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

BUREAU OF CONSUMER FINANCIAL PROTECTION, Plaintiff, v. EQUIFAX INC., Defendant.	Civil Action Number: **COMPLAINT FOR PERMANENT INJUNCTION AND OTHER RELIEF**

Plaintiff, the Bureau of Consumer Financial Protection ("Bureau"), alleges:

1. The Bureau brings this action under Sections 1031(a), 1036(a)(1), and 1054 of the Consumer Financial Protection Act of 2010 ("CFPA"), 12 U.S.C. §§ 5531(a), 5536(a)(1), and 5564, to obtain permanent injunctive relief, restitution, disgorgement, damages, civil money penalties, and other relief for Defendant's violations of the CFPA.

JURISDICTION AND VENUE

2. This Court has subject matter jurisdiction pursuant to 12 U.S.C. § 5565(a)(1).

3. Venue is proper in the United States District Court for the Northern District of Georgia because Defendant does business and maintains its principal place of business in this District, 28 U.S.C. §§ 1391(b), and 12 U.S.C. § 5564(f).

PARTIES

4. Plaintiff Bureau is an independent agency of the United States Government created by the CFPA. 12 U.S.C. § 5491(a). The Bureau is charged with enforcing Federal consumer financial laws, including the CFPA. 12 U.S.C. §§ 5531(a), 5564(a)-(b), 5481(12) and (14).

5. The Bureau is authorized to initiate federal district court proceedings, by its own attorneys, to address violations of Federal consumer financial law, including the CFPA. 12 U.S.C. § 5564(a)-(b). Sections 1031 and 1036(a) of the CFPA, 12 U.S.C. §§ 5531 and 5536(a), prohibit unfair, deceptive, or abusive acts or practices, or other violations of Federal consumer financial law, by any covered person or service provider. The Bureau is authorized to secure any appropriate legal or equitable relief with respect to a violation of Federal consumer financial law, including, without limitation, permanent injunctive relief, restitution, disgorgement, damages, civil money penalties, and other relief. 12 U.S.C. § 5565(a).

6. Defendant Equifax Inc. ("Equifax" or "Defendant"), is a Georgia corporation with its principal place of business at 1550 Peachtree St., NW, Atlanta, Georgia 30309. Equifax transacts business in this district and throughout the United States.

7. Defendant collects, analyzes, maintains or provides consumer report information or other account information, including information related to the credit history of consumers, used or expected to be used in connection with any decision regarding the offering or provision of a consumer financial product or service. Thus, Defendant provides a financial product or service covered by the CFPA, 12 U.S.C. § 5481(15)(A)(ix). This financial product or service includes providing consumer reports, credit file disclosures, credit scores, and the ability to freeze or lock consumer credit files. Defendant offers or provides these financial products or services to consumers primarily for personal, family, or household purposes, and delivers, offers, and provides them in connection with a consumer financial product or service such as consumer credit. Defendant is therefore engaged in offering or providing a consumer financial product or service and thus is a covered person within the meaning of the CFPA, *id.* § 5481(6). Consumer reports, credit file disclosures, credit scores, and the ability to freeze or lock consumer credit files are consumer financial products or services because (i) they

are consumer reports or other account information, including information relating to the credit history of consumers that Defendant collects and maintains about a consumer's account, and (ii) they are offered or provided for use by consumers primarily for personal, family, or household purposes or are delivered, offered, or provided in connection with a consumer financial product or service.

DEFENDANT'S BUSINESS PRACTICES

8. Defendant offers various credit reporting and information products and services to businesses and consumers. Defendant collects, processes, stores and maintains vast quantities of consumers' personal information, including personal information about more than 200 million U.S. consumers. Consumers have no control over what information businesses share with the Defendant, little control over what Defendant does with that information, and no control over how, or whether, that information is protected.

9. Defendant warehouses much of this information in its primary U.S. credit reporting database, known as Automated Credit Reporting Online ("ACRO"). Defendant uses ACRO to provide credit reports, credit scores, collections, and prescreening products, among other things.

10. Defendant also maintains on its network a system referred to as the Automated Consumer Interview System ("ACIS"). ACIS is a network of

applications and automated processes that handles consumer questions, concerns, and disputes regarding consumer credit data. Among other things, the ACIS network services an online dispute portal (the "ACIS Dispute Portal"), a web application where consumers can dispute items appearing on their consumer credit reports and upload supporting documentation. ACIS also services Defendant's platform for consumer credit freezes and fraud alerts, as well as all consumer requests for a free annual file disclosure through AnnualCreditReport.com ("ACR").

11. When a consumer disputes issues on his credit report through the ACIS Dispute Portal or otherwise transacts with Defendant for a consumer product or service (such as a subscription to a credit monitoring product, a request to freeze the consumer's credit, or a request for a free credit report from ACR), the consumer must first submit sensitive personal information. For example, a consumer who requests a free credit report from ACR must submit, among other things, a name, date of birth, and Social Security number ("SSN"). A consumer who requests a security freeze or a copy of their credit score or credit report must submit similar personally identifiable information ("PII"), as well as a credit card number and expiration date if a purchase is being made. Defendant logs and stores

consumers' PII in databases connected to ACIS. These databases thus contain hundreds of millions of records of sensitive consumer personal information.

12. ACIS was originally built in the 1980s. It was designed to connect to ACRO and runs on outdated systems, many of which are no longer supported. Today, Defendant considers ACIS to be legacy infrastructure and its own documents describe the system as "archaic" and using "antiquated technology." As of 2016, about 25 million consumers interact with ACIS every year, with about 6.6 million of those consumers disputing transactions in their credit reports.

DEFENDANT'S 2017 DATA BREACH

13. On or about September 7, 2017, Defendant publicly disclosed a massive data breach (the "Breach") involving the theft of sensitive consumer personal information from nearly 148 million consumers. As described below, the Breach resulted from Defendant's failures to undertake numerous basic security measures to secure the PII stored in databases connected to the ACIS Dispute Portal.

14. On or about March 8, 2017, the United States Computer Emergency Readiness Team ("US-CERT") alerted Defendant to a new critical security vulnerability (referred to as 2017-CVE-5638) found in Apache Struts, an open source framework used to build Java web applications. The alert encouraged

anyone using a vulnerable version of the software to update the software to a new version released by the Apache Software Foundation, which was available for free online to all Apache software users. Within days, press reports indicated that attackers had already begun to exploit this critical vulnerability.

15. Defendant's security team received the US-CERT alert and, on or about March 9, 2017, disseminated the alert internally by a mass email to more than 400 employees. The mass email directed employees, "if [they were] responsible for an Apache Struts installation," to patch the vulnerability within 48 hours, as required by Defendant's Patch Management Policy.

16. The ACIS Dispute Portal contained a vulnerable version of Apache Struts. However, Defendant failed to apply the patch to the ACIS Dispute Portal for months. Defendant's security team issued an order to patch all vulnerable systems within 48 hours, yet Defendant failed to include the employee responsible for maintaining the ACIS Dispute Portal on the mass email ordering a patch. As a result, the ACIS Dispute Portal was not patched, and the fact that the ACIS Dispute Portal was unpatched went unnoticed.

17. On or about March 15, 2017, Defendant performed an automated vulnerability scan intended to search for vulnerable instances of Apache Struts that remained on Defendant's network. But Defendant used a scanner that was not

configured to correctly search all of Defendant's potentially vulnerable assets. As a result, the automated scanner did not identify any systems vulnerable to 2017-CVE-5638 and the ACIS Dispute Portal remained unpatched.

18. Defendant failed to discover the unpatched vulnerability for more than four months. On or about July 29, 2017, Defendant's security team identified some suspicious traffic on the ACIS Dispute Portal after replacing expired security certificates. Defendant's security personnel blocked the suspicious traffic but identified additional suspicious traffic the next day, at which time Defendant took the ACIS Dispute Portal offline.

19. Defendant retained a forensic consultant who ultimately determined that between May 13, 2017, and July 30, 2017, multiple attackers were each able to separately exploit the 2017-CVE-5638 vulnerability in the ACIS Dispute Portal to gain unauthorized access to Defendant's network. Once inside, the attackers were able to crawl through dozens of unrelated databases containing information that went well beyond the ACIS Dispute Portal, in part because of a lack of network segmentation. The attackers also accessed an unsecured file share (or common storage space) connected to the ACIS databases where they discovered numerous administrative credentials, stored in plain text, that they used to obtain further access to Defendant's network, including the ACIS databases. By August 11,

2017, Defendant had determined that the attack had compromised a large amount of consumer PII.

20. During the months that the attackers were able to operate undetected on Defendant's network, the attackers ran nearly ten thousand queries on Defendant's databases. These queries were specifically designed to identify SSNs, dates of birth, and other sensitive consumer information most valuable for identity theft.

21. According to Defendant's forensic analysis, the attackers were able to steal approximately 147 million names and dates of birth, 145.5 million SSNs, 99 million physical addresses, 20.3 million telephone numbers, 17.6 million email addresses, and 209,000 payment card numbers and expiration dates, among other things. This data, in part, came from consumers who had previously obtained direct-to-consumer products from Defendant, such as credit scores, credit monitoring, and identity theft prevention products ("DTC Products"), as well as from consumers who had requested a free copy of their Equifax credit report through ACR.

22. The attackers were able to infiltrate the network and exfiltrate large volumes of consumer personal information due to a series of basic security failures that Defendant failed to address, including:

A. Defendant failed to patch 2017-CVE-5638, a critical vulnerability. Defendant's patch management policies and procedures, which did not require any of Defendant's more than four hundred employees to acknowledge receipt of a critical patch directive or otherwise confirm that a critical patch was applied, directly contributed to this failure.

B. Defendant's reliance on an automated vulnerability scanner – without any other compensating controls to ensure that the vulnerability had been fully addressed – further contributed to Defendant's failure to patch the vulnerability. Although many companies use automated vulnerability scanners, Defendant (1) did not maintain an accurate inventory of public facing technology assets running Apache Struts (and therefore did not know where the scanner needed to run) and (2) relied on a scanner that was not configured to search through all potentially vulnerable public facing websites.

C. Defendant failed to segment the database servers connected to ACIS, a failure that permitted the attackers to easily gain access to vast amounts of information related to a broad variety of Equifax consumer products and services. The attackers did not need complex or advanced tools to pivot across Defendant's network.

D. Defendant left a file share connected to the ACIS databases where it was easily accessible by the attackers. The file share contained numerous administrative credentials and passwords in plain text. The file share also contained PII and was not protected by access controls. The attackers were able to leverage the credentials and passwords to access and comb through dozens of unrelated databases, including databases maintained by Defendant to support its consumer reporting activities, searching for sensitive consumer personal information.

E. Defendant stored more than 145 million SSNs and other sensitive consumer personal information in plain text, contrary to its own policies that require strong encryption and access controls for such PII.

F. Defendant had minimal protections for detecting intrusions on "legacy" technology systems, such as ACIS, which contributed to Defendant's months-long failure to detect the attackers on its network. For instance, the ACIS system lacked any File Integrity Monitoring, which would have alerted Defendant to unauthorized activity within the ACIS environment. In addition, Defendant failed to update expired security certificates on the ACIS Dispute Portal, which prevented Defendant from using tools in its possession that would have decrypted suspicious

traffic. The security certificate on the ACIS Dispute Portal had expired at least 10 months before the discovery of the Breach.

DEFENDANT'S DATA SECURITY PRACTICES

23. Defendant engaged in a number of practices that, taken together, failed to provide reasonable security for the massive quantities of sensitive personal information stored within Defendant's computer network. Among other things:

A. Defendant failed to implement reasonable procedures to detect, respond to and timely correct critical and other high-risk security vulnerabilities across Defendant's systems, including:

i. Patch management policies and procedures that failed to ensure the timely remediation of critical security vulnerabilities;

ii. Widespread noncompliance with Defendant's patch management policy, including unpatched critical and high-risk vulnerabilities across Defendant's systems that persisted for months;

iii. A failure to implement reasonable intrusion protection controls in legacy systems, including:

a) Failures to implement host and network intrusion prevention or file integrity monitoring that could have identified unauthorized access to Defendant's network; and

b) Failures to maintain security certificates that would have allowed Defendant to examine traffic for suspicious activity;

iv. Failures to implement readily-available protections, including many low-cost protections, against well-known and reasonably foreseeable vulnerabilities that could be exploited to gain unauthorized access to consumers' sensitive personal information and local networks, such as Cross-Site Scripting ("XSS"), Structured Query Language ("SQL") injection, security misconfigurations, and other common vulnerabilities;

B. Defendant failed to use readily available security measures to segment its servers and databases;

C. Defendant failed to implement or enforce reasonable access controls to prevent unauthorized access to sensitive consumer personal information. For example:

i. Defendant stored numerous administrative credentials with access to sensitive consumer personal information in plain text;

ii. Defendant copied sensitive consumer personal information, including SSNs, to numerous systems for development and testing purposes, which were accessible by employees and contractors without any business need;

iii. Defendant failed to monitor or log privileged account activity across numerous systems; and

iv. Until at least 2017, Defendant failed to limit administrative rights for any of its employees on company-issued PCs and other devices, and allowed users to install any software or alter configurations;

D. Defendant stored the sensitive personal information in plain text, including hundreds of millions of SSNs and payment card information, including credit card account numbers provided by consumers to Defendant to pay for DTC Products; and

E. Defendant failed to provide adequate security training for engineers and other employees.

24. Defendant could have prevented or mitigated the failures described in **Paragraphs 22-23** through cost-effective measures suitable for an organization of Defendant's size and complexity.

25. Internal company documents, since at least 2014, clearly demonstrate Defendant's awareness and actual knowledge of the failures described in **Paragraphs 22-23**.

26. Defendant's failure to reasonably secure the sensitive consumer personal information in its network, described in **Paragraphs 22-23**, has resulted in substantial injury to approximately 147 million consumers whose personal information was stolen. These injuries may include wasted time and money to secure personal accounts and consumer reports from future identity theft, the cost of obtaining additional credit monitoring products or security freezes, and a significant risk of becoming victims of identity theft in the future. Additionally, because information such as SSNs and dates of birth are immutable, identity thieves could wait years before capitalizing on the stolen information. Thus, Defendant's security failures are likely to continue to substantially injure consumers in the future. In addition to the injury to consumers from having to spend time and money taking measures to protect their identities, Defendant's failures caused or are likely to cause consumers to experience identity theft.

DEFENDANT'S SECURITY REPRESENTATIONS TO CONSUMERS

27. Since at least October 2013, Defendant has maintained a privacy policy for Defendant's direct-to-consumer offerings, including credit scores, credit

monitoring and identity management services, provided by Equifax Consumer Services LLC, which states:

> We are committed to protecting the security of your information through procedures and technologies designed for this purpose by taking these steps: We limit access to your personal information to employees having a reasonable need to access this information to provide products and services to you . . . We have reasonable physical, technical, and procedural safeguards to help protect your personal information.

28. In fact, as described above in **Paragraphs 22-23**, Defendant's security practices did not live up to the representations contained in these privacy policies. First, as previously described, Defendant did not limit access to personal information only to employees having a reasonable need to access the information. In many instances, Defendant stored sensitive personal information obtained from consumers who purchased Defendant's DTC Products in systems without any access controls where employees and contractors could access it without any business need. Second, Defendant's many security failures described in **Paragraphs 22-23** failed to provide reasonable technical, physical, or procedural safeguards for consumer data on Defendant's network.

DEFENDANT'S ACTS AND PRACTICES IN RESPONSE TO THE BREACH

29. In response to the Breach, Defendant engaged in acts and practices that caused additional harm or risk of harm to consumers.

30. Defendant created a dedicated website, www.equifaxsecurity2017.com ("Incident Website"), to allow consumers to determine whether their information was compromised in the Breach and to take remedial action, such as enrolling in Defendant's free credit monitoring product ("TrustedID Premier") or freezing their Equifax credit reports.

31. Defendant deployed the Incident Website in a manner that exposed consumers to additional security risks and delayed or impeded their efforts to take remedial actions.

32. When Defendant deployed the Incident Website on September 7, 2017, the Incident Website contained an XSS vulnerability. An XSS vulnerability exposes consumers to the risk that attackers will run harmful code on the site that can, among other things, capture consumers' sensitive personal information. Defendant patched the vulnerability within a few days, but by that time, millions of consumers had already visited the Incident Website and were exposed to this additional risk of harm.

33. Defendant also deployed the Incident Website in a way that made it impossible for visitors to distinguish between the actual site and malicious lookalike "phishing" sites created by criminals seeking to steal or "phish" consumers' PII in the wake of the Breach. Defendant did so by (a) hosting the

Incident Website on a different domain than its primary website (Equifax.com) and (b) registering the Incident Website in a manner that could not be traced back to Defendant as the owner and operator of the website. The Incident Website thus lacked typical indicia of legitimacy that would allow consumers to distinguish the website from phishing websites set up by criminals. Defendant's actions therefore made phishing easier for criminals and increased consumers' risk of falling victim to a phishing attack.

34. Consumers who were able to place a security freeze were exposed to additional risk of harm by Defendant. When a consumer signed up for a security freeze of her Equifax credit report, Defendant assigned the consumer a 10-digit personal identification number ("PIN") that she must use if she chooses to lift (or "thaw") the freeze in the future. From September 7, 2017, through September 11, 2017, Defendant assigned PINs that reflected the date and time that the consumer requested a security freeze. For example, if a consumer requested a security freeze at 2:15pm Eastern Time on September 8, 2017, Defendant assigned her the PIN number 0908171415.

35. Time and date stamp PINs are much more predictable than random PINs and are therefore vulnerable to brute-force attacks and other types of intrusions. Defendant's failure to provide sufficiently secure PINs was especially

problematic given that to lift a security freeze, an attacker needs only the PIN and the type of personal information already exfiltrated in the Breach.

36. Defendant did not contact or automatically re-assign random PINs to consumers who received non-random PINs prior to September 11, 2017.

37. Consumers were dependent on Defendant for information and services they needed to mitigate harm from the Breach (such as determining whether they were affected, placing a security freeze on their Equifax credit reports, and enrolling in TrustedID Premier). Defendant alone could provide these services to consumers. Further, consumers could not control how Defendant generated its "thaw" PINs and most consumers lacked Defendant's knowledge of basic flaws on the Incident Website.

38. By deploying the Incident Website and assigning security freeze PINs in a manner that exposed consumers to additional security risks, Defendant injured, or was likely to injure, consumers. Defendant exposed millions of consumers who had already been victimized by the Breach to additional risks that their information would be compromised and misused by criminals. Defendant's actions in response to the Breach also delayed and deterred consumers from mitigating the risk of identity theft or other misuse of their PII through protective measures.

VIOLATIONS OF SECTIONS 1031 AND 1036 OF THE CFPA

39. Sections 1031 and 1036(a)(1)(B) of the CFPA, 12 U.S.C. §§ 5531 and 5536(a)(1)(B), prohibit covered persons from engaging "in any unfair, deceptive, or abusive act or practice." A representation, omission, act, or practice is deceptive under the CFPA when it misleads or is likely to mislead the consumer, the consumer's interpretation of it is reasonable under the circumstances, and it is material. Acts or practices are unfair under the CFPA if "the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers" and "such substantial injury is not outweighed by countervailing benefits to consumers or competition." 12 U.S.C. § 5531(c).

Count I: Unfair Acts and Practices Regarding Defendant's Data Security Practices

40. In numerous instances, Defendant has failed to provide reasonable security for the sensitive consumer personal information collected, processed, maintained or stored within Defendant's computer networks.

41. Defendant's actions caused or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid and that is not outweighed by countervailing benefits to consumers or competition.

42. Defendant's practices as described in **Paragraph 40** above constitute unfair acts or practices in violation of the CFPA, 12 U.S.C. §§ 5531(a) and (c), and 12 U.S.C. § 5536(a)(1)(B).

Count II: Deceptive Acts and Practices Regarding Defendant's Data Security to Consumers

43. Through the means described in **Paragraph 27**, Defendant has represented, directly or indirectly, expressly or by implication, that Defendant limits access to consumer personal information to employees having a reasonable need to access this information to provide products and services to consumers, and that Defendant has reasonable physical, technical, and procedural safeguards to protect consumer personal information, for Defendant's DTC Products.

44. In truth and in fact, in numerous instances, Defendant failed to limit access to consumer personal information to employees having a reasonable need to access this information and lacked reasonable physical, technical, or procedural safeguards to protect this information.

45. Defendant's representations were likely to mislead consumers acting reasonably under the circumstances.

46. Defendant's representations were material because they were likely to affect a consumer's choice regarding whether to purchase or continue purchasing DTC Products from Equifax.

47. Defendant's representations as set forth in **Paragraph 43** are false or misleading and constitute a deceptive act or practice in violation of the CFPA, 12 U.S.C. §§ 5531(a) and 5536(a)(1)(B).

Count III: Unfair Acts and Practices Regarding Defendant's Response to the Data Breach

48. Defendant's acts and practices in response to the Breach, as set forth in **Paragraphs 29-38**, caused or were likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition.

49. Defendant provided an Incident Website and security freeze PINs in a manner that injured, or was likely to injure, consumers. Defendant exposed millions of consumers who had already been victimized by the Breach to additional risks that their information would be compromised and misused by criminals.

50. Consumers could not reasonably avoid the harm they have experienced as a result of Defendant's acts and practices in response to the Breach. Consumers were dependent on Defendant for information and services they needed to mitigate harm from the Breach, such as determining whether they were affected, placing a security freeze on their Equifax credit files, and enrolling in TrustedID Premier. Further, consumers could not control how Defendant generated its

"thaw" PINs and most consumers lacked detailed information about the security flaws on the Incident Website.

51. The injuries sustained or likely to be sustained by consumers are not outweighed by countervailing benefits to consumers or to competition. Defendant could have provided random PINs or implemented readily-available protections to secure the Incident Website from well-known and reasonably foreseeable vulnerabilities, at little or no extra cost, and any savings from Defendant's failure to design and implement these security measures did not benefit consumers or competition. Even if Defendant's failure to reasonably secure the Incident Website provided some countervailing benefits to consumers or competition, such benefits are not outweighed by the additional risks and injuries to which Defendant exposed consumers.

52. Defendant's practices as described in **Paragraph 48** above constitute unfair acts or practices in violation of the CFPA, 12 U.S.C. §§ 5531(a) and (c), and 12 U.S.C. § 5536(a)(1)(B).

CONSUMER INJURY

53. Consumers have suffered and will continue to suffer substantial injury as a result of Defendant's violations of the CFPA. In addition, Defendant has been unjustly enriched as a result of its unlawful acts or practices. Absent injunctive

relief by this Court, Defendant is likely to continue to injure consumers, reap unjust enrichment, and harm the public interest.

THIS COURT'S POWER TO GRANT RELIEF

54. Section 1055 of the CFPA, 12 U.S.C. § 5565, empowers this Court to "grant any appropriate legal or equitable relief with respect to a violation of Federal consumer financial law" including the CFPA. This relief includes rescission, refund of monies, restitution, disgorgement or compensation for unjust enrichment, payment of damages or other monetary relief, public notification regarding the violation, limits on the activities or functions of the person, and civil money penalties. 12 U.S.C. § 5565(a)(2). In addition, the Bureau may recover its costs in connection with the action, if it is the prevailing party. 12 U.S.C. § 5565(b).

PRAYER FOR RELIEF

55. Wherefore, Plaintiff Bureau, pursuant to Sections 1054 and 1055 of the CFPA, 12 U.S.C. §§ 5564 and 5565, and the Court's own equitable powers, requests that the Court:

A. Permanently enjoin Defendant from committing unfair and deceptive acts or practices in connection with its provision of consumer financial products or services to consumers;

B. Award such relief as the Court finds necessary to redress injury to consumers resulting from Defendant's violations of the CFPA, including but not limited to rescission or reformation of contracts, restitution, refund of monies paid, disgorgement of ill-gotten monies, and payment of damages and other monetary relief;

C. Award the Bureau civil money penalties for Defendant's violations of the CFPA;

D. Award the Bureau the costs of bringing this action; and

E. Award additional relief as the Court may determine to be just and proper.

Dated: July 22, 2019

LOCAL COUNSEL:

BYUNG J. PAK
United States Attorney

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

FOR PLAINTIFF:

BUREAU OF CONSUMER FINANCIAL PROTECTION

CARA PETERSEN
Acting Enforcement Director

JOHN WELLS
Deputy Enforcement Director

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