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

FEDERAL TRADE COMMISSION, Plaintiff, v. EQUIFAX INC., Defendant.	Case No. 1:19-cv-03297-TWT **STIPULATED ORDER FOR PERMANENT INJUNCTION AND MONETARY JUDGMENT**

Plaintiff, the Federal Trade Commission ("Commission"), filed its Complaint for a permanent injunction and other relief in this matter, pursuant to Section 13(b) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 53(b). The Commission and Defendant Equifax Inc. ("Defendant") stipulate to entry of this Order for Permanent Injunction and Monetary Judgment ("Order") to resolve all matters 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 charges that Defendant engaged in acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45, and the Standards for

Safeguarding Customer Information Rule ("Safeguards Rule"), 16 C.F.R. Part 314, issued pursuant to Sections 501(b) and 505(b)(2) of the Gramm-Leach-Bliley Act ("GLB Act"), and 15 U.S.C. §§ 6801(b) and 6805(6b)(2), by failing to reasonably secure sensitive consumer personal information in Defendant's networks and computer systems.

3. Defendant neither admits nor denies any of the allegations in the Complaint, except as specifically stated in this Order. Only for purposes of this action, Defendant admits the facts necessary to establish jurisdiction.

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. Defendant and the Commission waive all rights to appeal or otherwise challenge or contest the validity of this Order.

DEFINITIONS

For the purpose of this Order, the following definitions apply:

1. "**Affected Consumer**" means the approximately One Hundred Forty Seven Million (147,000,000) U.S. consumers whom Defendant has identified whose Personal Information was accessed without authorization as a result of the Breach.

2. "**Alternative Reimbursement Compensation**" means compensation for any Affected Consumer who does not make a claim to enroll in the Product, and instead, has or has concurrent with their claim obtained a credit monitoring or protection product.
3. "**Assisted Identity Restoration Services**" means the identity restoration services, as set forth in Section IX and described in Exhibit A, offered to all Affected Consumers who have or may have experienced identity theft or fraud.
4. "**Breach**" means the information security incident publicly disclosed by Defendant on or about September 7, 2017.
5. "**Claims Administration Protocol**" means the protocol that has been approved by a representative of the Commission and which will be submitted to and approved by the MDL Court, to implement the claims administration and Settlement process in the Multi-District Litigation.
6. "**Claims Forms**" are the forms that have been approved by a representative of the Commission and which will be submitted to and approved by the MDL Court, that Affected Consumers submit to the Settlement Administrator in paper or via the Settlement Website to make claims for Out-of-Pocket Losses, Alternative Reimbursement Compensation, the Product, and Single-Bureau Monitoring.

7. "**Class Action Effective Date**" means the first business day after the MDL Court enters final approval of the Settlement, 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 regarding any issue with the Settlement, 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, rehearings, or other reviews are dismissed or otherwise disposed of and the time for further appeals, petitions, requests for rehearing or other review has expired.
8. "**Clear(ly) and Conspicuous(ly)**" means that a required disclosure is difficult to miss (i.e., easily noticeable) and easily understandable by ordinary consumers, including in all of the following ways:
    a. In any communication that is solely visual or solely audible, the disclosure must be made through the same means through which the communication is presented. In any communication made through both visual and audible means, such as a television advertisement, the disclosure must be presented simultaneously in both the visual and audible portions of the communication even if the representation

requiring the disclosure ("Triggering Representation") is made in only one means.

b. A visual disclosure, by its size, contrast, location, the length of time it appears, and other characteristics, must stand out from any accompanying text or other visual elements so that it is easily noticed, read, and understood.

c. An audible disclosure, including by telephone or streaming video, must be delivered in a volume, speed, and cadence sufficient for ordinary consumers to easily hear and understand it.

d. In any communication using an interactive electronic medium, such as the Internet or software, the disclosure must be unavoidable.

e. The disclosure must use diction and syntax understandable to ordinary consumers and must appear in a language in which the Triggering Representation appears.

f. The disclosure must comply with these requirements in each medium through which it is received, including all electronic devices and face-to-face communications.

g. The disclosure must not be contradicted or mitigated by, or inconsistent with, anything else in the communication.

h. When the representation or sales practice targets a specific audience, such as children, the elderly, or the terminally ill, "ordinary consumers" includes reasonable members of that group.

9. "**Consumer Fund**" means the account established to provide restitution and redress to Affected Consumers as described in Sections VIII, IX and X, and which will be overseen by the MDL Court and which represents an undifferentiated portion of the consumer restitution fund as defined in the Settlement.

10. "**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 entry 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 FCRA Section 604, 15 U.S.C. § 1681b.

11. "**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 entry 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.

12. "**Covered Incident**" means any instance in which any U.S. 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 at least 250 U.S. consumers.

13. "**Defendant**" means (1) Equifax Inc., and its successors and assigns, and (2) Equifax Inc.'s subsidiaries, and 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 their conduct falls within the Commission's jurisdiction.

14. "**Extended Claims Period**" means the period of time ending four years after the conclusion of the Initial Claims Period.

15. "**Full Service Identity Restoration Services**" means the identity restoration services offered to all Affected Consumers enrolled in the Product, as described in Exhibit A.

16. "**Initial Claims Period**" means the period of time ending six months after entry of the order permitting issuance of notice in the Multi-District Litigation.

17. "**MDL Court**" means the Court presiding over the Multi-District Litigation.

18. "**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 Breach Litigation*, 1:17-md-02800-TWT (N.D. Ga.).

19. "**Notice and Settlement Administration Costs and Expenses**" means the costs and expenses of the Notice Provider, Notice Plan, Claims Administration Protocol, and Settlement Administrator.

20. "**Notice Date**" means sixty days after the MDL Court issues an order permitting issuance of notice of the Settlement.

21. "**Notice Plan**" means the plan that has been approved by a representative of the Commission and which will be submitted to, approved by, and overseen by the MDL Court, for providing notice to Affected Consumers in the Multi-District Litigation.

22. "**Notice Provider**" means Signal Interactive Media or another independent third-party agent or administrator that has been approved by a representative of the Commission, and which will be submitted to, approved by, and overseen by the MDL Court to implement the Notice Plan.

23. "**Out-of-Pocket Losses**" means verifiable unreimbursed costs or expenditures that an Affected Consumer incurred and that are fairly traceable to the Breach, which are eligible for reimbursement from the Consumer Fund as set forth in Sections IX.B.1.c and IX.B.2.

24. "**Personal Consumer Report**" means the 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).

25. "**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.

26. "**Preventative Measures**" means placement or removal of security freezes or obtaining credit monitoring services.

27. "**Product**" means the three-bureau credit and identity monitoring product, including any changes, as described in Exhibit A and approved by a representative of the Commission and then approved by the MDL Court.

28. "**Service Awards**" means compensation awarded to the consumers named as plaintiffs in the Multi-District Litigation.

29. "**Settlement**" means the settlement resolving the Multi-District Litigation.

30. "**Settlement Administrator**" means JND Legal Administration, or another independent third-party agent or administrator that has been approved by a representative of the Commission, and which will be submitted to, approved by, and overseen by the MDL Court to implement the processes described in the Claims Administration Protocol, and claims and Settlement process in the Multi-District Litigation.

31. "**Settlement Website**" means the website established by the Settlement Administrator, and described in the Claims Administration Protocol, that has been approved by a representative of the Commission to provide information about the Settlement, including deadlines and case documents, and permit Affected Consumers to electronically submit Claims Forms.

32. "**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.

33. "**Time Compensation**" means compensation to an Affected Consumer 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 good 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 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 assessments required under Section II.D;
2. Documented safeguards required under Section 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 Section 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 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 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 Section II.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, including notifying employees of the process for submitting complaints and concerns pursuant to Section II.E.12; 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 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 months and, as they relate to a Covered Incident, promptly (not to exceed sixty 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 months and, as it relates to a Covered Incident, promptly (not to exceed sixty days) following verification of such an incident, and penetration testing of Defendant's network at least once every twelve months and, as it relates to a Covered Incident, promptly (not to exceed sixty 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 months and, as it relates to a Covered Incident, promptly (not to exceed sixty 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 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 years after completion of such Assessment, and to provide such documents to the Commission within fourteen days of receipt of a written request from a representative of the Commission. 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 the Assessor, although such documents can be designated for confidential treatment in accordance with applicable law.

B. For each Assessment, Defendant shall provide the Associate Director for Enforcement for the Bureau of Consumer Protection at the Federal Trade Commission with the name and affiliation of the person selected to conduct the Assessment, which the Associate Director shall have the authority to approve in his or her sole discretion. If the Associate Director for Enforcement 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 Commission.

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 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 Commission representative in writing, Defendant must submit each Assessment to the Commission within ten days after the Assessment has been completed via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "Federal Trade Commission v. Equifax Inc., FTC File No. 1723203." Defendant must notify the Commission 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 Commission's procedures concerning public disclosure set forth in 15 U.S.C. 46(f) and 16 CFR 4.10.

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 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 years and commencing one year after the entry date of this Order, and each year thereafter, provide the Commission 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 Commission; (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 Commission representative in writing, submit all annual certifications to the Commission pursuant to this Order via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue N.W., Washington, D.C. 20580. The subject line must begin, "Federal Trade Commission v. Equifax Inc., FTC File No. 1723203."

VI. COVERED INCIDENT REPORTS

IT IS FURTHER ORDERED that for twenty 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 Commission.

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 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, a report summarizing all Covered Incidents that occurred in that calendar quarter.

C. Unless otherwise directed by a Commission representative in writing, all Covered Incident reports to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue N.W., Washington, D.C. 20580. The subject line must begin, "Federal Trade Commission v. Equifax Inc., File No. 172 3203." Defendant must notify the Commission 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 Commission's procedures concerning public disclosure set forth in 15 U.S.C. § 46(f) and 16 CFR Part 4.10.

VII. MONETARY JUDGMENT AND ADDITIONAL MONETARY OBLIGATIONS

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 Commission against Defendant.

B. This order imposes additional financial obligations ("Additional Financial Obligations") on Defendant for the purpose of monetary relief for Affected Consumers. If more than seven million Affected Consumers enroll in the

Product, then Defendant's Additional Financial Obligations will be calculated using the following formulas:

1. If, at the end of the Initial Claims Period, more than seven million Affected Consumers enroll in the Product, then:
    a. If the total payments for Alternative Reimbursement Compensation, Out-of-Pocket Losses, Assisted Identity Restoration Services, Notice and Settlement Administration Costs and Expenses, Service Awards, and the cost of providing the Product to seven 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 the Commission an amount equal to the cost of providing the Product to enrollees above seven million (the "Additional Credit Monitoring Cost");
    b. If the Costs are less than Two Hundred Fifty-Six Million Five Hundred Thousand Dollars ($256,500,000) and the Additional Credit Monitoring Cost is greater than Forty-Three Million Five Hundred Thousand Dollars ($43,500,000), Equifax Inc., its successors and assigns, shall pay the Commission an amount

equal to the Additional Credit Monitoring Cost less Forty-Three Million Five Hundred Thousand Dollars ($43,500,000); or

c. If (i) the Costs are greater than or equal to Two Hundred Fifty-Six Million Five Hundred Thousand Dollars ($256,500,000) but less than Three Hundred Million Dollars ($300,000,000) and (ii) the Costs plus the Additional Credit Monitoring Costs are greater than Three Hundred Million Dollars ($300,000,000), Equifax Inc., its successors and assigns, shall pay the Commission an amount equal to the Costs plus Additional Credit Monitoring Costs less Three Hundred Million Dollars ($300,000,000); and

2. If, during the Extended Claims Period, more than seven million Affected Consumers have enrolled in the Product and either (i) the Costs are greater than or equal to Two Hundred Fifty-Six Million Five Hundred Thousand Dollars ($256,500,000)or (ii) the Additional Credit Monitoring Costs are greater than or equal to Forty-Three Million Five Hundred Thousand Dollars ($43,500,000) then, on a monthly basis, Equifax Inc., its successors and assigns, shall deposit any additional money to the Commission that would be required

pursuant to the calculations in Section VII.B.1.a-c, less any amounts previously deposited as the Additional Financial Obligations.

VIII. CONSUMER RESTITUTION AND REDRESS THROUGH MULTI-DISTRICT LITIGATION

IT IS FURTHER ORDERED that consumer relief that would otherwise be conducted by the Commission using the monetary relief in Section VII may be instead conducted through final resolution of the Multi-District Litigation consistent with Sections VIII, IX, and X of this Order, beginning with filing an executed Settlement agreement and motion for entry of an order permitting issuance of notice of the Settlement containing each of the following components:

A. Equifax Inc., its successors and assigns, shall deposit Three Hundred Million Dollars ($300,000,000) (the "Payment") into the Consumer Fund as follows: (i) One Hundred Fifty Thousand Dollars ($150,000) no later than fifteen days after the filing of this Order, to cover reasonable set-up costs of the Notice Provider; (ii) Twenty-Five Million Dollars ($25,000,000) no later than fifteen days after the MDL Court enters an order permitting issuance of notice of the Settlement, to cover reasonable costs and expenses of the Settlement Administrator and Notice Provider and set-up costs for the independent third-party provider of the Product and Assisted Identity Restoration Services; and (iii) Three Hundred Million Dollars

($300,000,000) into the Consumer Fund, less any amounts paid pursuant to (i) and (ii), no later than fifteen days after the Class Action Effective Date.

B. If the Consumer Fund lacks sufficient funds to pay claims for Out-of-Pocket Losses made during the Initial and Extended Claims Periods, Equifax Inc., its successors and assigns, deposits into the Consumer Fund, as needed to pay such claims on a monthly basis, up to an additional aggregate amount of One Hundred Twenty-Five Million Dollars ($125,000,000) within fourteen days after receipt of written notification from the Settlement Administrator that there are insufficient funds remaining in the Consumer Fund.

C. Equifax Inc., its successors and assigns, pays any Additional Financial Obligations required under Section VII into the Consumer Fund.

D. Sections IX and X of this Order shall be construed in a manner consistent with the Settlement.

IX. CONSUMER FUND FOR MULTI-DISTRICT LITIGATION

IT IS FURTHER ORDERED that:

A. An amount no less than Three Hundred Million Dollars ($300,000,000), plus any amount deposited in the Consumer Fund pursuant to Sections VIII.B and VIII.C, including all accumulated interest, must be used and administered as described in Section IX for the exclusive purpose of providing restitution and redress to Affected Consumers.

B. Subject to Sections IX.C and IX.D, the Consumer Fund shall be used to pay:

1. After either the Class Action Effective Date or the conclusion of the Initial Claims Period, whichever is later, for claims submitted during the Initial Claims Period:

a. Four years of enrollment in the Product to Affected Consumers, which shall include One Million Dollars ($1,000,000) in identity theft insurance and Full Service Identity Restoration Services.

i. The Product shall be offered, provided and maintained by an independent third party and shall not be provided to any Affected Consumer by Defendant. Defendant shall not receive any monetary benefit from the Product;

ii. 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 days after either the Class Action Effective Date or the conclusion of the Initial Claims Period, whichever is later. Affected Consumers shall be eligible to

enroll in the Product for a period of at least ninety days following receipt of the activation code.

b. Alternative Reimbursement Compensation of up to One Hundred Twenty-Five Dollars ($125);

c. Claims for Out-of-Pocket Losses, including, without limitation, the following:

i. Up to twenty-five percent (25%) reimbursement for costs incurred by an Affected Consumer enrolled in an Equifax credit or identity monitoring subscription product on or after September 7, 2016, through September 7, 2017;

ii. Credit monitoring costs that were incurred by an Affected Consumer on or after September 7, 2017, through the date of the Affected Consumer's claim submission;

iii. Costs incurred on or after September 7, 2017, associated with placing or removing a security freeze on a Consumer Report with any Consumer Reporting Agency;

iv. 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 Affected Consumers' personal information;

v. Other miscellaneous expenses incurred related to any Out-Of-Pocket Loss such as notary, fax, postage, copying, mileage, and long-distance telephone charges; and

vi. Time Compensation for up to twenty hours.

2. For claims submitted during the Extended Claims Period, reimbursement of claims for the following Out-of-Pocket Losses incurred during the Extended Claims Period:

a. 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 Affected Consumers' Personal Information;

b. 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; and

c. Time Compensation 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.

3. For a period of seven years from the Class Action Effective Date, Assisted Identity Restoration Services to an Affected Consumer. Affected Consumers shall not be required to enroll in the Product to obtain Assisted Identity Restoration Services.

    a. The Assisted Identity Restoration Services shall be offered, provided and maintained by the independent third party that has been approved by a representative of the Commission and that will be presented to the MDL Court for its approval. Assisted Identity Restoration Services shall not be provided to any Affected Consumer by Defendant. Defendant shall not receive any monetary benefit from the Assisted Identity Restoration Services.

4. Notice and Settlement Administration Costs and Expenses;

5. Applicable taxes, duties, and similar charges due from the Consumer Fund to the extent that the principal is not reduced; and

6. Service Awards in an aggregate amount not to exceed Two Hundred Fifty Thousand Dollars ($250,000). To the extent the MDL Court approves Service Awards in excess of Two Hundred Fifty Thousand Dollars ($250,000), such amount shall not be paid from the funds

deposited into the Consumer Fund pursuant to this Order and shall be paid solely by the Defendant.

C. Subject to Section IX.D, payments from the Consumer Fund shall be subject to the following limitations:

1. Each Affected Consumer will be eligible to receive a maximum aggregate reimbursement of Twenty Thousand Dollars ($20,000) for Out-of-Pocket Losses.

2. No more than Thirty-One Million Dollars ($31,000,000) shall be used to pay Alternative Reimbursement Compensation (the "Alternative Reimbursement Compensation Cap"). To the extent valid claims for Alternative Reimbursement Compensation exceed the Alternative Reimbursement Compensation Cap, then payments for valid Alternative Reimbursement Compensation claims shall be reduced on a *pro rata* basis.

3. 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 will be reduced on a *pro rata*

basis. Valid claims for Time Compensation made during the Extended Claims Period will 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 (the "Aggregate Time Compensation Cap"). At the conclusion of the Extended Claims Period, and following payment of valid claims made during the Extended Claims Period, Time Compensation claims may be subject to Section IX.D, if applicable, in which case all valid Time Compensation claims will be paid at the same *pro rata* rate.

D. If amounts remain in the Consumer Fund at the conclusion of the Extended Claims Period, the remaining funds shall be distributed to provide restitution and redress as follows:

1. First, the Aggregate Time Compensation Cap and Alternative Reimbursement Compensation Cap shall both be lifted (if applicable) and payments increased *pro rata* to Affected Consumers with valid claims up to the full amount of those claims; then,

2. Second, to provide Assisted Identity Restoration Services to all Affected Consumers for up to an additional thirty-six months; 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.

X. NOTICE AND CLAIMS IN MULTI-DISTRICT LITIGATION

IT IS FURTHER ORDERED, if Defendant elects to deposit money in the Consumer Fund:

A. Defendant shall supply the Notice Provider with information in its possession, custody, or control, to the extent reasonably available, regarding Affected Consumers sufficient to enable the Notice Provider to implement the Notice Plan.

B. Defendant shall supply the Settlement Administrator with information in its possession, custody, or control, to the extent reasonably available, regarding Affected Consumers sufficient to enable the Settlement Administrator to implement the Claims Administration Protocol. This shall include providing the Settlement Administrator with sufficient information to identify consumers who are eligible for reimbursement pursuant to IX.B.1.c.i, as those consumers are not required to submit supporting documentation for this type of Out-of-Pocket Loss.

C. Defendant must notify a designated representative of the Commission 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 Commission, 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 Commission may send a request for information regarding compliance with Sections VII – X of this Order to the Notice Provider and/or Settlement Administrator, and any request will include all parties to the Settlement and the Bureau. Discussion and fulfillment of responses to a request from the Commission shall be made consistent with the Claims Administration Protocol;
2. Defendant shall provide to the Commission the weekly reports prepared by the Settlement Administrator pursuant to the Multi-District Litigation that summarize information related to the claims administration; and

3. Defendant shall provide to the Commission copies of any information requested by and submitted to the Bureau.

Any information submitted to the Commission pursuant to this Section shall be treated as confidential until the Class Action Effective Date.

E. From the beginning of the Initial Claims Period until the Consumer Fund is exhausted, Defendant shall provide a representative of the Commission, on an annual basis, with the following information for the prior year:

1. A summary by month of the total number of claims submitted to the Settlement Administrator, the total dollar amount of claims submitted to the Settlement Administrator, the total number of claims paid by the Settlement Administrator, the total amount of claims paid by the Settlement Administrator, and the total amount of claim payments negotiated.
2. Regarding the Product and Assisted Identity Restoration Services outlined in Exhibit A, the following information:
    a. The number of Affected Consumers who enrolled in the Product;
    b. The number and total dollar amount of claims filed by Affected Consumers under the identity theft insurance provided pursuant to the Product and what percentage of those claims were paid;

c. The number of Affected Consumers who availed themselves of Full Service Identity Restoration Services in the year preceding the publication of the annual report; and

d. The number of Affected Consumers who availed themselves of Assisted Identity Restoration Services in the year preceding the publication of the annual report.

3. Information regarding notice, including the number of viewers who opened emails sent pursuant to the Notice Plan, the number of unique visitors to the Settlement Website, and the number of unique visitors who arrived from a hyperlink to the Settlement Website posted on or in each of the following:

a. www.equifax.com;

b. www.equifaxsecurity2017.com;

c. Defendant's Twitter notifications referenced in Section XV.A.4;

d. Defendant's Facebook notifications referenced in Section XV.A.5; and

e. The emails sent pursuant to the Notice Plan.

4. Regarding consumer complaints:

a. The number of unique consumer complaints received by the Settlement Administrator or the third party providing the Product regarding:

i. Access to the Settlement Website;

ii. Enrollment in the Product;

iii. Any of the Product components, including identity theft insurance;

iv. Any other consumer rights to obtain relief under this Order; or

v. Identity theft; and

b. Defendant shall develop and implement a process to direct consumers that contact Defendant with issues related to the Settlement or the Consumer Fund to the Settlement Administrator and/or the Settlement Website.

5. The reporting period must cover: (1) the first year after the entry date of the order permitting issuance of notice of the Settlement; and (2) each year thereafter until the Consumer Fund has been exhausted.

6. This information must be submitted to the Commission within sixty days after the reporting period has been completed via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service)

to Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue N.W., Washington, D.C. 20580. The subject line must begin, "Federal Trade Commission v. Equifax Inc., FTC File No. 1723203."

7. Defendant shall transmit the information required pursuant to Section X.D without alteration and shall disclose any fact material to the information submitted. No information may be withheld 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 the Settlement Administrator, although such documents can be designated for confidential treatment in accordance with applicable law.
8. The information described in Section X.D shall be treated as confidential until the Class Action Effective Date. Defendant shall not object to publication of this information by the Commission, to the extent that such publication occurs after the Class Action Effective Date.

XI. REVERSION OF CONSUMER RELIEF TO ADMINISTRATION BY COMMISSION

IT IS FURTHER ORDERED that the Commission may end its forbearance of the collection of the judgment and use the procedures set forth in this Section,

rather than through the Multi-District Litigation in Section VIII, and receive Defendant's payments directly as follows:

A. The forbearance will terminate upon written notice to Defendant upon the occurrence of one or more Termination Events. If any of the following Termination Events should occur, a representative of the Commission and the Bureau may, in their sole discretion, jointly send Defendant a written notice of a Termination Event:

   1. An executed Settlement agreement, and a motion for an order permitting issuance of notice of the Settlement, containing terms materially similar to those outlined in Sections VIII, IX, X, and XIII and Exhibit A of this Order, are not submitted to the MDL Court within fourteen days after the filing of this proposed Order, provided however that the Defendant, Commission, or the Bureau are not the cause of such failure;
   2. The MDL Court declines to enter an order permitting issuance of notice of the Settlement and either (i) a modified Settlement agreement is not submitted to the MDL Court within sixty days or (ii) a modified Settlement agreement is submitted to the MDL Court without Defendant first obtaining written approval from a representative of the Commission;

3. The MDL Court enters a final approval of a Settlement agreement in the Multi-District Litigation with terms that are materially different from the terms in Sections VIII-X and Exhibit A of this Order and Defendant has not obtained written approval from a representative of the Commission;
4. The MDL Court declines to enter a final approval of a Settlement agreement in the Multi-District Litigation with terms materially similar to those outlined in Sections VIII, IX, X, and XIII and Exhibit B of this Order and (i) a modified Settlement agreement is not submitted to the MDL Court within sixty days, or (ii) a modified Settlement agreement is submitted to the MDL Court without Defendant first obtaining written approval from a representative of the Commission;
5. The MDL Court's Final Approval Order is overturned on appeal and either (i) a modified Settlement agreement in the Multi-District Litigation is not submitted to the MDL Court within sixty days or (ii) a modified Settlement agreement in the Multi-District Litigation is submitted to the MDL Court without Defendant first obtaining approval from a representative of the Commission;

6. The MDL Court approves a Settlement agreement or modified Settlement agreement, other than one approved by the Commission, resolving the Multi-District Litigation that interferes in any way with the Commission's ability to enforce this Order; or
7. If at any time the Settlement is terminated by any party to the Multi-District Litigation.

Where approval is required by a representative of the Commission, such approval shall not be unreasonably withheld (e.g., if the proposed modification is no less favorable to Affected Consumers than the terms of this Order) and shall be timely provided.

B. If an event described in Sections XI.B.2 – 6 results from an objection from the Commission, Bureau, or the States' Attorneys General in the MDL Court to either (i) the Settlement or (ii) a modified Settlement agreement in the Multi-District Litigation, and such Settlement or modified Settlement agreement contains terms that are materially similar to Sections VIII, IX, X, and XIII and Exhibit A, such event shall not constitute a Termination Event.

C. If the Commission and the Bureau jointly send Defendant a written notice of a Termination Event, Section XI of this Order will not be construed in a way that interferes with the Multi-District Litigation.

D. If the forbearance ends, within twenty-one days of receipt of written notice of a Termination Event, Equifax Inc., its successors and assigns, is ordered to pay the following amounts, plus any interest accumulated, less any payments that have already been disbursed by the Settlement Administrator from the Consumer Fund; Defendant is not entitled to any offset or other deduction unless a representative of the Commission agrees in writing in advance:

1. Three Hundred Million Dollars ($300,000,000), plus any interest accumulated, less any payments that have already been disbursed by the Settlement Administrator from the Consumer Fund;
2. If the funds paid pursuant to Section XI.D.1 are insufficient to pay claims for Out-of-Pocket Losses made during the Initial and Extended Claims Periods, and subject to the monetary limits, if applicable, set forth in Sections IX.B, IX.C and IX.D, Equifax Inc., its successors and assigns, shall make additional payments of up to One Hundred Twenty-Five Million Dollars ($125,000,000) in the aggregate as needed on a monthly basis within fourteen days after receipt of written notification from a representative of the Commission that there are insufficient funds remaining; and

3. Additional Financial Obligations, subject to the monetary limits, if applicable, set forth in Section IX.B, IX.C and IX.D, pursuant to Section VII.B.

E. All payments to the Commission must be made by electronic fund transfer in accordance with instructions provided by a representative of the Commission.

F. The Notice Provider and Settlement Administrator's acceptance of funds shall constitute the Notice Provider and Settlement Administrator's agreement to consent to the jurisdiction of this Court.

G. In addition to payment, Defendant remains obligated to cooperate in the administration of consumer relief. If a representative of the Commission requests in writing any information related to consumer relief, Defendant must provide it, in the form prescribed by the Commission, within fourteen days. Defendant shall provide the Commission with:

1. Sufficient information to enable the Commission to efficiently administer consumer relief.

2. Sufficient information regarding any steps toward consumer notice, claims, and relief that has been provided pursuant to the Consumer Fund by the Notice Provider or the Settlement Administrator to enable the Commission to efficiently administer consumer relief.

H. The Commission may, at its sole discretion, continue to work with the Notice Provider and Settlement Administrator on behalf of itself, the Bureau, and the States' Attorneys General.

1. Whether the Commission elects to continue to retain them, the Notice Provider and the Settlement Administrator shall provide the Commission with sufficient information regarding any steps toward consumer notice, claims, and relief that has been provided pursuant to the Consumer Fund to enable the Commission to efficiently administer consumer relief.

2. If a representative of the Commission requests in writing any information related to consumer relief, Defendant shall require the Notice Provider and the Settlement Administrator to provide it, to the extent reasonably available, in the form prescribed by the Commission, within fourteen days.

I. All other provisions of this Order shall remain in full force and effect.

XII. ADDITIONAL MONETARY PROVISIONS

IT IS FURTHER ORDERED that:

A. 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.

B. 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 Commission 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.

C. The facts alleged in the Complaint establish all elements necessary to sustain an action by the Commission 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.

D. Defendant acknowledges that its Taxpayer Identification Number, which Defendant must submit to the Commission, may be used for collecting and reporting on any delinquent amount arising out of this Order, in accordance with 31 U.S.C. § 7701.

E. All money paid to the Commission shall be deposited into a fund administered by the Commission or its designee to be used for consumer relief, on behalf of the Commission, the Bureau, and States' Attorneys General, including the types of consumer relief enumerated in Section IX (such as enrollment in a credit monitoring product, out-of-pocket losses, time compensation, miscellaneous expenses, and identity theft restoration services), and any attendant expenses for the administration of any fund. If a

representative of the Commission decides that direct redress to consumers is wholly or partially impracticable or money remains after consumer relief is completed under this subsection, the Commission may apply any remaining money for such other consumer relief (including consumer information remedies) as it determines to be reasonably related to Defendant's practices alleged in the Complaint. Any money not used for such consumer relief is to be deposited to the U.S. Treasury as disgorgement. All processes and protocols for the effective and efficient administration of the consumer relief are within the sole discretion of the Commission or its representatives and Defendant has no right to challenge any actions the Commission or its representatives may take pursuant to Section XII.E.

XIII. SINGLE-BUREAU MONITORING AND IDENTITY THEFT PROTECTION

IT IS FURTHER ORDERED that Defendant shall:

A. Offer a single-bureau monitoring service with the features described in Exhibit A ("Single-Bureau Monitoring) that has been approved by a representative of the Commission, to Affected Consumers who file a valid claim for Single-Bureau Monitoring and who enroll in the Product. Such Affected Consumers may enroll in the Single-Bureau Monitoring upon expiration of the Product, including any extensions thereof pursuant to Section IX, such that the aggregate number of years of credit monitoring

provided under Section IX and the Single-Bureau Monitoring equals ten years, except as described in Subsection XIII.B, below.

B. Offer Affected Consumers who were under the age of eighteen on May 13, 2017, additional years of Single-Bureau Monitoring such that the aggregate number of years of credit monitoring provided under Section IX and the Single-Bureau Monitoring equals eighteen years. If an Affected Consumer who enrolled in the Product is under the age of eighteen when the Product expires, the Single-Bureau Monitoring offered will be child monitoring services until such Affected Consumer reaches eighteen years of age.

C. Provide all Affected Consumers with an easily accessible process to place or remove security freezes or locks on their Personal Consumer Report for free for a period of ten years following the date of entry of this Order. Defendant shall not 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 (e.g., Lock & Alert), Defendant shall not seek to persuade Affected Consumers to choose the alternative product or service instead of a security freeze.

D. Separate and apart from any statutory or other legal requirements, for a period of seven years starting December 31, 2019, provide to all U.S.

consumers a clearly accessible process to obtain six free copies during any twelve-month period of their Personal Consumer Report.

XIV. PROHIBITION ON ADVERTISING OR MARKETING TO CONSUMERS WHO USE IDENTITY THEFT PROTECTION SERVICES

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, shall not use any information provided by an Affected Consumer to enroll in or to use the products and services set forth in Sections IX, XIII.D, and Exhibit A, including the Product, Full Service Identity Restoration Services, Assisted Identity Restoration Services, and the Single-Bureau Credit Monitoring, or the free credit monitoring products (Equifax TrustedID Premier, Equifax Credit Watch Gold with 3 in 1 Monitoring, or Experian IDNotify) offered or paid by Defendant in connection with the Breach (or the fact that the consumer provided such information), to sell, upsell, cross-sell, or directly market or advertise its products or services unless Defendant:

A. Makes a Clear and Conspicuous disclosure, separate and apart from any "End User License Agreement," "Privacy Policy," "Terms of Use" page, describing how Defendant will use the Affected Consumer's information; and

B. Obtains and documents the Affected Consumer's affirmative express consent.

XV. ADDITIONAL NOTICE

IT IS FURTHER ORDERED that Defendant shall provide the following notices:

A. To Affected Consumers within seven days of entry of an order permitting issuance of notice of the Settlement, or the Commission notifying Defendant that it is exercising its rights under a Termination Event, whichever is earlier:

1. Posting a Clear and Conspicuous hyperlink to the Settlement Website on the top portion of the landing page for Defendant's primary, consumer-facing website, www.equifax.com, which shall state "Visit [hyperlink to the Settlement Website] for information on the Equifax Data Breach Settlement" or "Equifax Data Breach Settlement," which shall remain posted until the expiration of the Initial Claims Period;
2. Posting a Clear and Conspicuous hyperlink to the Settlement Website on the top portion for the landing page for Defendant's www.equifaxsecurity2017.com website, which shall state "Visit [hyperlink to the Settlement Website] for information on the Equifax Data Breach Settlement" or "Equifax Data Breach Settlement," which

shall remain posted until the expiration of the Extended Claims Period;

3. Issuing a press release, using terms consistent with the approved Notice Plan, including a hyperlink to the Settlement Website, with information about the Product, the Consumer Fund, and the Settlement Website;
4. Sending a Twitter notification via Defendant's primary Twitter account monthly during the Initial Claims Period and then biannually during the Extended Claims Period, the text of which shall read "Visit [hyperlink to the Settlement Website] for information on the Equifax Data Breach Settlement"; and
5. Posting a Facebook notification via Defendant's primary account monthly during the Initial Claims Period and then biannually during the Extended Claims Period, the text of which shall read "Visit [hyperlink to the Settlement website] for information on the Equifax Data Breach Settlement."

B. To U.S. consumers, issuing a press release seven days after the relief described in Section XIII.D 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.

XVI. RULE VIOLATIONS

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 product or service, are hereby permanently restrained and enjoined from violating any provision of the Standards for Safeguarding Consumer Information Rule, 16 C.F.R. Part 314, a copy of which is attached hereto as Exhibit B.

XVII. ORDER ACKNOWLEDGMENTS

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

A. Defendant, within seven days of entry of this Order, must submit to the Commission an acknowledgment of receipt of this Order sworn under penalty of perjury.

B. For ten years after entry of this Order, Defendant must deliver a copy of this Order to: (a) all principals, officers, directors, and LLC managers and members; (b) all employees, agents, and representatives having managerial or supervisory responsibilities for conduct related to the subject matter of the

Order; and (c) any business entity resulting from any change in structure as set forth in the Section titled Compliance Reporting; and

C. Delivery must occur within 7 days of entry of this Order for current personnel. For all others, delivery must occur before they assume their responsibilities.

D. 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, which can be obtained electronically.

XVIII. COMPLIANCE REPORTING

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

A. 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 Commission 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, including the types of 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 Commission.

B. For 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.

C. Defendant must submit to the Commission notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against the Defendant within 14 days of its filing.

D. Any submission to the Commission 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.

E. Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin "Federal Trade Commission v. Equifax Inc., FTC File No. 1723203."

XIX. RECORDKEEPING

IT IS FURTHER ORDERED that Defendant must create certain records for 20 years after entry of the Order, and retain each such record for 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 or 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. 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;

E. 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;

F. For five years after the date of preparation of each Assessment required by this Order, all materials and evidence that are in the 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

G. All records necessary to demonstrate full compliance with each provision of this Order; including all submissions to the Commission.

XX. COMPLIANCE MONITORING

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

A. Within 14 days of receipt of a written request from a representative of the Commission, Defendant must: submit additional compliance reports or other requested information, which must be sworn under penalty of perjury; appear for depositions; and produce documents for inspection and copying. The Commission 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 Commission is authorized to communicate directly with Defendant. Defendant must permit representatives of the Commission 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 Commission 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

Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

XXI. 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.

XXII. RETENTION OF JURISDICTION

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

SO ORDERED this 23 day of July, 2019.

Thomas W. Thrash

United States District Judge

FOR PLAINTIFF FEDERAL TRADE COMMISSION:

/s/ Jacqueline K. Connor

JACQUELINE K. CONNOR
TIFFANY GEORGE
CATHLIN TULLY
Federal Trade Commission
600 Pennsylvania Ave. N.W.,
CC-8232
Washington, D.C. 20580
Telephone: (202) 326-2844
Facsimile: (202) 656-3062
E-mail(s): jconnor@ftc.gov
tgeorge@ftc.gov
ctully@ftc.gov

ANNA M. BURNS
GA Bar No. 558234
Federal Trade Commission
Southeast Region
225 Peachtree Street, N.E., Suite 1500
Atlanta, GA 30303
Telephone: (404) 656-1350
Facsimile: (404) 656-1379
E-mail: aburns@ftc.gov

Date: 07/19/2019

FOR DEFENDANT EQUIFAX INC:

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

Date: 7/19/19

EDITH RAMIREZ
HARRIET PEARSON
MICHELLE KISLOFF
TIMOTHY TOBIN
Hogan Lovells US LLP
555 Thirteenth Street, NW
Washington, DC 20024
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.

(ii) If it shares with nonaffiliated third parties, state, as applicable: ''*Nonaffiliates we share with can include [list categories of companies such as mortgage companies, insurance companies, direct marketing companies, and nonprofit organizations].*''

(3) *Joint Marketing.* As required by §313.13 of this part, where [*joint marketing*] appears, the financial institution must:

(i) If it does not engage in joint marketing, state: ''*[name of financial institution] doesn't jointly market*''; or

(ii) If it shares personal information for joint marketing, state, as applicable: ''*Our joint marketing partners include [list categories of companies such as credit card companies].*''

(c) *General instructions for the ''Other important information'' box.* This box is optional. The space provided for information in this box is not limited. Only the following types of information can appear in this box.

(1) State and/or international privacy law information; and/or

(2) Acknowledgment of receipt form.

[74 FR 62966, Dec. 1, 2009]

PART 314—STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

Sec.

AUTHORITY: 15 U.S.C. 6801(b), 6805(b)(2).

SOURCE: 67 FR 36493, May 23, 2002, unless otherwise noted.

§ 314.1 Purpose and scope.

(a) *Purpose.* This part, which implements sections 501 and 505(b)(2) of the Gramm-Leach-Bliley Act, sets forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.

(b) *Scope.* This part applies to the handling of customer information by all financial institutions over which the Federal Trade Commission (''FTC'' or ''Commission'') has jurisdiction. This part refers to such entities as ''you.'' This part applies to all customer information in your possession, regardless of whether such information pertains to individuals with whom you have a customer relationship, or pertains to the customers of other financial institutions that have provided such information to you.

§ 314.2 Definitions.

(a) *In general.* Except as modified by this part or unless the context otherwise requires, the terms used in this part have the same meaning as set forth in the Commission's rule governing the Privacy of Consumer Financial Information, 16 CFR part 313.

(b) *Customer information* means any record containing nonpublic personal information as defined in 16 CFR 313.3(n), about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates.

(c) *Information security program* means the administrative, technical, or physical safeguards you use to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.

(d) *Service provider* means any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a financial institution that is subject to this part.

§ 314.3 Standards for safeguarding customer information.

(a) *Information security program.* You shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue. Such safeguards shall include the elements set forth in §314.4 and shall be reasonably designed to achieve the objectives of this part, as set forth in paragraph (b) of this section.

(b) *Objectives.* The objectives of section 501(b) of the Act, and of this part, are to:

(1) Insure the security and confidentiality of customer information;

EXHIBIT B

(2) Protect against any anticipated threats or hazards to the security or integrity of such information; and

(3) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

§ 314.4 Elements.

In order to develop, implement, and maintain your information security program, you shall:

(a) Designate an employee or employees to coordinate your information security program.

(b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:

(1) Employee training and management;

(2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and

(3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.

(c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

(d) Oversee service providers, by:

(1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and

(2) Requiring your service providers by contract to implement and maintain such safeguards.

(e) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.

§ 314.5 Effective date.

(a) Each financial institution subject to the Commission's jurisdiction must implement an information security program pursuant to this part no later than May 23, 2003.

(b) Two-year grandfathering of service contracts. Until May 24, 2004, a contract you have entered into with a nonaffiliated third party to perform services for you or functions on your behalf satisfies the provisions of §314.4(d), even if the contract does not include a requirement that the service provider maintain appropriate safeguards, as long as you entered into the contract not later than June 24, 2002.

PART 315—CONTACT LENS RULE

AUTHORITY: Pub. L. 108–164, secs. 1–12; 117 Stat. 2024 (15 U.S.C. 7601–7610).

SOURCE: 69 FR 40508, July 2, 2004, unless otherwise noted.

§ 315.1 Scope of regulations in this part.

This part, which shall be called the ''Contact Lens Rule,'' implements the Fairness to Contact Lens Consumers Act, codified at 15 U.S.C. 7601–7610, which requires that rules be issued to address the release, verification, and sale of contact lens prescriptions. This part specifically governs contact lens prescriptions and related issues. Part 456 of Title 16 governs the availability of eyeglass prescriptions and related issues (the Ophthalmic Practice Rules (Eyeglass Rule)).