NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES

In the Matter of

EQUIFAX INC., EQUIFAX INFORMATION SERVICES, LLC, and EQUIFAX CONSUMER SERVICES, LLC,

Respondents.

CONSENT ORDER

WHEREAS, pursuant to § 404 of the Financial Services Law ("FSL"), the Consumer Protection and Financial Enforcement Division of the New York State Department of Financial Services (the "Department") investigated whether Equifax Inc., Equifax Information Services, LLC, and Equifax Consumer Services, LLC (collectively, "Respondents") were complying with the requirements of the FSL and the Consumer Financial Protection Act of 2010, 12 U.S.C. § 5481 *et seq.* (the "CFPA"), in collecting, maintaining, and selling consumers' sensitive personal and financial information in connection with offering and providing consumer financial products and services (the "Investigation"); and

WHEREAS, the Department investigated Respondents' 2017 data breach and their security practices prior to and at the time of the breach, as well as their communications and the services provided to consumers after announcement of the 2017 data breach (the "Relevant Period"); and

WHEREAS, the Department and Respondents are willing to resolve the matters cited herein in lieu of proceeding by notice and hearing;

NOW, THEREFORE, this Consent Order (the "Consent Order") contains the Department's findings and the relief agreed to by the Department and Respondents.

FINDINGS

The findings of the Department's Investigation are as follows:

Overview of the Respondents

1. Respondent Equifax Inc. is a global data, analytics, and technology company that was founded and is headquartered in Atlanta, Georgia. Equifax Inc. is a "covered person" as that term is defined in the CFPA, 12 U.S.C. § 5481(6). Equifax Inc., through its subsidiaries and affiliates, offers or provides a "financial product or service" within the meaning of the FSL, and is registered with the New York Department of State to do business within New York State.

2. Respondent Equifax Information Services, LLC ("EIS") is a Georgia limited liability company, is one of the three primary national consumer reporting agencies in the United States, and engages in the business of collecting, analyzing, maintaining, and providing consumer report information. EIS is a "covered person" as that term is defined in the CFPA, 12 U.S.C. § 5481(6), offers and provides a "financial product or service" to New York consumers within the meaning of the FSL, FSL § 104(a)(2), is registered with the New York Department of State to do business within New York State, and is registered with the Department as a credit reporting agency.

3. Respondent Equifax Consumers Services, LLC ("ECS") is a Georgia limited liability company that sells or provides, among other things, credit monitoring and identity protection products and services to consumers. ECS also is a "covered person" as that term is defined in the CFPA, 12 U.S.C. § 5481(6), and offers and provides a "financial product or service" to New York consumers within the meaning of the FSL. FSL § 104(a)(2).

4. EIS and ECS are subsidiaries of Equifax Inc.

Respondents' Business Activities

5. Collectively, Respondents' businesses involve collecting, maintaining, and analyzing the sensitive personal and financial information of individual consumers and businesses. Respondents, together with their various affiliates and subsidiaries, have collected and maintain data regarding more than 91 million businesses and 820 million people worldwide, including millions of New York consumers.

6. Collectively, Respondents maintain a variety of sensitive data, including full Social Security numbers, current and former residential addresses, dates of birth, names of employers, bankruptcies filed by consumers, and detailed information on consumers' financial accounts including balances owed, credit extended, and payment history. EIS may use some of this information to generate credit reports and credit scores and provide those reports and scores to third parties.

7. Financial services companies, including many institutions the Department regulates, rely on EIS's credit report information to make decisions that impact important financial transactions in consumers' lives, including purchasing a home and financing an education.

8. Collectively, Respondents' business model relies on the ability to collect consumer information from consumers and businesses at a low cost, and to use that consumer information to create credit reports, which Respondents sell to entities that offer financial products and services to consumers. To maintain their business model, and the public's trust, Respondents made numerous statements, both expressly and implicitly representing that they were taking appropriate steps to protect data security.

Respondents' Inadequate Information Security Practices

9. During the Relevant Period, Respondents' information security program failed in certain respects to safeguard certain sensitive consumer information.

10. Among the deficiencies in the security program, Respondents failed initially to detect a critical vulnerability affecting the online consumer dispute portal that consumers use to dispute the completeness or accuracy of information in their credit files (the "Dispute Application"). That vulnerability related to Apache Struts, an open-source web application framework that Respondents used in connection with the Dispute Application.

11. Respondents should have been fully aware that the Dispute Application utilized Apache Struts.

12. Between March 7 and 10, 2017, Apache Software Foundation ("Apache"), the non-profit organization that provides Apache Struts to the public, and the federal government warned of a new security vulnerability in Apache Struts version 2.x, assigned the CVE identifier CVE-2017-5638 (the "Struts Vulnerability").

13. On March 7, 2017, Apache published two security bulletins on its website that described the Struts Vulnerability and rated it as "critical." Certain versions of Apache Struts were vulnerable to "Remote Code Execution," a method of hacking whereby an attacker can use code to infiltrate and run commands on a website's server. Apache recommended that Apache Struts users patch the Struts Vulnerability by upgrading to a newer version of Apache Struts or implementing a workaround.

14. On March 8, 2017, the United States Computer Emergency Readiness Team of the United States Department of Homeland Security issued a notice by email to entities,

including Respondents, warning that a remote attacker could exploit the Struts Vulnerability to take control of an affected system. Within 24 hours of receiving that notice, Respondents pushed out an internal alert to over 400 system and application owners, highlighting that the Struts Vulnerability was a critical risk and required patching within 48 hours under Equifax Inc.'s security policy. Respondents' Security team discussed the Struts Vulnerability at its weekly meeting following the US-CERT alert and at the March 2017 Global Threat Vulnerability Management monthly meeting. However, Security was not aware of the fact that the Dispute Portal used Apache Struts, was vulnerable to the Struts Vulnerability, or was in need of patching, and therefore the Struts Vulnerability was not discussed in the initial alert, at the Security team's weekly meeting, or at the March 2017 Global Threat Vulnerability Management monthly meeting.

15. On or about March 10, 2017, the United States Department of Commerce's National Institute of Standards and Technology ("NIST") advised that the severity of the Struts Vulnerability was an overall score of 10.0 on two different versions of a scale called the Common Vulnerability Scoring System, the highest possible severity score on either scale. The NIST notice also stated that an attack based on the Struts Vulnerability "[a]llows unauthorized disclosure of information," would be low in complexity to accomplish, and would not require the attacker to provide authentication (for example, a user name and password).

16. Respondents' Intel Collections team found proof-of-concept exploit code online and shared it with Respondents' Countermeasures team, who then created a Sourcefire IPS rule to detect and block attempts to exploit the Struts Vulnerability. That IPS rule was in effect by March 14, 2017.

17. In March 2017, several financial institution customers contacted Respondents to inquire whether Respondents' systems were impacted by the vulnerability, and if so, the steps being taken to address the vulnerability.

18. On or about March 15, 2017, Respondents completed an initial series of scans of their systems for the Struts Vulnerability. However, Respondents failed to identify the Struts Vulnerability on the Dispute Application.

19. Between May 13, 2017 and July 30, 2017, at least two unique criminal attackers exploited the Struts Vulnerability and gained unauthorized access to Respondents' computer system via the Dispute Application and accessed files that contained credentials (username and password). Moreover, because Respondents stored certain user credentials in clear, unencrypted text, and Respondents did not appropriately limit certain points of access between and among databases, the attackers were able to perform queries that provided access to more than 40 databases or database tables that stored consumers' sensitive information. During this period, the attackers exfiltrated the information of at least 145.5 million consumers, including more than 8.4 million New Yorkers (the "Data Breach").

20. The condition of certain aspects of Respondents' information security program contributed to the effects of the Data Breach. Among other things, Respondents had:

    a. an unpatched vulnerability that was not detected by Respondents' scanners and not patched;
    b. inadequate database segmentation;
    c. an expired certificate; and
    d. inadequate access management control.

21. The Data Breach exposed New York consumers' sensitive personal information, including full names, Social Security numbers, dates of birth, addresses, and for some

consumers, credit card numbers, driver's license numbers, and dispute documents containing personally identifying information ("PII"), and thus could have the potential to cause injury, including financial injury, to consumers and businesses.

22. Consumers could not have known the condition of Respondents' information security program. Moreover, consumers whose sensitive personal information was provided to Respondents by third parties or collected by Respondents from sources other than the consumers themselves could not have reasonably avoided Respondents from collecting such information, and consumers could not have demanded that Respondents remove their sensitive information from Respondents' systems.

Respondents' Awareness of the Condition of their Information Security Program

23. During the Relevant Period, Respondents conducted internal and external reviews of the information security program that identified areas for improvement. In addition, during the Relevant Period, Respondents failed to timely implement some security measures that were mandated by their own policies.

A. Inadequate Vulnerability Scanning and Patching

24. In 2016, Respondents' Vulnerability Assessment Team was aware that it did not have complete visibility into where the vulnerable version of Struts was used. This is the same lack of visibility that Respondents had a year later, into exposure to the Struts Vulnerability.

25. In addition, an internal audit and other review noted areas for improvement regarding Respondents' vulnerability scanning and patch management process.

B. Failure to Secure Certain User Credentials

26. Respondents' own policies purported to prohibit the storing of passwords and PINS

unencrypted in batch files, log-in scripts, application programs, programmable function keys, executables, macros or in other locations where unauthorized persons might discover them; and required that computer files that contain passwords or PINs must be secured in a manner than prevents access or copying by unauthorized persons, and password files must be stored separately from application system data.

27. In violation of their own policies, in certain instances, Respondents stored unencrypted user credentials in source code and configuration files.

C. Storage of PII in Development and Testing Environments

28. Respondents' internal documents demonstrate that Respondents were aware that they were storing PII in development and testing environments, increasing the risk of identity theft, misuse of data, and fraud.

D. Deficiencies in Monitoring the Network to Detect or Prevent Unauthorized Access

29. Respondents' internal documents demonstrate deficiencies in the monitoring of certain systems for unauthorized access and exportation of data.

E. Failure to Encrypt Certain Consumers' PII

30. Respondents' internal documents demonstrate that they did not encrypt certain data at rest. Respondents created a policy that was ostensibly effective as of May 2015, that required Respondents to encrypt consumers' PII and payment card information when this information was stored at rest on Respondents' network.

31. An external assessment from November 2016 noted that Respondents were storing sensitive data in unencrypted format in certain data repositories. In 2017—during the Data Breach—Respondents were still maintaining consumer information at rest in unencrypted text in certain data repositories, which violated Respondents' own policies.

32. Respondents also sometimes failed to encrypt data in transit over their internal network.

F. Failure to Consistently Decrypt Certain Network Traffic

33. Respondents at times also failed to decrypt certain incoming and outgoing traffic. Beginning in at least January 2017, Respondents had identified certain deficiencies in its management of secure sockets layer ("SSL") certificates to decrypt incoming and outgoing network traffic.

34. On or about March 14, 2017, Respondents installed an SSL certificate that allowed them to decrypt and inspect encrypted traffic on their TALX website that provides employment verification services to certain customers. This change demonstrates that Respondents understood that employing methods to allow them to decrypt and inspect encrypted traffic to or from external-facing websites was an appropriate and reasonable safeguard.

35. Deficiencies in Respondents' certificate management program contributed to Respondents' inability to timely detect and inspect encrypted traffic to or from hundreds of their websites, including the Dispute Application, and as a result, contributed to the theft of data from their servers.

36. When an updated SSL certificate was installed for the Dispute Application on July 29, 2017, Respondents immediately discovered suspicious outbound traffic from the Dispute Application—i.e., the Data Breach.

G. Respondents' Investments in Data Security Generally

37. Respondents were aware that they needed to continue to invest in data security. In June 2017, Respondents' Chief Security Officer ("CSO") circulated a security growth playbook.

38. In that growth playbook, the CSO assessed Respondents' threat resilience and concluded

that Respondents needed to address gaps in, or expand on, their existing controls by making new foundational investments in the next three years in enterprise logging, authentication and access upgrade, database activity monitoring, encryption at rest, and web application firewall, among other things.

Respondents' Representations Concerning Data Security

39. In connection with maintaining consumer report information and providing credit monitoring and identity theft protection services, Respondents for years have represented directly or indirectly, expressly or by implication, that they had implemented reasonable and appropriate measures to protect personal information against unauthorized access, including by representing that cybersecurity and data security was a top priority and that Respondents had reasonable, physical, technical and procedural safeguards in place for the protection of consumer data.

40. At all times relevant to this Consent Order, Respondents have maintained a publicly available website at www.equifax.com. Each page of Respondents' website includes a hyperlink to Respondents' privacy policies. The hyperlink takes consumers to a web page, www.equifax.com/privacy, that describes Respondents' privacy practices and priorities. Respondents have represented at all relevant times on www.equifax.com/privacy that:

> We have built our reputation on our commitment to deliver reliable information to our customers (both businesses and consumers) and to protect the privacy and confidentiality of personal information about consumers. We also protect the sensitive information we have about businesses. Safeguarding the privacy and security of information, both online and offline, is a top priority for Equifax.

41. Respondents repeat certain representations concerning data security throughout their public website, including in privacy policies for various products. The privacy policy

that applies when consumers use the Dispute Application to dispute the completeness or accuracy of information in their credit files includes a section entitled "Efforts We Make to Safeguard Your Personal Information." At all times relevant to this Consent Order, Equifax Inc. and EIS have represented in this policy that they have "reasonable physical, technical and procedural safeguards to help protect your personal information" and that "in areas that contain your personal information, we use secure socket layer (SSL) encryption to help protect this information while it is in transit between our servers and your computer."

42. From at least October 18, 2013 to April 24, 2017, the "Privacy Policy for Personal Products," which applies to the credit monitoring and identity theft products that Equifax Inc. and ECS sell to consumers, included identical representations.

43. Since at least May 8, 2017, in response to the question "How secure is the information I provide to Equifax.com?" posted in the "FAQ" section of www.equifax.com, Respondents stated, "Equifax understands the importance of keeping your information secure from unauthorized access. All of your data, such as your Social Security number and credit card number(s) are encrypted before being transmitted to/from our servers."

44. Among other deficiencies, Respondents failed to identify a vulnerability for more than four months, and Respondents failed to identify intruders for approximately two and a half months. Moreover, Respondents stored certain user credentials as well as certain consumers' sensitive information in clear unencrypted text, and did not extend their network segmentation sufficiently to limit access from the Dispute Application to certain back end databases.

45. Respondents' representations about the adequacy of Respondents' data- and cyber-

security were inconsistent with these deficiencies.

46. Respondents for years misrepresented, directly or indirectly, expressly or by implication, to consumers that Respondents had implemented reasonable and appropriate measures to protect personal information against unauthorized access, including by representing that cybersecurity and data security was a top priority and that Respondents had reasonable physical, technical and procedural safeguards in place for the protection of consumer data.

Respondents' Conduct After Discovering the Data Breach

47. Respondents' response to consumers following the announcement of the Data Breach on September 7, 2017 failed to provide adequate assistance to affected consumers.

48. On September 7, 2017, Respondents launched a website to provide consumers, including New York consumers, with information about the Data Breach: www.equifaxsecurity2017.com (the "Data Breach Website").

49. However, in September 2017 for a short period of time, Respondents' official Twitter account inadvertently directed consumers to a website set up by a third party, www.securityequifax2017.com, before the Company corrected the error.

50. At all times relevant to this Consent Order, the Data Breach Website has stated that consumer data was "accessed" by attackers, but this description could have led to confusion among the public about whether consumer information was stolen. In reality, consumer information was not only accessed but also exfiltrated.

51. The Data Breach Website includes a page where consumers can input information to determine whether they were victims of the Data Breach. Initially, the Data Breach Website was unable to provide certainty for consumers about whether they were impacted by the Data Breach. Instead of definitively informing consumers whether they

were impacted, Respondents initially advised consumers that their sensitive information may have been compromised.

52. Some consumers who called Respondents concerning the Data Breach—rather than providing their sensitive personal information to Respondents over the Internet—were subjected to inadequate customer service. At times, consumers experienced lengthy hold times or were not able to get through to a live representative at all. Some consumers who did manage to reach a live representative found that the representatives could not provide requested information or could not assist consumers attempting to place a credit freeze. For several days following the Data Breach, Respondents did not provide customer service in languages other than English.

53. Following the Data Breach, Respondents offered to consumers a credit monitoring and identity theft protection product, "TrustedID Premier." From September 7, 2017 to on or around September 17, 2017, consumers were unable to sign up for TrustedID Premier immediately, but instead were provided an enrollment date. The Data Breach Website advised consumers "[b]e sure to write [the enrollment date] down and return to the site on or after that date."

54. Many consumers who returned to the Data Breach Website on or after the specified enrollment date were still unable to enroll and instead were advised that they would receive an email with a link to finalize enrollment and activate the product. The promised email concerning finalization of enrollment in TrustedID Premier was often delayed, sometimes by more than 72 hours.

55. Moreover, some consumers were unable to finalize enrollment in TrustedID Premier. For these consumers, even though they had not yet finalized enrollment in TrustedID Premier, the Data Breach Website stated:

> Product Already Activated
>
> Our records indicate that you may have already enrolled and activated the TrustedID Premier product. Attempting to enroll again is not necessary. Please go to www.TrustedID.com to log in to your product.
>
> If you have any questions, please contact our call center at 877-742-1415.

56. Respondents' actions following the Data Breach did not adequately reassure consumers concerning matters important to them concerning the breach.

57. Respondents also did not adequately inform consumers about the timeframe in which enrollment in TrustedID Premier would occur, leading consumers to believe they would be able to lock their credit files and obtain a credit report within a few days, when that was not true.

58. These representations were material to consumers, including because consumers could not understand if they were victims of the Data Breach or if they needed to take steps to protect the security of their sensitive information.

Violations

59. Based on the foregoing, the Department finds that Respondents engaged in unfair, abusive and deceptive acts and practices in violation of the CFPA, and made inaccurate or misleading representations in violation of Financial Services Law § 408.

AGREEMENT

IT IS HEREBY UNDERSTOOD AND AGREED, by Respondents and the Department that:

Monetary Penalty

60. Equifax Inc. shall pay to the State $10,000,000 in penalties, payable to the Department via electronic transfer in accordance with instructions provided by the Department.

61. Payment of penalties shall be made in full within 30 days of the execution of this Consent Order. Respondents shall not claim, assert, or apply for a tax deduction or tax credit with regard to any U.S. federal, state, or local tax, directly or indirectly, for any portion of the civil monetary penalty paid pursuant to this Consent Order.

Consumer Restitution

62. Respondents represent that, in connection with their agreement with consumer plaintiffs in *In re: Equifax Inc. Customer Data Security Breach Litigation*, MDL No. 2800 (Consumer Cases) (the "Related Litigation"), they have agreed to provide restitution to New York consumers pursuant to a settlement fund ("Fund") to be established in conjunction with a nationwide class action settlement ("Settlement") in the Related Litigation, to be submitted to, approved by, and overseen by the court in the Related Litigation, as follows:

a. A court-approved outside administrator (the "Administrator") shall be retained to distribute restitution to affected New York consumers identified by Respondents as having their personal information compromised as a result of the Data Breach ("Impacted New York Consumers");

b. Impacted New York Consumers will have the opportunity to enroll in at least four years of three-bureau credit monitoring services, which shall be provided and maintained by an independent third party through a court-approved Settlement of the Related Litigation. The three-bureau credit monitoring

services shall include:

i. Three-bureau (EIS, Experian, TransUnion) credit monitoring and automated alerts regarding key changes to the consumer's credit report at the respective nationwide bureau;

ii. Internet monitoring that includes searching suspicious web sites for the consumer's Social Security number; and

iii. A $1,000,000 identity theft insurance policy.

c. Contingent upon the court's entry of the Order Permitting Issuance of Notice of Class Action Settlement in the Related Litigation, the claims period for the credit monitoring services in sub-paragraph (b) above shall run for a period of six months after the entry of the Order Permitting Issuance of Notice of Class Action Settlement in the Related Litigation. The minimum of four years of three-bureau credit monitoring services shall be provided in addition to any free credit monitoring services Respondents are currently providing or have previously offered as a result of the Data Breach.

d. Impacted New York Consumers who certify that they have credit monitoring in place and will maintain it for at least six months after submitting their claim may file a claim for alternative compensation in the amount of $125 in lieu of the free credit monitoring described in sub-paragraph (b) above which shall be distributed from the Fund. Impacted New York Consumers who elect to receive payment under this provision are not eligible to enroll in credit monitoring services offered in sub-paragraph (b) above or to seek reimbursement under the Fund, as Out-of-Pocket Losses described in sub-paragraph (e) below, for

purchasing credit monitoring or protection services covering the six-month period after the date a claim is made for alternative compensation.

e. Impacted New York Consumers can submit valid claims for Out-of-Pocket Losses as set forth in the Settlement that are fairly traceable to the Data Breach. Individual claimants will be subject to an aggregate claims cap of $20,000 and paid directly by the Administrator from the Fund in the Related Litigation. This provision does not prevent Impacted New York Consumers from submitting claims under applicable insurance policies.

f. To obtain any of the restitution described above, Impacted New York Consumers will need to submit a valid claim during one of the two claims periods: the "Initial Claims Period" and the "Extended Claims Period." The Initial Claims Period will run for a period of six months from a date set by the court in the Related Litigation. The Extended Claims Period will run for up to four years after the conclusion of the Initial Claims Period. During the Extended Claims Period, Impacted New York Consumers can seek reimbursement for valid Out-of-Pocket Losses, as set forth in the Settlement, (excluding losses of money and time associated with placing or removing freezes on credit files and purchasing credit monitoring services) incurred during the Extended Claims Period only if the Impacted New York Consumer provides a certification that he or she has not obtained reimbursement for the claimed expense through other means. All restitution claims described above are subject to the terms set forth in the court-approved Settlement in the Related Litigation.

63. EIS shall offer Impacted New York Consumers two free copies of their EIS credit

report every twelve months for five years (in addition to the free credit report per year a consumer may obtain on annualcreditreport.com), beginning December 31, 2019;

64. Impacted New York Consumers shall receive notice of the restitution available under the Settlement in accordance with the notice plan approved by the court in the Related Litigation.

65. Respondents, including by or through any partner, affiliate, agent, or third party, shall not use any information provided by consumers to enroll, or to attempt to enroll, in the credit monitoring services set forth in paragraph 62 above to sell, upsell, or directly market or advertise its fee-based products or services. Nothing in this paragraph shall relieve Respondents of any obligation, or prevent Respondents from complying with their obligations, under federal and/or state law to offer and/or advertise security freezes.

66. For those Impacted New York Consumers who have placed a one-year fraud alert through EIS's online channel beginning on or after the effective date of this agreement, Respondents shall send an e-mail reminder to the consumer within one month prior to the expiration of the consumer's one-year fraud alert reminding the consumer of the expiration date. The injunctive relief in this paragraph shall apply for four years from the effective date of this agreement.

IT and Security Practices

67. Respondents have agreed to undertake certain actions, including with respect to IT and Security practices, as stated in the consent order dated June 25, 2018 between Equifax Inc. and the Multi-State Regulatory Agencies, to which the Department is a party.

Other Provisions

68. Respondents submit to the authority of the Superintendent of Financial Services of the State of New York (the "Superintendent") to effectuate this Consent Order.

69. If the Department believes Respondents to be in material breach of this Consent Order, the Department will provide written notice to Respondents and they must, within fifteen business days of receiving such notice, or on a later date if so determined in the Department's sole discretion, appear before the Department to demonstrate that no material breach has occurred or, to the extent pertinent, that the breach is immaterial or has been cured.

70. Respondents' failure to make the required showing within the designated time period as set forth in paragraph 69 of this Consent Order shall be presumptive evidence of Respondents' material breach. Upon a finding by the Department that any Respondent has breached this Consent Order, the Department has all the remedies available to it under all applicable laws and may use any evidence available to it in connection with any ensuing hearings, notices, orders or other remedies that are available.

71. The Department has agreed to the terms of this Consent Order based on, among other things, representations made to the Department by Respondents, either directly or through counsel, and the Department's own factual investigation. To the extent that representations made by Respondents are later found to be materially incomplete or materially inaccurate, this Consent Order is voidable by the Superintendent in her sole discretion.

72. Upon the Department's request, Respondents shall provide all non-privileged documentation and information reasonably necessary for the Department to verify compliance with this Consent Order.

73. Respondents represent and warrant, through the signature below, that the terms and conditions of this Consent Order are duly approved, and the execution of this Consent Order is duly authorized.

74. All written communications to any party pursuant to this Consent Order shall be directed as follows.

If to the Department:

New York State Department of Financial Services
One State Street
New York, New York 10004-1511
Attn: Christopher B. Mulvihill, Deputy Superintendent, or Serwat Farooq, Assistant Counsel

If to Respondents:

Equifax
General Counsel
1550 Peachtree St NW
Atlanta, GA 30309

William Johnson, Esq.
King & Spalding LLP
1185 Avenue of the Americas
New York, NY 10036

75. This Consent Order and any dispute thereunder shall be governed by the laws of the State of New York without regard to any conflicts of laws principles.

76. Respondents waive their right to further notice and hearing in this matter as to any allegations of past violations by the Department's Consumer Protection and Financial Enforcement Division (but expressly excluding any allegations of past violations arising out of any prior or current regulatory examinations of Respondents conducted by the Department's Banking Division (Licensed Financial Services)) up to and including the effective date of this Consent Order and agrees that no provision of this Consent Order is subject to review in any court or tribunal outside of the Department.

77. This Consent Order is binding on the parties, as well as any successors and assigns. This Consent Order does not bind any federal or other state agency or any law enforcement authority.

78. The Consent Order may not be altered, modified, or changed unless in writing signed by the parties hereto.

79. The Consent Order shall be enforceable and remain in effect unless stayed or terminated in writing by the Superintendent or her designee.

80. This Consent Order constitutes the entire agreement between the Department and Respondents and supersedes any prior communication, understanding, or agreement, whether written or oral, concerning the subject matter of this Consent Order (but expressly does not supersede the Consent Order dated June 25, 2018 between Equifax Inc. and the Multi-State Regulatory Agencies named in that Order).

81. No inducement, promise, understanding, condition, or warranty not set forth in this Consent Order has been relied upon by any party to this Consent Order.

82. In the event that one or more provisions contained in this Consent Order shall for any reason be held to be invalid, illegal, or unenforceable in any respect, such invalidity, illegality, or unenforceability shall not affect any other provision of this Consent Order.

83. Upon the parties' execution of this Consent Order, the Department will discontinue the Investigation as to and against Respondents solely with respect to the conduct set forth herein during the Relevant Period. No further action will be taken by the Department against Respondents for the conduct set forth in this Consent Order that occurred during the Relevant Period provided they comply with the terms of the Consent Order. This paragraph shall not be construed to prevent the Department from enforcing the Consent

Order dated June 25, 2018 between Equifax Inc. and the Multi-State Regulatory Agencies named in that Order.

84. Nothing in this Consent Order shall be construed to prevent any consumer from pursuing any right or remedy at law.

85. Nothing contained in this Consent Order shall create any third-party beneficiary rights or give rise to or support any right of action in favor of any consumer or group of consumers, or confer upon any person other than the parties hereto any rights or remedies. The Department's Findings in this Consent Order were not the subject of an adjudicated proceeding and are not intended to be and shall not be construed as, deemed to be, represented as, or relied upon in any manner by any party in any domestic or foreign civil, criminal, or administrative proceeding before any court, administrative agency, arbitration, or other tribunal as evidence that Respondents have violated any foreign, federal, state, or local law.

86. Except with regard to the enforcement of this Consent Order, Respondents' consent to the provisions of this Consent Order does not bar, estop, waive, or otherwise prevent Respondents from raising any defenses to any action taken by any federal or state agency or department, or any private action against Respondents.

87. This Consent Order may be executed in one or more counterparts, and shall become effective on July 22, 2019, provided that such counterparts have been signed by each of the parties hereto and So Ordered by the Superintendent or her designee.

WHEREFORE, the signatures evidencing assent to this Consent Order have been affixed hereto on the dates set forth below.

NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES

By: _____
Serwat Farooq
Assistant Counsel, Enforcement
Consumer Protection & Financial Enforcement Division

July __, 2019

By: _____
Christopher B. Mulvihill
Deputy Superintendent, Enforcement
Consumer Protection & Financial Enforcement Division

July __, 2019

By: _____
Katherine A. Lemire
Executive Deputy Superintendent
Consumer Protection & Financial Enforcement Division

July __, 2019

EQUIFAX INC.

By: _____
John J. Kelley III
Corporate Vice President, Chief Legal Officer and Corporate Secretary

July __, 2019

EQUIFAX INFORMATION SERVICES, LLC

By: _____
John J. Kelley III
Corporate Vice President, Chief Legal Officer and Corporate Secretary

July __, 2019

EQUIFAX CONSUMER SERVICES, LLC

By: _____
John J. Kelley III
Corporate Vice President, Chief Legal Officer and Corporate Secretary

July __, 2019

THE FOREGOING IS HEREBY APPROVED. IT IS SO ORDERED.

_____
LINDA A. LACEWELL
Superintendent of Financial Services

July __, 2019

WHEREFORE, the signatures evidencing assent to this Consent Order have been affixed hereto on the dates set forth below.

NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES

By: Serwat Farooq
Serwat Farooq
Assistant Counsel, Enforcement
Consumer Protection & Financial Enforcement Division

July 19, 2019

By: Christopher B. Mulvihill
Christopher B. Mulvihill
Deputy Superintendent, Enforcement
Consumer Protection & Financial Enforcement Division

July 19, 2019

By: Katherine Lemire /SF
Katherine A. Lemire
Executive Deputy Superintendent
Consumer Protection & Financial Enforcement Division

July 19, 2019

EQUIFAX INC.

By: _____
John J. Kelley III
Corporate Vice President, Chief Legal Officer and Corporate Secretary

July __, 2019

EQUIFAX INFORMATION SERVICES, LLC

By: _____
John J. Kelley III
Corporate Vice President, Chief Legal Officer and Corporate Secretary

July __, 2019

EQUIFAX CONSUMER SERVICES, LLC

By: _____
John J. Kelley III
Corporate Vice President, Chief Legal Officer and Corporate Secretary

July __, 2019

THE FOREGOING IS HEREBY APPROVED. IT IS SO ORDERED.

Linda A. Lacewell
LINDA A. LACEWELL
Superintendent of Financial Services

July 19, 2019