUIFAX and its directors, officers, and employees from all civil claims alleged in the Complaint, and any civil claims that it could have brought based on EQUIFAX's conduct related to the 2017 DATA BREACH under the Montana Unfair Trade Practices and Consumer Protection Act, including, without limitation, Mont. Code Ann. §§ 30-14-101 through 144 (Part 1) and 30-14-1701 through 1736 (Part 17), the Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq. and any state credit reporting law, or common law claims, including those concerning unfair, deceptive, or fraudulent trade practices. Nothing contained in this paragraph shall be construed to limit the ability of the Montana Attorney General to enforce the obligations that EQUIFAX has under this Judgment.

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

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

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

i. State or federal antitrust violations;

ii. State or federal securities violations; or

iii. State or federal tax claims.

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

VIII. NO ADMISSION OF LIABILITY

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

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

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

IX. GENERAL PROVISIONS

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

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

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

75. EQUIFAX shall deliver a copy of this Judgment to, and otherwise fully apprise, its Chief Executive Officer, Chief Technology Officer, Chief Information Security Officer, each of its Business Information Security Officers, Patch Supervisor designated pursuant to this Judgment, General Counsel, and Board of Directors within ninety (90) days of the EFFECTIVE DATE. To the extent EQUIFAX replaces any of the above listed officers, counsel, or Directors, EQUIFAX shall deliver a copy of this Judgment to their replacements within ninety (90) days from the date on which such person assumes his/her position with EQUIFAX.

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

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

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

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

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

81. Whenever EQUIFAX shall provide notice to the Montana Attorney General under this Judgment, that requirement shall be satisfied by sending notice to: Mark Mattioli, Bureau Chief, Montana Office of Consumer Protection, P.O. Box 200151, Helena, MT 59620-0151. Any notices or other documents sent to EQUIFAX pursuant to this Judgment shall be sent to the following address: Chief Legal Officer, Equifax, Inc., 1550 Peachtree Street, N.W., Atlanta, GA 30309; Phyllis Sumner, King & Spalding LLP, 1180 Peachtree Street, N.E., Suite 1600, Atlanta, GA 30309; and Zachary Fardon, King & Spalding LLP, 444 West Lake Street, Suite 1650, Chicago, IL 60606. All notices or other documents to be provided under this Judgment shall be sent by United States mail, certified mail return receipt requested, or other nationally recognized courier service that provides for tracking services and identification of the person signing for the notice or document, and shall have been deemed to be sent upon mailing. Any party may update its designee or address by sending written notice to the other party informing them of the change.

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

sure the violation does not occur again. The Montana Attorney General may agree to provide EQUIFAX with more than thirty (30) days to respond. The Montana Attorney General shall receive and consider the response from EQUIFAX prior to initiating any proceeding for any alleged failure to comply with this Judgment.

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

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

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

ORDERED AND ADJUDGED this _____ day of July, 2019.

_____

District Court Judge

For Defendant Equifax Inc.

By: Counsel for Defendant Equifax Inc.:

SHELDON BRADSHAW (Montana Bar No. 3430)
KING & SPALDING LLP
1700 Pennsylvania Avenue, NW
2nd Floor
Washington, DC 20006-4707
Tel.: (202) 626-9225
sbradshaw@kslaw.com

and

PHYLLIS B. SUMNER
CHRISTOPHER C. BURRIS
SHANNON F. COX
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

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

For Plaintiff State of Montana

By: Mark Mattioli
Mark Mattioli
Assistant Attorney General

Dated: 2/22/2019