

**IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF GEORGIA  
ATLANTA DIVISION**

BUREAU OF CONSUMER  
FINANCIAL PROTECTION,

Plaintiff,

v.

EQUIFAX INC.,

Defendant.

Civil Action Number:  
1:19-cv-3300-TWT

**STIPULATED ORDER FOR  
PERMANENT INJUNCTION  
AND MONETARY JUDGMENT**

Plaintiff, the Bureau of Consumer Financial Protection (“Bureau”), has filed its Complaint for a permanent injunction, civil penalties, and other relief in this matter. The Bureau brought this action pursuant to Sections 1031(a), 1036(a)(1), and 1054 of the Consumer Financial Protection Act of 2010 (“CFPA”), 12 U.S.C. §§ 5531(a), 5536(a)(1), and 5564, and sought relief, including civil penalties, pursuant to Section 1055 of the CFPA, 12 U.S.C. § 5565(c). Defendant Equifax Inc. (“Defendant” or “Equifax”) waived service of the summons and the Complaint. The Bureau and Defendant stipulate to entry of this Order for Permanent Injunction and Monetary Judgment (“Order”) to resolve all claims in dispute in this action between them.

THEREFORE, IT IS ORDERED as follows:

**FINDINGS**

1. This Court has jurisdiction over this matter.
2. The Complaint alleges claims for relief under Sections 1031(a) and 1036(a)(1) of the CFPA, 12 U.S.C. §§ 5531(a) and 5536(a)(1).
3. Defendant neither admits nor denies any of the allegations in the Complaint, except as specifically stated in this Order. For purposes of this Order, Defendant admits the facts necessary to establish jurisdiction over it and the subject matter of this action.
4. Defendant waives any claim that it may have under the Equal Access to Justice Act, 28 U.S.C. § 2412, concerning the prosecution of this action through the date of this Order, and agrees to bear its own costs and attorneys' fees.
5. All parties waive all rights to appeal or otherwise challenge or contest the validity of this Order.
6. Entry of the Order is in the public interest.

## **DEFINITIONS**

For purposes of this Order, the following definitions apply:

7. “Affected Consumer” means the approximately One Hundred Forty Seven Million (147,000,000) U.S. consumers whom Defendant has identified as having their Personal Information accessed without authorization as a result of the Breach.
8. “Assisted Identity Restoration” means the identity restoration services offered to all Affected Consumers, as set forth in Subsection VII.D and described in Exhibit A.
9. “Breach” means the information security incident publicly disclosed by Defendant on or about September 7, 2017.
10. “Claims Administration Protocol” means the protocol that has been approved by the Bureau, and which will be submitted to and approved by the MDL Court, to implement the claims administration process consistent with Sections VII, IX, X and XI of this Order and the Class Action Settlement.
11. “Class Action Settlement” means the settlement agreement, including release of settlement class member claims, filed in the Multi-District Litigation with the MDL Court.

12. “Class Action Effective Date” means the first business day after the MDL Court enters a Final Approval Order and Judgment, and either:
  - a. the time for appeal, petition, rehearing or other review has expired, or
  - b. if one or more appeals, petitions, requests for rehearing or other reviews are filed, when:
    - i. the Final Approval Order and Judgment is affirmed without material change and the time for further appeals, petitions, requests for rehearing or other reviews has expired, or
    - ii. all appeals, petitions, rehearsings, or other reviews are dismissed or otherwise disposed of, no other appeals, petitions, rehearsings, or other reviews are pending, and the time for further appeals, petitions, requests for rehearing or other reviews has expired.
13. “Consumer Fund” means the account established to provide restitution and redress to Affected Consumers, as described in Sections IX, X, and XI, which will be overseen by the MDL Court and which represents an undifferentiated portion of the consumer restitution fund as defined in the Class Action Settlement.

14. “Consumer Report” has the meaning provided in the Fair Credit Reporting Act (“FCRA”), 15 U.S.C. § 1681 *et seq.*, and any amendments thereto. As of the date of this Order, “Consumer Report” is defined under the FCRA as any written, oral, or other communication of any information by a Consumer Reporting Agency bearing on a consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living, which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer’s eligibility for:
  - a. credit or insurance to be used primarily for personal, family, or household purposes;
  - b. employment purposes; or
  - c. any other purpose authorized under the FCRA, Section 604, 15 U.S.C. § 1681b.
15. “Consumer Reporting Agency” has the meaning provided in the FCRA, 15 U.S.C. § 1681 *et seq.*, and any amendments thereto. As of the date of this Order, “Consumer Reporting Agency” is defined under the FCRA as any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or

evaluating consumer credit information or other information on consumers for the purpose of furnishing Consumer Reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing Consumer Reports.

16. “Covered Incident” means any instance in which any United States federal, state, or local law or regulation requires Defendant to notify any U.S. federal, state, or local government entity that Personal Information collected or received, directly or indirectly, by Defendant from or about an individual consumer was, or is reasonably believed to have been, accessed or acquired without authorization, and the incident affects no fewer than 250 U.S. consumers.
17. “Defendant” means Equifax Inc., its successors and assigns, and its subsidiaries, their successors and assigns, incorporated in the United States, that do business in the United States, or that collect, store, or process Personal Information from or about consumers in the United States to the extent that Defendant’s conduct falls within the Bureau’s jurisdiction.
18. “Effective Date” means the date on which this Stipulated Order is issued.

19. “Enforcement Director” means the Assistant Director of the Office of Enforcement for the Bureau of Consumer Financial Protection, or her delegate.
20. “Extended Claims Period” means the period beginning with the conclusion of the Initial Claims Period through four (4) years after the conclusion of the Initial Claims Period.
21. “Final Approval Order and Judgment” means an order and judgment that the MDL Court enters finally approving settlement, including release of the settlement class member claims in the Multi-District Litigation.
22. “FTC Order” means the Stipulated Order entered in the matter styled as *Federal Trade Commission v. Equifax Inc.*, filed on or about July 22, 2019 in the Federal District Court for the Northern District of Georgia.
23. “Full Service Identity Restoration” means the identity restoration services offered to all Affected Consumers enrolled in the Product, as set forth in Subsection VII.A and described in Exhibit A.
24. “Initial Claims Period” means six (6) months after the MDL Court enters an order permitting issuance of notice of class action settlement for the Class Action Settlement.
25. “MDL Court” means the Court presiding over the Multi-District Litigation.

26. “Multi-District Litigation” means those actions filed against Equifax Inc. and/or one or more of its subsidiaries asserting claims related to the 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*, 1:17-md-02800-TWT (N.D. Ga.).
27. “Notice Date” means the date sixty (60) days after the MDL Court issues an order permitting issuance of notice of class action settlement for the Class Action Settlement.
28. “Notice Plan” means the notice plan for providing notice to Affected Consumers which has been approved by a representative of the Bureau, and is to be submitted to, approved by, and overseen by the MDL Court.
29. “Notice Provider” means an independent third-party agent or administrator approved by a representative of the Bureau, and which is to be submitted to, approved by, and overseen by the MDL Court to implement the notice provisions of the Notice Plan, and as set forth in Section X.
30. “Out-of-Pocket Losses” means verifiable unreimbursed costs or expenditures incurred by an Affected Consumer that are fairly traceable (as described in the Claims Administration Protocol) to the Breach, which are

eligible for reimbursement from the Consumer Fund as set forth in

Subsection IX.B.4, and defined as follows:

- a. Costs incurred for credit monitoring services at any time between September 7, 2017 and the date of the Affected Consumer's claim(s) submission;
- b. Up to twenty-five percent (25%) reimbursement for costs incurred by an Affected Consumer enrolled in Equifax credit or identity monitoring subscription products at any time between September 7, 2016 and September 7, 2017;
- c. Costs incurred by an Affected Consumer to place or remove a security freeze on a Consumer Report with any Consumer Reporting Agency at any time on or after September 7, 2017;
- d. Unreimbursed costs, expenses, losses, or charges incurred as a result of identity theft or identity fraud, falsified tax returns, or other alleged misuse of the Affected Consumer's Personal Information;
- e. Reimbursement for Time Compensation; and
- f. Miscellaneous expenses incurred by the Affected Consumer related to any Out-Of-Pocket Losses, such as notary, fax, postage, copying, mileage, and telephone charges.

31. “Personal Consumer Report” means, for purposes of this Order only, a Consumer Report made available to consumers by any entity within Defendant that compiles and maintains files on consumers on a nationwide basis as defined under 15 U.S.C. § 1681a(p).
32. “Personal Information” means individually identifiable information from or about an individual consumer, including:
  - a. first and last name;
  - b. home or other physical address;
  - c. email address;
  - d. telephone number;
  - e. date of birth;
  - f. Social Security number;
  - g. other government-issued identification numbers, such as a driver’s license number, military identification number, passport number, or other personal identification number;
  - h. financial institution account number;
  - i. credit or debit card information; or
  - j. authentication credentials, such as a username and password.

33. “Preventative Measures” means placement or removal of security freezes or obtaining credit monitoring services.
34. “Product” means the credit monitoring, identity theft insurance, and identity restoration services further described in Subsection VII.A and on pages 1-4 of Exhibit A, that has been approved by the Bureau and will be presented to the MDL Court for approval.
35. “Related Consumer Action” means any private action by or on behalf of one or more consumers, or enforcement action by another governmental agency, entity, or representative, brought against Defendant based on substantially the same facts as described in the Complaint.
36. “Settlement Administrator” means an independent third-party agent or administrator that has been approved by the Bureau, which will be submitted to, approved by, and overseen by the MDL Court, and which will implement the claims and administration process in the Multi-District Litigation.
37. “Settlement Website” means the website established by the Settlement Administrator that provides information to Affected Consumers about their rights and options consistent with Sections VII, IX, X and XI of this Order, including the components of the Consumer Fund available to Affected Consumers, where and how Affected Consumers may submit claims during

the Initial and Extended Claims Periods, and all deadlines for making such claims.

38. “Single Bureau Monitoring” means credit monitoring provided by Defendant and offered to all Affected Consumers enrolled in the Product, as set forth in Subsection VII.B and described in Exhibit A.
39. “States’ Attorneys General” means the 50 state and territory attorneys general that are each entering into a stipulated judgment on or about July 22, 2019 with Equifax Inc. for claims related to the Breach.
40. “Time Compensation” means compensation to an Affected Consumer for a valid claim for time spent by that Affected Consumer (1) taking Preventative Measures and/or (2) remedying fraud, identity theft, or other misuse of an Affected Consumer’s Personal Information that is fairly traceable to the Breach.

## **ORDER**

### **I. PROHIBITION AGAINST MISREPRESENTATIONS**

**IT IS ORDERED** that Defendant, Defendant’s officers, agents, employees, and all other persons in active concert or participation with any of them who receive actual notice of this Order, whether acting directly or indirectly, in connection with any product or service, are hereby permanently restrained and

enjoined from misrepresenting, expressly or by implication, the extent to which Defendant maintains and protects the privacy, security, confidentiality, or integrity of any Personal Information.

**II. MANDATED INFORMATION SECURITY PROGRAM**

**IT IS FURTHER ORDERED** that Defendant shall establish and implement, and thereafter maintain, for twenty (20) years after entry of this Order, a comprehensive information security program (“Information Security Program”) designed to protect the security, confidentiality, and integrity of Personal Information. To satisfy this requirement, Defendant must, at a minimum:

- A. Document in writing the content, implementation, and maintenance of the Information Security Program, including the following:
  1. Documented risk assessment required under Subsection II.D;
  2. Documented safeguards required under Subsection II.E; and
  3. A description of the procedures adopted to implement and monitor the Information Security Program, including procedures for evaluating and adjusting the Information Security Program as required under Subsection II.I.
- B. Provide the written Information Security Program and any material evaluations thereof or updates thereto to Defendant’s board of directors or a

- relevant subcommittee thereof, or equivalent governing body or, if no such board or equivalent governing body exists, to a senior officer of Defendant responsible for Defendant's Information Security Program at least once every twelve (12) months;
- C. Designate a qualified employee or employees to coordinate, oversee, and be responsible for the Information Security Program;
  - D. Assess, at least once every twelve (12) months, internal and external risks to the security, confidentiality, or integrity of Personal Information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information and document those risks that are material. Defendant shall further assess and document internal and external risks as described above as they relate to a Covered Incident promptly (not to exceed forty-five days) following verification of such a Covered Incident;
  - E. Design, implement, maintain, and document safeguards that control for the material internal and external risks Defendant identifies to the security, confidentiality, or integrity of Personal Information identified in response to Subsection D. Each safeguard shall be based on the volume and sensitivity of the Personal Information that is at risk, and the likelihood, given the existence of other safeguards, that the risk could be realized and result in the

unauthorized access, collection, use, alteration, destruction, or disclosure of the Personal Information. Such safeguards shall also include:

1. Establishing patch management policies and procedures that require confirmation that any directives to apply patches or remediate vulnerabilities are received and completed and that include timelines for addressing vulnerabilities that account for the severity and exploitability of the risk implicated;
2. Establishing and enforcing policies and procedures to ensure the timely remediation of critical and/or high-risk security vulnerabilities;
3. Identifying and documenting a comprehensive information technology (“IT”) asset inventory that includes hardware, software, and location of the assets;
4. Designing and implementing protections such as network intrusion protection, host intrusion protection, and file integrity monitoring, across Defendant’s network and IT assets, including Defendant’s legacy technologies;
5. Designing, implementing, and maintaining measures to limit unauthorized access in any network or system that stores, collects,

maintains, or processes Personal Information, such as segmentation of networks and databases and properly configured firewalls;

6. Implementing access controls across Defendant's network, such as multi-factor authentication and strong password requirements;
7. Limiting user access privileges to systems that provide access to Personal Information to employees, contractors, or other authorized third parties with a business need to access such information and establishing regular documented review of such access privileges;
8. Implementing protections, such as encryption, tokenization, or other at least equivalent protections, for Personal Information collected, maintained, processed, or stored by Defendant, including in transit and at rest. To the extent that any of the identified protections are infeasible, equivalent protections shall include effective alternative compensating controls designed to protect unencrypted data at rest or in transit, which shall be reviewed and approved by the qualified employee or employees designated to coordinate, oversee, and be responsible for the Information Security Program;
9. Establishing and enforcing written policies, procedures, guidelines, and standards designed to:

- a. Ensure the use of secure development practices for applications developed in-house; and
  - b. Evaluate, assess, or test the security of externally developed applications used within Defendant's technology environment;
10. Establishing regular information security training programs, updated, as applicable, to address internal or external risks identified by Defendant, including, at a minimum:
  - a. At least annual information security awareness training for all employees; and
  - b. Training for software developers relating to secure software development principles and intended to address well-known and reasonably foreseeable vulnerabilities, such as cross-site scripting, structured query language injection, and other risks identified by Defendant through risk assessments and/or penetration testing;
11. Establishing a clear and easily accessible process for receiving and addressing security vulnerability reports from third parties such as security researchers and academics; and

12. By August 30, 2019, establishing a clear and easily accessible process overseen by a senior corporate manager for employees to submit complaints or concerns about Defendant's information security practices, including establishing a clear process for reviewing, addressing, and escalating employee complaints or concerns.

F. Assess, at least once every twelve (12) months, the sufficiency of any safeguards in place to address the risks to the security, confidentiality, or integrity of Personal Information, and evaluate and implement any needed modifications to the Information Security Program based on the results. Defendant shall further assess the sufficiency of safeguards as described above as they relate to a Covered Incident promptly (not to exceed forty-five days) following verification of such an incident. Each such assessment must evaluate safeguards in each area of relevant operation, including:

1. Employee training and management;
2. Information systems, such as network and software design, or information processing, storage, transmission, and disposal; and
3. Prevention, detection, and response to attacks, intrusions, or other system failures;

- G. Test and monitor the effectiveness of the safeguards at least once every twelve (12) months and, as they relate to a Covered Incident promptly (not to exceed sixty (60) days) following verification of such an incident, and modify the Information Security Program based on the results. Such testing shall include vulnerability testing of Defendant's network at least once every four (4) months and, as it relates to a Covered Incident, promptly (not to exceed sixty (60) days) following verification of such an incident, and penetration testing of Defendant's network at least once every twelve (12) months and, as it relates to a Covered Incident promptly (not to exceed sixty (60) days) following verification of such an incident;
- H. Select and retain service providers capable of safeguarding Personal Information they access through or receive from Defendant, and contractually require service providers to implement and maintain safeguards tailored to the amount and the type of Personal Information at issue; and
- I. Evaluate and adjust the Information Security Program in light of any changes to Defendant's operations or business arrangements, including, without limitation, acquisition or licensing of any new information systems, technologies, or assets through merger or acquisition, a Covered Incident, or

any other circumstances that Defendant knows or has reason to know may have a material impact on the effectiveness of the Information Security Program. At a minimum, Defendant must evaluate the Information Security Program at least once every twelve (12) months and, as it relates to a Covered Incident promptly (not to exceed sixty (60) days) following verification of such an incident and modify the Information Security Program based on the results.

### **III. INFORMATION SECURITY ASSESSMENTS BY A THIRD PARTY**

**IT IS FURTHER ORDERED** that, in connection with compliance with Section II of this Order, titled Mandated Information Security Program, Defendant must obtain initial and biennial assessments (“Assessments”):

- A. The Assessments must be obtained from a qualified, objective, independent third-party professional (“Assessor”), who: (1) uses procedures and standards generally accepted in the profession; (2) is a Certified Information Systems Security Professional (“CISSP”) or a Certified Information Systems Auditor (“CISA”), or other similarly qualified person or organization; (3) has at least five (5) years of experience evaluating the effectiveness of computer system security or information system security; (4) conducts an independent review of the Information Security Program; and (5) is

contractually required to retain all documents relevant to each Assessment for five (5) years after completion of such Assessment, and to provide such documents to the Bureau within fourteen days of receipt of a written request from a representative of the Bureau. No documents may be withheld by the Assessor on the basis of (1) a claim of confidentiality, proprietary or trade secrets, or any similar claim, or (2) any privilege asserted between Defendant and Assessor, although such documents can be designated for confidential treatment in accordance with applicable law.

- B. For each Assessment, Defendant shall provide the Enforcement Director with the name and affiliation of the person selected to conduct the Assessment, which the Bureau shall have the authority to approve in its sole discretion. If the Bureau does not approve of the person Defendant has selected, Defendant must choose a person or entity to conduct the Assessment from a list of at least three Assessors provided by a representative of the Bureau.
- C. The reporting period for the Assessments must cover: (1) the first 180 days after the entry date of the Order for the initial Assessment; and (2) each two-year period thereafter for twenty (20) years after entry of the Order for the biennial Assessments.

- D. Each Assessment must:
1. Evaluate whether Defendant has implemented and maintained the Information Security Program required by Section II of this Order, titled Mandated Information Security Program;
  2. Assess the effectiveness of Defendant's implementation and maintenance of Subsections A-I of Section II;
  3. Identify gaps or weaknesses in the Information Security Program and make recommendations to remediate or cure any such gaps and weaknesses; and
  4. Identify specific evidence (including, but not limited to, documents reviewed, sampling and testing performed, and interviews conducted) examined to make such determinations, assessments, and identifications, and explain why the evidence that the Assessor examined is sufficient to justify the Assessor's findings. No finding of any Assessment shall rely solely on assertions or attestations by Defendant's management. The Assessment shall be signed by the Assessor and shall state that the Assessor conducted an independent review of the Information Security Program, and did not rely solely on assertions or attestations by Defendant's management.

- E. Each Assessment must be completed within sixty days after the end of the reporting period to which the Assessment applies. Unless otherwise directed by a Bureau representative in writing, Defendant must submit each Assessment to the Bureau within ten days after the Assessment has been completed via secure email to Enforcement\_Compliance@cfpb.gov or by overnight courier (not the U.S. Postal Service) to Enforcement Director, Office of Enforcement, Bureau of Consumer Financial Protection, 1700 G Street NW, Washington, DC 20552. The subject line must begin, “Bureau of Consumer Financial Protection v. Equifax Inc., BCFP File No. 2017-1906-02.” Defendant must notify the Bureau of any portions of the Assessment containing trade secrets, commercial or financial information, or information about a consumer or other third party, for which confidential treatment is requested pursuant to the Bureau’s procedures concerning public disclosure set forth in 12 U.S.C. § 5512(c)(6)(A) and 12 C.F.R. § 1070.20 (2018).
- F. An Assessment required pursuant to this Section may be satisfied by an assessment conducted in connection with the FTC Order.

#### **IV. COOPERATION WITH THIRD PARTY INFORMATION SECURITY ASSESSOR**

**IT IS FURTHER ORDERED** that Defendant, Defendant's officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with any Assessment required by Section III of this Order titled Information Security Assessments by a Third Party, must not withhold any material facts from the Assessor, and must not misrepresent, expressly or by implication, any fact material to the Assessor's: (1) evaluation of whether Defendant has implemented and maintained the Information Security Program required by Section II of this Order, titled Mandated Information Security Program; (2) assessment of the effectiveness of the implementation and maintenance of subsections A-I of Section II; or (3) identification of any gaps or weaknesses in the Information Security Program. Defendant shall provide the Assessor with information about the Defendant's entire network and all of Defendant's IT assets so that the Assessor can determine the scope of the Assessment, and visibility to those portions of the network and IT assets deemed in scope. Defendant shall also provide or otherwise make available to the Assessor all information and material in its possession, custody, or control that is relevant to the Assessment.

## V. ANNUAL CERTIFICATION

**IT IS FURTHER ORDERED** that, in connection with compliance with Section II of this Order titled Mandated Information Security Program, Defendant shall:

- A. For a total of twenty (20) years and commencing one year after the entry date of this Order, and each year thereafter, provide the Bureau with a certification from the board of directors, or a relevant subcommittee thereof, or other equivalent governing body or, if no such board or equivalent governing body exists, a senior officer of Defendant responsible for Defendant's Information Security Program, that: (1) Defendant has established, implemented, and maintained the requirements of this Order; (2) Defendant is not aware of any material noncompliance that has not been (a) corrected or (b) disclosed to the Bureau; (3) Defendant has cooperated with the Assessor as required by Section IV of this Order; and (4) includes a brief description of any Covered Incident. The certification must be based on the personal knowledge of the senior corporate manager, senior officer, or subject matter experts upon whom the board of directors, or relevant subcommittee thereof, or other equivalent governing body, reasonably relies in making the certification.

- B. Unless otherwise directed by a Bureau representative in writing, submit all annual certifications to the Bureau pursuant to this Order via email to Enforcement\_Compliance@cfpb.gov or by overnight courier (not the U.S. Postal Service) to Enforcement Director, Office of Enforcement, Bureau of Consumer Financial Protection, 1700 G Street NW, Washington, DC 20552. The subject line must begin, “Bureau of Consumer Financial Protection v. Equifax Inc., BCFP File No. 2017-1906-02.”

## **VI. COVERED INCIDENT REPORTS**

**IT IS FURTHER ORDERED** that for twenty (20) years from the entry of the Order, Defendant, within a reasonable time after the date of Defendant’s discovery of a Covered Incident, but in any event no later than ten days after the date Defendant first notifies any U.S. federal, state, or local government entity of the Covered Incident, must submit a report to the Bureau.

- A. The report must include, to the extent possible:
1. The date, estimated date, or estimated date range when the Covered Incident occurred;
  2. A description of the facts relating to the Covered Incident, including the causes and scope of the Covered Incident, if known;

3. A description of each type of information that triggered the notification obligation to the U.S. federal, state, or local government entity;
  4. The number of consumers whose information triggered the notification obligation to the U.S. federal, state, or local government entity;
  5. The acts that Defendant has taken to date to remediate the Covered Incident and protect Personal Information from further exposure or access, and, if applicable, to protect affected individuals from identity theft or other harm that may result from the Covered Incident; and
  6. A representative copy of each materially different notice required by U.S. federal, state, or local law or regulation and sent by Defendant to consumers or to any U.S. federal, state, or local government entity.
- B. No more than thirty days after every calendar quarter, Defendant must provide Defendant's board of directors or relevant subcommittee thereof, or equivalent governing body or, if no such board or equivalent governing body exists, to a senior officer of Defendant responsible for Defendant's Information Security Program, a report summarizing all Covered Incidents that occurred in that calendar quarter.

C. Unless otherwise directed by a Bureau representative in writing, all Covered Incident reports to the Bureau pursuant to this Order must be emailed to the Bureau via secure email to Enforcement\_Compliance@cfpb.gov or sent by overnight courier (not the U.S. Postal Service) to Enforcement Director, Office of Enforcement, Bureau of Consumer Financial Protection, 1700 G Street NW, Washington, DC 20552. The subject line must begin, “Bureau of Consumer Financial Protection v. Equifax Inc., BCFP File No. 2017-1906-02.” Defendant must notify the Bureau of any portions of the Covered Incident Report containing trade secrets, commercial or financial information, or information about a consumer or other third party, for which confidential treatment is requested pursuant to the Bureau’s procedures concerning public disclosure set forth in 12 U.S.C. § 5512(c)(6)(A) and 12 C.F.R. § 1070.20 (2018).

**VII. CREDIT MONITORING AND IDENTITY THEFT PROTECTION**

**IT IS FURTHER ORDERED** that,

A. Defendant must, through an independent third party that will be subject to appointment and oversight by the MDL Court, offer all Affected Consumers four (4) years of a free three-bureau credit monitoring and identity theft protection product, including \$1 million in identity theft insurance and Full

Service Identity Restoration, as described in the attached Exhibit A (the “Product”).

1. The Product shall be offered, provided, and maintained by an independent third party, and shall not be directly provided to any Affected Consumer by Defendant, Defendant’s successors or assigns, or any subsidiary, affiliate, or joint venture of Defendant. Defendant shall not receive any monetary benefit from the Product.
2. Affected Consumers may file a claim to enroll in the Product at any time during the Initial Claims Period, as described in the Claims Administration Protocol.
3. Defendant shall, through the independent third party provider of the Product, provide activation codes for enrollment in the Product to Affected Consumers who file a valid claim for the Product. Activation codes shall be sent no later than forty-five (45) days after either the Class Action Effective Date or the conclusion of the Initial Claims Period, whichever is later. An Affected Consumer shall be eligible to enroll in the Product for a period of at least ninety (90) days following receipt of an activation code.

4. To the extent the independent third party providing the Product assigns personal identification numbers (PINs) to Affected Consumers who made a claim to enroll in the Product, such PINs shall be randomized. As part of the enrollment process, Affected Consumers shall be authenticated using knowledge-based authentication questions, or other comparable authentication procedures. Authentication procedures shall be used any time an Affected Consumer requests a Consumer Report, if applicable, or to lock or unlock their Consumer Report through the Product.
  5. As provided in Subsection XI.G.3, the period during which the Product shall be provided to Affected Consumers may be extended.
- B. Defendant shall also offer Affected Consumers who file valid claims and enroll in the Product with a single-bureau credit monitoring service (“Single Bureau Monitoring”), as described in Exhibit A.
1. Defendant shall provide such Single Bureau Monitoring upon expiration of the Product, including any extensions thereof pursuant to Subsection XI.G.3, to Affected Consumers who enroll in the Product and file valid claims for Single Bureau Monitoring. Defendant shall provide Single Bureau Monitoring for the period of time necessary for

the aggregate number of years of credit monitoring provided under Subsections VII.A, XI.G.3, and VII.B to equal ten (10) years.

2. Defendant shall offer Affected Consumers who were under the age of 18 as of May 13, 2017, additional years of Single Bureau Monitoring, as described in Exhibit A, necessary for the aggregate number of years of credit monitoring provided under Subsections VII.A, XI.G.3, and VII.B to equal eighteen (18) years.
- C. For any Affected Consumer who does not make a claim to enroll in the Product and instead has or has concurrently obtained a credit monitoring or protection product, which he or she will have in place for a minimum of six (6) months, such Affected Consumer may receive One Hundred Twenty-Five Dollars (\$125.00) in alternative compensation (“Alternative Reimbursement Compensation”) by submitting a claim for Alternative Reimbursement Compensation, as set forth in the Claims Administration Protocol.
- D. Defendant shall, through an independent third party that will be subject to appointment and oversight by the MDL Court, offer all Affected Consumers, regardless of whether they have enrolled in the Product, seven (7) years of

free identity restoration services, with the features described in Exhibit A (“Assisted Identity Restoration”).

1. Assisted Identity Restoration shall be offered, provided, and maintained by the independent third party that has been approved by a representative of the Bureau and that will be presented to the MDL Court for approval. Assisted Identity Restoration Services shall not be directly provided to any Affected Consumer by Defendant, Defendant’s successors or assigns, or any subsidiary, affiliate, or joint venture of Defendant. Defendant shall not receive any monetary benefit from Assisted Identity Restoration.
  2. Any Affected Consumer may avail himself or herself of the free Assisted Identity Restoration, as described in Exhibit A, for seven (7) years from the Class Action Effective Date regardless of whether that Affected Consumer filed a claim to enroll in the Product during the Initial Claims Period.
- E. Defendant shall provide all consumers, regardless of whether they are Affected Consumers, with an easily accessible process to place or remove security freezes or locks on their Personal Consumer Reports for free and

without filing a claim for ten (10) years from either (1) the Effective Date of this Order or (2) the Class Action Effective Date, whichever shall occur first.

1. Defendant shall randomize PINs to Affected Consumers requesting a Personal Consumer Report, or lock or security freeze of a Personal Consumer Report.
  2. Defendant, and all other persons acting at Defendant's direction, shall not dissuade or seek to dissuade Affected Consumers from placing or choosing to place a security freeze. Should Defendant offer any standalone product or service as an alternative with substantially similar features as a security freeze, Defendant shall not seek to persuade Affected Consumers to choose the alternative product or service instead of a security freeze.
- F. Defendant shall, for a period of seven (7) years beginning no later than December 31, 2019, provide to all U.S. consumers a clearly accessible process to obtain six (6) free copies during any 12-month period of their Personal Consumer Report, in addition to any free reports to which consumers are entitled under federal law, updated as of the time of request.
- G. Defendant shall, for a period of ten (10) years from the Effective Date of this Order, develop and implement dispute handling procedures, including

escalation to agents specially trained in fraud and a sufficient number of call center representatives to handle reasonably expected call volumes, for Affected Consumers who assert that information on their Personal Consumer Reports is inaccurate as a result of identity theft or fraud.

**VIII. PROHIBITION ON ADVERTISING OR MARKETING TO CONSUMERS WHO USE IDENTITY PROTECTION SERVICES**

**IT IS FURTHER ORDERED** that Defendant, Defendants' officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, shall not use any information provided by Affected Consumers (or the fact that the consumer provided information) to enroll in or use, the Product, the Single Bureau Monitoring, the Full Service or Assisted Identity Restoration set forth in Section VII and Exhibit A, or the free credit monitoring products offered by Defendant in connection with the Breach—Equifax TrustedID Premier, Equifax Credit Watch Gold with 3 in 1 Monitoring, or Experian IDNotify—to sell, upsell, cross-sell, or directly market or advertise its products or services, unless Defendant first obtains and documents the consumer's affirmative express consent.

## **IX. CONSUMER FUND**

**IT IS FURTHER ORDERED** that:

- A. Equifax Inc., its successors and assigns, must deposit the amounts specified in Section XI.B below into the Consumer Fund for the purpose of providing restitution and redress to Affected Consumers, as required by this Section. All applicable taxes, duties, and similar charges due from the Consumer Fund shall be paid from the interest earned on the Consumer Fund.
- B. Pursuant to Section XI, and as set forth in the Claims Administration Protocol, the Consumer Fund shall be used to pay or fund the following:
  1. The cost of providing the Product, including Full Service Identity Restoration, as described in Subsection VII.A and Exhibit A, subject to the requirements of Subsection XI.E;
  2. The cost of providing Assisted Identity Restoration, as described in Subsection VII.D and Exhibit A;
  3. Reimbursements to Affected Consumers who file valid claims for Alternative Reimbursement Compensation, as described in Subsection VII.C;
  4. Reimbursements to Affected Consumers who file valid claims for Out-of-Pocket Losses;

5. Costs and expenses of the Settlement Administrator, including but not limited to processing claims;
  6. Costs and expenses of the Notice Provider, including but not limited to implementing and providing notice to Affected Consumers pursuant to the Notice Plan; and
  7. Service awards, if any, to the Affected Consumers named as plaintiffs in the Multi-District Litigation in the amount approved by the MDL Court.
    - a. Such service awards are not being ordered by the Bureau. Nonetheless, the Bureau does not object to up to Two Hundred Fifty Thousand Dollars (\$250,000) from the Consumer Fund being used to pay service awards to the named plaintiffs in the Multi-District Litigation. To the extent the MDL Court approves service awards in excess of \$250,000, such amounts shall not be paid from the funds deposited into the Consumer Fund pursuant to Section XI.B and shall be paid solely by the Defendant.
- C. Subject to Subsection XI.G, payments from the Consumer Fund shall be subject to the following limitations:

1. Any Affected Consumer may request the restitution and redress described in this Section as follows:
  - a. During the Initial Claims Period, Affected Consumers may file claims for (1) the Product, (2) Single Bureau Monitoring, (3) Alternative Reimbursement Compensation, and (4) reimbursement of Out-of-Pocket Losses;
  - b. During the Extended Claims Period, Affected Consumers may file claims for reimbursement for the following Out-of-Pocket Losses incurred during the Extended Claims Period, only if the Affected Consumer provides a certification that he or she has not obtained reimbursement for the claimed expense through other means:
    - (i) Unreimbursed costs, expenses, losses, or charges incurred by an Affected Consumer as a result of identity theft or identity fraud, falsified tax returns, or other alleged misuse of an Affected Consumer's Personal Information;
    - (ii) Time Compensation to an Affected Consumer, limited to time spent remedying fraud, identity theft, or other

misuse of an Affected Consumer's Personal Information

that is fairly traceable to the Breach; and

(iii) Other miscellaneous expenses, incurred by an Affected Consumer related to remedying fraud, identity theft, or other misuse of an Affected Consumer's Personal Information, such as notary, fax, postage, copying, mileage, and long-distance telephone charges.

2. An Affected Consumer may obtain up to an aggregate maximum amount of \$20,000 in Out-of-Pocket Losses.
3. Time Compensation, a subcategory of Out-of-Pocket Losses, shall be subject to the following provisions:
  - a. Affected Consumers who spent or spend time (1) taking Preventative Measures or (2) remedying fraud, identity theft, or other alleged misuse of the Affected Consumer's Personal Information fairly traceable to the Breach may seek reimbursement for their time.
  - b. Subject to Subsection IX.C.5, Time Compensation shall be paid at a rate of \$25 per hour, reimbursable in 15-minute

increments, with a minimum reimbursement of 1 hour per valid claim for Time Compensation.

- c. Affected Consumers may submit a claim for up to 10 hours of Time Compensation, provided they certify (i) to taking Preventative Measures and/or remedying fraud, identity theft, or other alleged misuse of the Affected Consumer's Personal Information fairly traceable to the Breach, and (ii) an explanation of the time they spent taking Preventative Measures or remedying fraud, identity theft, or other alleged misuse of their Personal Information.
- d. Affected Consumers may submit a claim for up to 20 hours of Time Compensation, provided they spent time remedying fraud, identity theft, or other alleged misuse of the Affected Consumer's Personal Information fairly traceable to the Breach, and provide (i) reasonable documentation (as defined in the Claims Administration Protocol) of the fraud, identity theft, or other alleged misuse of the Affected Consumer's Personal Information fairly traceable to the Breach and

(ii) describe the time spent remedying these issues or time spent taking Preventative Measures in response to these issues.

4. No more than Thirty-One Million Dollars (\$31,000,000) shall be paid as Alternative Reimbursement Compensation for valid claims filed during the Initial Claims Period (the “Alternative Reimbursement Compensation Cap”). To the extent valid claims for Alternative Reimbursement Compensation made during the Initial Claims Period exceed the Alternative Reimbursement Compensation Cap, payments for such valid claims shall be reduced on a *pro rata* basis. At the conclusion of the Extended Claims Period, after all payments required by Subsection IX.B have been made, if there are remaining unused funds in the Consumer Fund, the Alternative Reimbursement Compensation Cap shall be lifted, and payments to Affected Consumers who filed valid claims for Alternative Reimbursement Compensation shall be increased on a *pro rata* basis, up to the full amount of the valid claim, as set forth in Section XI.G.1 below.
5. No more than Thirty-One Million Dollars (\$31,000,000) shall be paid as Time Compensation for valid Time Compensation claims made during the Initial Claims Period (the “Initial Time Compensation

Cap”). To the extent valid claims for Time Compensation made during the Initial Claims Period exceed the Initial Time Compensation Cap, payments for such valid claims shall be reduced on a *pro rata* basis. Valid claims for Time Compensation made during the Extended Claims Period shall be paid in the order they are received and approved at the same *pro rata* rate (if applicable) as valid Time Compensation claims made during the Initial Claims Period. No more than Thirty-Eight Million Dollars (\$38,000,000) in the aggregate shall be paid as Time Compensation for valid claims made during both the Initial Claims Period and Extended Claims Period (“Aggregate Time Compensation Cap”). At the conclusion of the Extended Claims Period, after payment of valid claims made during the Extended Claims Period, to the extent there are remaining unused funds in the Consumer Fund, the Aggregate Time Compensation Cap shall be lifted, and payments to all Affected Consumers who filed valid claims for Time Compensation shall be increased on a *pro rata* basis, up to the full amount of the valid claim, as set forth in Section XI.G.1 below.

## X. NOTICE AND CLAIMS ADMINISTRATION

**IT IS FURTHER ORDERED,** that

- A. The Notice Plan: Notice to Affected Consumers shall be provided pursuant to the Notice Plan. Defendant shall supply the Notice Provider with information in its possession, custody, or control, to the extent reasonably available, regarding the Affected Consumers to enable the Notice Provider to implement the Notice Plan.
- B. The Claims Administration Protocol: Restitution and redress to Affected Consumers shall be administered from the Consumer Fund consistent with the Claims Administration Protocol. Defendant shall supply the Settlement Administrator with information in its possession, custody, or control, to the extent reasonably available, regarding the Affected Consumers to enable the Settlement Administrator to implement and administer the Claims Administration Protocol.
- C. Defendant must notify the Bureau of any requested modifications to the Notice Plan or Claims Administration Protocol, including any change of the Notice Provider or Settlement Administrator, and any such modification requested by the Defendant must be approved by a designated representative

of the Bureau, with such approval not unreasonably withheld, and shall also require approval from the MDL Court.

- D. In connection with the administration of the Consumer Fund overseen by the MDL Court:
1. The Bureau may send a request for information regarding compliance with the Notice Plan, the claims process, and proper administration of the Consumer Fund, and any request will include all parties to the Class Action Settlement and the Commission. Discussion and fulfillment of responses to a request from the Bureau will be made consistent with the Claims Administration Protocol;
  2. The Defendant shall provide to the Bureau the weekly reports prepared by the Settlement Administrator pursuant to the Multi-District Litigation that summarize information related to claims administration;
  3. The Defendant shall provide to the Bureau copies of any reports submitted to the Federal Trade Commission under the FTC Order; and
  4. The information provided to the Bureau described in this Section X.D' shall be treated as confidential pursuant to 12 C.F.R. §1070 (2018) until at least the Class Action Effective Date.

- E. Following the Class Action Effective Date, upon written request by the Bureau, Defendant shall provide the following information, if available, in accordance with instructions provided by a representative of the Bureau to Defendant.
1. The number of unique clicks on the hyperlink for the Settlement Website from the homepage of Defendant's primary, consumer-facing website, [www.equifax.com](http://www.equifax.com);
  2. The number of unique clicks on the hyperlink for the Settlement Website from Defendant's incident website, [www.equifaxsecurity2017.com](http://www.equifaxsecurity2017.com);
  3. The number of viewers who reached the Settlement Website through the notice methods as described in the Notice Plan, where such information can be obtained, including via email communication;
  4. The number of Affected Consumers who filed a claim to enroll in the Product;
  5. The number of Affected Consumers who completed enrollment in the Product;

6. The number and total dollar amount of claims filed by Affected Consumers under the identity theft insurance provided pursuant to the Product, and the total dollar figure and percentage of claims paid;
7. The number of Affected Consumers who filed a claim to enroll in the Single Bureau Monitoring;
8. The number of Affected Consumers who completed enrollment in the Single Bureau Monitoring;
9. The number of Affected Consumers who availed themselves of the Full Service Identity Restoration and Assisted Identity Restoration;
10. The number of Affected Consumers who filed claims for Out-of-Pocket Losses; the total amounts claimed for each subcategory of Out-of-Pocket Losses; the total amount disbursed from the Consumer Fund for each subcategory of Out-of-Pocket Losses, and the average number of days between the date of the claim and the date of disbursement;
11. The number of Affected Consumers who filed claims for Alternative Reimbursement Compensation; the total dollar amount of claims filed for Alternative Reimbursement Compensation; the total amount disbursed from the Consumer Fund for Alternative Reimbursement

Compensation; and the average number of days between the date of the claim and the date of disbursement;

12. The number of consumer complaints received by the Settlement Administrator or the third party providing the Product, regarding (a) access to the Settlement Website, (b) enrollment in the Product, (c) the Product components, (d) identity theft, and (e) other complaints received by the Settlement Administrator relating to the provision of restitution and redress through the Consumer Fund, including the claims process. Defendant shall develop and implement a process to direct consumers that contact Defendant with issues related to the Class Action Settlement or the Consumer Fund to the Settlement Administrator and/or the Settlement Website;
13. The number of consumers who file a dispute or appeal with the Settlement Administrator regarding a denial of any claim; the number of appeals denied; the number of appeals approved; the average number of days between the date of the appeal and the appeal decision; and the average number of days between the appeal decision and disbursement, if applicable; and

14. Any annual reports submitted to the Federal Trade Commission pursuant to the FTC Order.

F. Defendant shall also take the following additional measures to notify Affected Consumers of their ability to enroll in the Product and obtain the restitution and redress set forth in this Order using terms consistent with the approved Notice Plan by, no later than:

1. One day after filing of this Order:

a. Posting a hyperlink to the Settlement Website on the top portion of the landing page for Defendant's primary, consumer-facing website, [www.equifax.com](http://www.equifax.com), which shall state "Visit [www.EquifaxBreachSettlement.com](http://www.EquifaxBreachSettlement.com) for information on the Equifax Data Breach Settlement" or "Equifax Data Breach Settlement," until the expiration of the Initial Claims Period; and

b. Posting a hyperlink to the Settlement Website on Defendant's incident website, [www.equifaxsecurity2017.com](http://www.equifaxsecurity2017.com), which shall state "Visit [www.EquifaxBreachSettlement.com](http://www.EquifaxBreachSettlement.com) for information on the Equifax Data Breach Settlement" or

“Equifax Data Breach Settlement,” until the expiration of the Extended Claims Period.

2. Seven (7) days of entry of an order permitting issuance of notice of the Class Action Settlement:
  - a. Issuing a press release, including a hyperlink to [www.EquifaxBreachSettlement.com](http://www.EquifaxBreachSettlement.com) with information about the Product, the Consumer Fund, and the Settlement Website;
  - b. Posting a monthly Twitter notification via Defendant’s primary Twitter account, the text of which shall read “Visit [www.EquifaxBreachSettlement.com](http://www.EquifaxBreachSettlement.com) for information on the Equifax Data Breach Settlement” until the expiration of the Initial Claims Period, and biannually thereafter until the expiration of the Extended Claims Period; and
  - c. Posting a monthly Facebook notification via Defendant’s primary Facebook account, the text of which shall read “Visit [www.EquifaxBreachSettlement.com](http://www.EquifaxBreachSettlement.com) for information on the Equifax Data Breach Settlement” until the expiration of the Initial Claims Period, and biannually thereafter until the expiration of the Extended Claims Period.

3. To U.S. Consumers, issuing a press release seven (7) days after the relief described in Section VII.F becomes available, with information about the availability of six free copies of a U.S. consumer's Personal Consumer Report during any twelve-month period for seven years, including a hyperlink to the webpage where consumers can request free Personal Consumer Reports.

## XI. MONETARY JUDGMENT

**IT IS FURTHER ORDERED** that:

- A. Judgment in the amount of Four Hundred Twenty-Five Million Dollars (\$425,000,000) is entered in favor of the Bureau against Defendant for the purpose of providing restitution and redress to Affected Consumers.
- B. Equifax Inc., its successors and assigns, shall pay this judgment as follows:
  1. No later than fifteen (15) days following the date this Order is filed, Equifax Inc. shall deposit into the Consumer Fund One Hundred Fifty Thousand Dollars (\$150,000) to cover reasonable set-up costs of the Notice Provider;
  2. No later than fifteen (15) days after the MDL Court enters an order permitting issuance of notice of class action settlement for the Class Action Settlement, Equifax Inc., its successors and assigns, shall

deposit into the Consumer Fund Twenty-Five Million Dollars (\$25,000,000) to cover reasonable costs and expenses of the Settlement Administrator and Notice Provider and set-up costs for the independent third-party providing the Product and Assisted Identity Restoration;

3. No later than fifteen (15) days following the Class Action Effective Date, Equifax Inc., its successors and assigns, shall deposit Three Hundred Million Dollars (\$300,000,000) into the Consumer Fund, less any amounts paid pursuant to Sections XI.B.1 and XI.B.2, to be used for the purposes set forth in Sections VII and IX; and
4. Equifax Inc., its successors and assigns, shall make all payments into the Consumer Fund as required by Section XI.C, up to a maximum of One Hundred Twenty-Five Million Dollars (\$125,000,000).

- C. If at any time during the Initial Claims Period or the Extended Claims Period, there are insufficient funds in the Consumer Fund (or, if it has received a written notice of a Triggering Event as described below in Subsection XI.I, a fund administered by the Federal Trade Commission or its designee on behalf of the Federal Trade Commission, the Bureau, and the States' Attorneys' General) to pay valid claims pursuant to Section IX (a

“Shortfall”), Equifax Inc., its successors and assigns, shall make additional payments into the Consumer Fund of up to One Hundred Twenty-Five Million Dollars (\$125,000,000) for the purpose of paying Out-of-Pocket Losses.

- D. Defendant shall notify the Enforcement Director within three (3) business days of when the Settlement Administrator notifies Defendant of a Shortfall, as set forth in the Claims Administration Protocol. This notification shall identify the amount needed to pay the Shortfall. Within fourteen (14) days of receiving written notice from the Settlement Administrator of a Shortfall, Equifax Inc., its successors and assigns, shall deposit money into the Consumer Fund in the amount necessary to cure the Shortfall.
- E. Equifax Inc., its successors and assigns, is ordered to pay into the Consumer Fund (or, if it has received a written notice of a Triggering Event as described below in Subsection XI.I, a fund administered by the Federal Trade Commission or its designee on behalf of the Federal Trade Commission, the Bureau, and the States’ Attorneys’ General) additional amounts for purposes of providing restitution and redress to Affected Consumers, as follows:

- l. If, at the end of the Initial Claims Period, more than 7 million Affected Consumers have enrolled in the Product, the following obligations apply:
  - a. If the total payments required under Subsections IX.B.2-7 and the cost of providing the Product to 7 million Affected Consumers (the “Costs”) are greater than or equal to Three Hundred Million Dollars (\$300,000,000), Equifax Inc., its successors and assigns, shall pay into the Consumer Fund an amount equal to the cost of providing the Product to enrollees above 7 million (the “Additional Credit Monitoring Cost”);
  - b. If the Costs are less than \$256,500,000 and the Additional Credit Monitoring Cost is greater than \$43,500,000, Equifax Inc., its successors and assigns, shall pay into the Consumer Fund an amount equal to the Additional Credit Monitoring Cost less \$43,500,000; and
  - c. If (i) the Costs are greater than or equal to \$256,500,000, but less than \$300,000,000 and (ii) the Costs plus the Additional Credit Monitoring Costs are greater than \$300,000,000, Equifax Inc., its successors and assigns, shall pay into the Consumer

Fund an amount equal to the Costs plus Additional Credit

Monitoring Costs less \$300,000,000.

2. If, during the Extended Claims Period, more than 7 million Affected Consumers have enrolled in the Product and either (i) the Costs are greater than or equal to \$256,500,000 or (ii) the Additional Credit Monitoring Costs are greater than or equal to \$43,500,000 then, on a monthly basis, Equifax Inc., its successors and assigns shall deposit any additional money into the Consumer Fund that would be required pursuant to the calculations in Subsection XI.E.1.a-c, less any amounts previously deposited pursuant to Subsection XI.E.1 or previously under this subsection.
- F. An amount no less than \$300 million, plus any amount deposited in the Consumer Fund pursuant to Subsections XI.C and XI.E, including all accumulated interest, must be used and administered as described in Subsections VII and IX for the exclusive benefit of Affected Consumers.
- G. At the conclusion of the Extended Claims Period, the Settlement Administrator shall distribute or use any remaining funds as follows:
  1. First, the Aggregate Time Compensation Cap and Alternative Reimbursement Compensation Cap, as described in Subsections

IX.C.4-5, shall both be lifted (if applicable) and payments increased *pro rata* to Affected Consumers who submitted valid claims for Time Compensations and/or Alternative Reimbursement Compensation up to the full amounts of those claims; then

2. Second, to provide Assisted Identity Restoration to all Affected Consumers for up to an additional thirty-six (36) months in full-month increments; then
3. Third, to extend the duration of the Product to Affected Consumers enrolled in the Product until the funds in the Consumer Fund are exhausted.

H. The money deposited into the Consumer Fund and all accumulated interest shall be administered by the Settlement Administrator consistent with the Claims Administration Protocol.

I. If any of the following events (“Triggering Events”) should occur, the Bureau and the Federal Trade Commission may, in their sole discretion, jointly send Defendant a written notice of a Triggering Event:

1. A settlement agreement releasing settlement class action member claims in the Multi-District Litigation and a motion for an order permitting issuance of notice of the Class Action Settlement

containing terms materially similar to those outlined in Sections VII, IX, X, and XI, and Exhibit A of this Order, is not submitted to the MDL Court within fourteen (14) days after the filing of this Order, provided however that the Defendant, the Bureau, or the Federal Trade Commission are not the cause of such failure;

2. The MDL Court declines to enter an order permitting issuance of notice of class action settlement for a settlement agreement releasing settlement class member claims in the Multi-District Litigation with terms materially similar to those outlined in Sections VII, IX, X, and XI, and Exhibit A of this Order and either (i) a modified settlement agreement releasing settlement class member claims is not submitted to the MDL Court within sixty (60) days; or (ii) a modified settlement agreement releasing settlement class member claims is submitted to the MDL Court without Defendant first obtaining approval from a representative of the Bureau, which approval shall not be unreasonably withheld, shall not be refused if the proposed modification is no less favorable to Affected Consumers than the terms of this Order, and shall be timely provided;

3. The MDL Court declines to enter a Final Approval Order for a settlement agreement releasing settlement class member claims in the Multi-District Litigation with terms materially similar to those outlined in Sections VII, IX, X, and XI, and Exhibit A of this Order and either (i) a modified settlement agreement releasing settlement class member claims is not submitted to the MDL Court within sixty (60) days; or (ii) a modified settlement agreement releasing settlement class member claims is submitted to the MDL Court without Defendant first obtaining approval from a representative of the Bureau, which approval shall not be unreasonably withheld, shall not be refused if the proposed modification is no less favorable to Affected Consumers than the terms of this Order, and shall be timely provided;
4. The MDL Court's Final Approval Order is overturned on appeal and either (i) a modified settlement agreement releasing settlement class member claims is not submitted to the MDL Court within sixty (60) days; or (ii) a modified settlement agreement releasing settlement class member claims in the Multi-District Litigation is submitted to the MDL Court without Defendant first obtaining approval from a

representative of the Bureau, which approval shall not be unreasonably withheld, shall not be refused if the proposed modification is no less favorable to Affected Consumers than the terms of this Order, and shall be timely provided; and

5. The MDL Court approves a modified settlement agreement other than the one approved by the Bureau releasing settlement class member claims in the Multi-District Litigation that interferes in any way with the Bureau's ability to enforce this Order.
- J. If one of the events described in Subsection XI.I.2-4 occurs as a result of an objection filed by the Bureau, the Commission, or the States' Attorneys General in the MDL Court to either the Class Action Settlement or a modified settlement agreement releasing settlement class member claims in the Multi-District Litigation and such Class Action Settlement or modified settlement agreement contains terms materially similar to Sections VII, IX, X, and XI, and Exhibit A, such event shall not constitute a Triggering Event. If the Commission and the Bureau jointly send Defendant a written notice of a Triggering Event, Sections XI.I-L of this Order will not be construed in a way that interferes with the Multi-District Litigation.

- K. Any modified settlement agreement submitted to the MDL Court pursuant to Subsections XI.I.2-4 shall contain terms that provide no less relief to Affected Consumers than set forth in this Order. If Defendant fails to comply with Subsections XI.B.1, XI.B.2, XI.B.3, or XI.B.4, and receives written notice of such failure, or if the Bureau and Federal Trade Commission send Defendant a written notice of a Triggering Event pursuant to XI.I, then the Bureau may move to enforce this Order. Defendant waives any objections to the Bureau's motion to enforce the Order under the circumstances described in this paragraph. All other provisions of this Order shall remain in full force and effect, and the Bureau and Commission shall jointly notify Defendant in writing that the Notice Plan (to the extent it has not already been administered) and the Claims Administration Protocol will be administered under the supervision of the Federal Trade Commission on behalf of the Bureau, the Federal Trade Commission, and the States' Attorneys General pursuant to Section XI of the FTC Order.
- L. If Defendant fails to comply with Subsections XI.B.1, XI.B.2, XI.B.3, or XI.B.4, and receives a written notice of such failure, or Defendant receives a written notice of a Triggering Event as further described in Subsection XI.I,

then Equifax Inc., its successors and assigns, shall pay the judgment as follows:

1. Within twenty one (21) days, deposit \$300,000,000 plus any interest accumulated in the Consumer Fund attributed to any payment required pursuant to Section XI.B, less any payments that have already been disbursed by the Settlement Administrator, into a fund administered by the Federal Trade Commission or its designee on behalf of the Federal Trade Commission, the Bureau, and States' Attorneys' General to be used for consumer restitution and redress as set forth in this Order;
2. Make all payments required by Subsection XI.C up to a maximum of One Hundred Twenty-Five Million Dollars (\$125,000,000) into such fund; and
3. Make all payments required by Subsection XI.E into such fund.

## **XII. CIVIL MONEY PENALTIES**

**IT IS FURTHER ORDERED** that:

- A. Under section 1055(c) of the CFPA, 12 U.S.C. § 5565(c), by reason of the violations of law described in the Complaint, and taking into account the factors in 12 U.S.C. § 5565(c)(3), Equifax Inc., its successors and assigns,

must pay a civil money penalty of One Hundred Million Dollars (\$100,000,000) to the Bureau (“Civil Money Penalty”). The penalty paid under this Order will be deposited in the Civil Penalty Fund of the Bureau as required by section 1017(d) of the CFPA, 12 U.S.C. § 5497(d).

- B. Within 30 days of the Effective Date of this Order, Equifax Inc., its successors and assigns, must pay the civil money penalty by wire transfer to the Bureau or to the Bureau’s agent in compliance with the Bureau’s wiring instructions.
- C. Defendant must treat the penalty paid under this Order as a penalty paid to the government for all purposes. Regardless of how the Bureau ultimately uses those funds, Defendant may not:
  - 1. Claim, assert, or apply for a tax deduction, tax credit, or any other tax benefit for the penalty paid under this Order; or
  - 2. Seek or accept, directly or indirectly, reimbursement or indemnification from any source, including but not limited to payment made under any insurance policy, with regard to the penalty paid under this Order.
- D. To preserve the deterrent effect of the penalty in any Related Consumer Action, Defendant may not argue that Defendant is entitled to, nor may

Defendant benefit by, any offset or reduction of any compensatory monetary remedies imposed in any Related Consumer Action because of the penalty paid in this action. If the court in any Related Consumer Action offsets or otherwise reduces the amount of compensatory monetary remedies imposed against Defendant based on the penalty paid in this action or based on any payment that the Bureau makes from the Civil Penalty Fund, Defendant must, within 30 days after entry of a final order granting such offset or reduction, notify the Bureau, and pay the amount of the offset or reduction to the U.S. Treasury. Such a payment will not be considered an additional civil money penalty and will not change the amount of the civil money penalty imposed in this action.

### **XIII. ADDITIONAL MONETARY PROVISIONS**

**IT IS FURTHER ORDERED** that:

- A. In the event of any default on Defendant's obligations to make payment under this Order, interest computed under 28 U.S.C. § 1961, as amended, will accrue on any outstanding amounts not paid from the date of default to the date of payment, and will immediately become due and payable.
- B. Defendant relinquishes dominion and all legal and equitable right, title, and interest in all assets transferred pursuant to this Order and may not seek the

return of any assets, except in the event of a Triggering Event. In that instance, Defendant shall have the right to seek the return of assets deposited into the Fund that have not been disbursed by the Settlement Administrator so that Defendant may provide such assets to the Federal Trade Commission to begin disbursing funds from the Consumer Fund and performing, pursuant to Subsections XI.K-L, all duties and obligations under this Order.

- C. The facts alleged in the Complaint will be taken as true, without further proof, in any subsequent civil litigation by or on behalf of the Bureau in a proceeding to enforce its rights to any payment or monetary judgment pursuant to this Order, such as a nondischargeability complaint in any bankruptcy case.
- D. The facts alleged in the Complaint establish all elements necessary to sustain an action by the Bureau pursuant to Section 523(a)(2)(A) of the Bankruptcy Code, 11 U.S.C. § 523(a)(2)(A), and this Order will have collateral estoppel effect for such purposes.
- E. Defendant acknowledges that its Taxpayer Identification Number, which Defendant must submit to the Bureau, may be used for collecting and reporting on any delinquent amount arising out of this Order, in accordance with 31 U.S.C. § 7701.

- F. On an annual basis for twenty (20) years following the Effective Date of this Order, Defendant must provide the Enforcement Director in writing with the total number of final judgments, consent orders, or settlements in Related Consumer Actions during the preceding year, as well as the total amount of redress, if any, that Defendant paid or was required to pay to consumers pursuant to those Related Consumer Actions, and describe the consumers or classes of consumers to whom that redress, if any, has been or will be paid.

#### **XIV. ORDER ACKNOWLEDGMENTS**

**IT IS FURTHER ORDERED** that Defendant obtain acknowledgments of receipt of this Order:

- A. Defendant, within seven (7) days of entry of this Order, must submit to the Bureau an acknowledgment of receipt of this Order sworn under penalty of perjury.
- B. Within 30 days of the Effective Date, Defendant must deliver a copy of this Order to all (1) principals, officers, directors, and LLC managers and members, and (2) all employees, managers, agents, representatives, and service providers having managerial or supervisory responsibilities for conduct related to the subject matter of the Order. For ten (10) years from the Effective Date, Defendant must deliver a copy of this Order to: (1) any

business entity resulting from any change in structure as set forth in Section XV; (2) all future board members and executive officers; and (3) all employees, managers, agents, representatives, and service providers having managerial or supervisory responsibilities for conduct related to the subject matter of the Order before the date on which they assume their responsibilities.

- C. From each individual or entity to which Defendant delivered a copy of this Order, Defendant must obtain, within 30 days, a signed and dated acknowledgment of receipt of this Order, ensuring that any electronic signatures conform with the requirements of the E-Sign Act, 15 U.S.C. § 7001 *et seq.*

## XV. COMPLIANCE REPORTING

**IT IS FURTHER ORDERED** that Defendant make timely submissions to the Bureau:

- A. Within seven (7) days after the entry of this Order, Defendant must identify the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Bureau may use to communicate with Defendant.

- B. One year after entry of this Order, Defendant must submit a compliance report, sworn under penalty of perjury, in which Defendant must: (a) identify the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Bureau may use to communicate with Defendant; (b) identify all of Defendant's businesses by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; (c) describe the activities of each business identified in (b), including the goods or services offered, the means of advertising, marketing, and sales, and the categories or types of Personal Information collected, transferred, maintained, processed or stored by each business; (d) describe in detail whether and how Defendant is in compliance with each Section of this Order; and (e) provide a copy of, or record proving, each Order Acknowledgment obtained pursuant to this Order, unless previously submitted to the Bureau.
- C. For twenty (20) years after entry of this Order, Defendant must submit a compliance notice, sworn under penalty of perjury, within 14 days of any change in the following: (a) any designated point of contact; or (b) the structure of any entity that Defendant has any ownership interest in or controls directly or indirectly that may affect compliance obligations arising

under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order.

- D. Defendant must submit to the Bureau notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against the Defendant within fourteen (14) days of its filing.
- E. Any submission to the Bureau required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by concluding: “I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: \_\_\_\_\_” and supplying the date, signatory’s full name, title (if applicable), and signature.
- F. Unless otherwise directed by a Bureau representative in writing, all submissions to the Bureau pursuant to this Order must be emailed to Enforcement\_Compliance@cfpb.gov and sent by overnight courier or first class mail to Enforcement Director, Bureau of Consumer Financial Protection, 1700 G Street NW, Washington, DC 20552. The subject line must begin “Bureau of Consumer Financial Protection v. Equifax Inc., BCFP File No. 2017-1906-02.”

## XVI. RECORDKEEPING

**IT IS FURTHER ORDERED** that Defendant must create certain records for twenty (20) years after entry of the Order, and retain each such record for five (5) years. Specifically, Defendant must create and retain the following records:

- A. Accounting records showing the revenues from all goods or services sold;
- B. Personnel records showing, for each person providing services, whether as an employee or otherwise, that person's: name; addresses; telephone numbers; job title or position; dates of service; and (if applicable) the reasons for termination;
- C. Copies of records of all U.S. consumer complaints concerning the subject matter of the Order, whether received directly or indirectly, such as through a third party, and any response;
- D. Copies of final judgments, consent orders, or settlements in Related Consumer Actions;
- E. A copy of each information security assessment required by this Order and any material evaluations of Defendant's physical, technical, or administrative controls to protect the confidentiality, integrity, or availability of Personal Information;

- F. A copy of each widely disseminated and unique representation by Defendant that describes the extent to which Defendant maintains or protects the privacy, confidentiality, security, or integrity of any Personal Information;
- G. For five (5) years after the date of preparation of each Assessment required by this Order, all materials and evidence that are in Defendant's possession and control that the Assessor considered, reviewed, relied upon or examined to prepare the Assessment, whether prepared by or on behalf of Defendant, including all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials concerning Defendant's compliance with related Sections of this Order, for the compliance period covered by such Assessment; and
- H. All records necessary to demonstrate full compliance with each Section of this Order; including all submissions to the Bureau.

## **XVII. COMPLIANCE MONITORING**

**IT IS FURTHER ORDERED** that, for the purpose of monitoring Defendant's compliance with this Order:

- A. Within fourteen (14) days of receipt of a written request from a representative of the Bureau, Defendant must: submit additional compliance reports or other requested information, related to the requirements of this

Order, which must be sworn under penalty of perjury; provide sworn testimony and appear for depositions; and produce documents related to the requirements of this Order and Defendant's compliance with those requirements, for inspection and copying. The Bureau is also authorized to obtain discovery, without further leave of court, using any of the procedures prescribed by Federal Rules of Civil Procedure 29, 30 (including telephonic depositions), 31, 33, 34, 36, 45, and 69.

- B. For matters concerning this Order, the Bureau is authorized to communicate directly with Defendant. Defendant must permit representatives of the Bureau to interview any employee or other person affiliated with Defendant who has agreed to such an interview. The person interviewed may have counsel present.
- C. The Bureau may use all other lawful means, including posing, through its representatives, as consumers, suppliers, or other individuals or entities, to Defendant or any individual or entity affiliated with Defendant, without the necessity of identification or prior notice. Nothing in this Order limits the Bureau's lawful use of civil investigative demands under 12. C.F.R. § 1080.6 (2018) or other compulsory process.

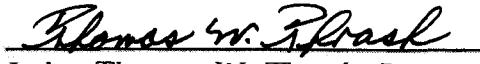
## XVIII. SEVERABILITY

**IT IS FURTHER ORDERED** that if any clause, provision, or section of this Order shall, for any reason, be held illegal, invalid, or unenforceable, such illegality, invalidity or unenforceability shall not affect any other clause, provision or section of this Order and this Order shall be construed and enforced as if such illegal, invalid or unenforceable clause, section or provision had not been contained herein.

## XIX. RETENTION OF JURISDICTION

**IT IS FUTHER ORDERED** that this Court retains jurisdiction of this matter for purposes of construction, modification, and enforcement of this Order.

SO ORDERED this 23 day of July, 2019.

  
\_\_\_\_\_  
Judge Thomas W. Thrash, Jr.  
United States District Court  
Chief Judge

**LOCAL COUNSEL:**

BYUNG J. PAK  
United States Attorney



AKASH DESAI  
Assistant U.S. Attorney  
Georgia Bar No. 338124  
600 U.S. Courthouse  
75 Ted Turner Drive SW  
Atlanta, Georgia 30303  
Telephone: 404-581-6364  
Facsimile: 404-581-6181

**FOR PLAINTIFF:**

**BUREAU OF CONSUMER  
FINANCIAL PROTECTION**

CARA PETERSEN  
Acting Enforcement Director

JOHN WELLS  
Deputy Enforcement Director



JENELLE M. DENNIS  
D.C. Bar No. 494958  
RICHYA DASGUPTA  
D.C. Bar No. 500509  
P. SOLANGE HILFINGER-PARDO  
California Bar No. 320055  
EMILY MINTZ SACHS  
Virginia Bar No. 82437  
Bureau of Consumer Financial Protection  
1700 G Street, NW  
Washington, DC 20552  
Telephone: (202) 435-9118 (Dennis)  
Facsimile: (202) 425-7722  
Email: jenelle.dennis@cfpb.gov

**FOR DEFENDANT:**

  
JOHN J. KELLEY III  
Corporate Vice President, Chief Legal  
Officer  
Equifax Inc.  
1550 Peachtree Street, NW  
Atlanta, GA 30309

Date: 7/17/19

  
EDITH RAMIREZ  
HARRIET PEARSON  
MICHELLE KISLOFF  
TIMOTHY TOBIN  
Hogan Lovells US LLP  
555 Thirteenth Street, NW  
Washington, DC 20004  
Tel: (202) 637-5600  
Fax: (202) 637-5910

Date: 7/19/19

# Exhibit A

## **Triple-Bureau Credit and Identity Monitoring Product**

The following provisions are subject to the terms and definitions set forth in the Stipulated Order for Permanent Injunctive and Monetary Judgment (the “Order”).

The Product as defined in the Order includes:

1. Daily Consumer Report monitoring from each of the three nationwide Consumer Reporting Agencies showing key changes to one or more of an Affected Consumer’s Consumer Reports, including automated alerts when the following occur: new accounts are opened; inquiries or requests for an Affected Consumer’s Consumer Report for the purpose of obtaining credit, including for new credit card applications; changes to an Affected Consumer’s address; and negative information, including delinquencies or bankruptcies;
2. On-demand online access to a free copy of an Affected Consumer’s Experian Consumer Report, updated on a monthly basis;
3. Automated alerts, using public or proprietary data sources:
  - i. 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;”

- ii. when names, aliases, and addresses have been associated with the Affected Consumer's Social Security number;
  - iii. when a payday loan or certain other unsecured credit has been taken or opened using the Affected Consumer's Social Security number;
  - iv. when an Affected Consumer's information matches information in arrest records or criminal court records;
  - v. when an individual uses an Affected Consumer's information for identity authentication;
  - vi. when an Affected Consumer's mail has been redirected through the United States Postal Service;
  - vii. when banking activity is detected related to new deposit account applications, opening of new deposit accounts, changes to an Affected Consumer's personal information on an account, and new signers being added to an Affected Consumer's account; and
  - viii. when a balance is reported on an Affected Consumer's credit line that has been inactive for at least six months;
4. 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 Product, provided the costs result from a stolen identity event first discovered during the policy period and subject to the terms of the insurance policy;

5. A customer service center to provide assistance with enrollment, website navigation, monitoring alerts questions, dispute assistance, fraud resolution assistance, and other assistance related to the Product;
6. Full Identity Restoration Services as described below; and
7. For Affected Consumers under the age of 18, the Product includes 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;" 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 Consumer Report at one or more of the three nationwide Consumer Reporting Agencies; and Full Service Identity Restoration, working with the legal guardian, in the event that an Affected Consumer under the age of 18 has their identity compromised. Upon turning 18, the Affected Consumer can enroll in the full Product. If an Affected Consumer under the age of 18 has an Experian Consumer Report with sufficient detail to permit

authentication, a parent or guardian may enroll them in the full Product prior to their eighteenth birthday.

## **Identity Restoration Services**

The following provisions are subject to the terms and definitions set forth in the Stipulated Order for Permanent Injunctive and Monetary Judgment (the “Order”).

Identity Restoration Services consist of “Assisted Identity Restoration” and “Full Service Identity Restoration” provided by a third party not affiliated with Defendant.

1. **Assisted Identity Restoration:** Any Affected Consumer who is not enrolled in the Product may avail themselves of Assisted Identity Restoration for seven (7) years from the Class Action Effective Date. Assisted Identity Restoration includes assignment of a dedicated identity theft restoration specialist to an Affected Consumer who has experienced an identity theft event. The specialist provides assistance to the Affected Consumer in addressing that identity theft event, including a customized step-by-step process with form letters to contact companies, government agencies, Consumer Reporting Agencies, or others, and by participating in conference calls with an affected financial institution or government agency related to the identity theft event.
2. **Full Service Identity Restoration:** Any Affected Consumer who is enrolled in the Product may avail themselves of Full Service Identity

Restoration while they are enrolled. Full Service Identity Restoration includes assignment of a dedicated identity theft restoration specialist to an Affected Consumer who has experienced an identity theft event, as well as use of a specialized limited power of attorney for the specialist to assist the Affected Consumer in addressing the identity theft event, including by contacting companies, government agencies, or Consumer Reporting Agencies on behalf of the Affected Consumer. Full Service Identity Restoration also includes the use of interactive dispute letters.

## **Equifax Single Bureau Monitoring**

The following provisions are subject to the terms and definitions set forth in the Stipulated Order for Permanent Injunctive and Monetary Judgment (the “Order”).

Equifax Single Bureau Monitoring will include the following:

1. Daily Consumer Report monitoring from Equifax showing key changes to an Affected Consumer’s Personal Consumer Report including automated alerts when the following occur: new accounts are opened; inquiries or requests for an Affected Consumer’s Consumer Report for the purpose of obtaining credit, including for new credit card applications; changes to an Affected Consumer’s address; and negative information, such as delinquencies or bankruptcies;
2. On-demand online access to a free copy of an Affected Consumer’s Personal Consumer Report, updated on a monthly basis;
3. 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;” and

4. For Affected Consumers under the age of 18, Equifax shall 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. 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 a Personal Consumer Report, a Personal Consumer Report is created, locked, and then monitored; and for minors with a Personal Consumer Report, their Personal Consumer Report is locked and then monitored. The types of alerts that minors receive through child monitoring services are the same as the types of alerts that adults receive.