UNITED STATES OF AMERICA
CONSUMER FINANCIAL PROTECTION BUREAU

ADMINISTRATIVE PROCEEDING
File No. 2023-CFPB-0011

In the Matter of: **TransUnion; Trans Union LLC; and TransUnion Interactive, Inc.**	**CONSENT ORDER**

The Consumer Financial Protection Bureau (Bureau) has reviewed certain consumer reporting activities and related consumer financial products or services of TransUnion, Trans Union LLC, and TransUnion Interactive, Inc. (collectively Respondents, as defined below) and has identified the following law violations: Respondents have failed to timely place or remove Security Freezes and Locks (as defined below) in violation of the prohibition in the Consumer Financial Protection Act (CFPA) on unfair acts or practices, 12 U.S.C. §§ 5531 and 5536; represented to consumers that their Security Freezes or Locks had been placed or removed when they had not, in violation of the CFPA's prohibition on deceptive acts or practices, 12 U.S.C. §§ 5531 and 5536; failed to timely place or remove Security

Freezes in violation of the requirements of the Fair Credit Reporting Act (FCRA) as amended by Economic Growth, Regulatory Relief, and Consumer Protection Act (EGRRCPA), 15 U.S.C. §§ 1681c-1(i)(2)-(3), (j)(2), j(4)(C); and failed to exclude from prescreened solicitation lists certain consumers with Extended Fraud Alerts or Active-Duty Alerts (as defined below) in violation of the FCRA, 15 U.S.C. §§ 1681c-1(b)(1)(B) and (c)(2). Under §§ 1053 and 1055 of the CFPA, 12 U.S.C. §§ 5563, 5565, the Bureau issues this Consent Order (Consent Order).

I.

Jurisdiction

1. The Bureau has jurisdiction over this matter under §§ 1053 and 1055 of the CFPA, 12 U.S.C. §§ 5563 and 5565, and § 621 of FCRA, 15 U.S.C. § 1681s(b)(1)(H).

II.

Stipulation

2. Respondents have executed a "Stipulation and Consent to the Issuance of a Consent Order," dated October 10, 2023 (Stipulation), which is incorporated by reference and is accepted by the Bureau. By this Stipulation, Respondents have consented to the issuance of this Consent Order by the Bureau under

§§ 1053 and 1055 of the CFPA, 12 U.S.C. §§ 5563, 5565, without admitting or denying any of the findings of fact or conclusions of law, except that Respondents admit the facts necessary to establish the Bureau's jurisdiction over Respondents and the subject matter of this action.

III.

Definitions

3. The following definitions apply to this Consent Order:

a. "Active-Duty Alert" is a "statement in the file of a consumer" that "notifies all prospective users of a consumer report relating to the consumer that the consumer . . . is an active duty military consumer." 15 U.S.C. § 1681a(q)(2).

b. "Affected Consumers" includes all consumers who were affected by at least one of the following issues prior to the Effective Date:

i. all consumers whose requests to place or remove Security Freezes or Locks were pending as of July 15, 2020 and resolved by Respondents during the Sync-Up Process;

ii. all consumers whose requests to place or remove Security Freezes after the Sync-Up Process were subject to a delay beyond the statutory deadlines set forth in 15 U.S.C.

§ 1681c-1(i)(2)-(3), (j)(2), (j)(4) as a result of being Out of Sync;

iii. all consumers whose requests to place or remove Locks after the Sync-Up Process were subject to a delay as a result of being Out of Sync; or

iv. all consumers who had an unexpired lift remaining on the consumer's report, as set forth in Paragraphs 47-48.

c. "Board" means TransUnion's duly-elected and acting Board of Directors.

d. "Effective Date" means the date on which the Consent Order is entered on the administrative docket.

e. "Enforcement Director" means the Assistant Director of the Office of Enforcement for the Consumer Financial Protection Bureau, or their delegate.

f. "Extended Fraud Alert" refers to a "statement in the file of a consumer" that "notifies all prospective users of a consumer report relating to the consumer that the consumer may be a victim of fraud, including identity theft." 15 U.S.C. § 1681a(q)(2).

g. "Freeze Request" means a request made by a consumer to place or remove a Security Freeze.

h. "Lock" means a feature which may be provided as part of a credit-related product, including TransUnion Credit Monitoring and TrueIdentity, that allows a consumer to limit certain third parties from accessing the consumer's credit file.

i. "Lock Request" means a request made by a consumer to place or remove a Lock.

j. "Out of Sync" means the circumstances in which two internal databases did not reflect the same freeze status with respect to a particular consumer resulting in the failure to effectuate requests from consumers for Security Freezes and Locks to be placed or removed in a timely manner.

k. "Protected Consumer" means a person who is "under the age of 16 years at the time a request for the placement of a security freeze is made;" or "an incapacitated person or a protected person for whom a guardian or conservator has been appointed." 15 U.S.C. § 1681c-1(j)(1)(B).

l. "Related Consumer Action" means a private action by or on behalf of one or more consumers or an enforcement action by another governmental agency brought against one or more of the Respondents based on substantially the same facts as described in Section IV of this Consent Order.

m. "Relevant Period" includes from July 21, 2011 to the date of this Consent Order.

n. "Respondents" means TransUnion, Trans Union LLC, and TransUnion Interactive, Inc., individually, collectively, or in any combination, and their successors and assigns.

o. "Respondents' Executives" means Respondents' Chief Executive Officer; Chief Risk and Compliance Officer; Chief Operations Officer; Chief Technology, Data, and Analytics Officer; and Chief Legal Officer, or their equivalents or successors.

p. "Security Freeze" means "a restriction that prohibits a consumer reporting agency from disclosing the contents of a consumer report that is subject to such security freeze to any person requesting the consumer report," 15 U.S.C. § 1681c-1(i)(1)(C), subject to the exceptions set forth in 15 U.S.C. § 1681c-1(i)(4).

q. "Sync-Up Process" means the processes effectuated by Respondents on or about July 15, 2020 to correct their failure to place or remove tens of thousands of Security Freezes or Locks on Consumer Reports.

r. "Supervision Director" means the Assistant Director of the Office of Supervision Policy for the Consumer Financial Protection Bureau, or their delegate.

IV.

Bureau Findings and Conclusions

The Bureau finds the following:

4. Respondent TransUnion Interactive, Inc. (TUI) is a Delaware corporation headquartered in Chicago, Illinois that is responsible for certain consumer-facing functions of its parent companies Respondent Trans Union LLC (TULLC) and ultimate parent Respondent TransUnion. TUI is responsible for providing certain resources and support functions, including personnel and technology resources, that allow TULLC to carry out its responsibility to provide the ability for consumers to obtain consumer reports and to take certain actions associated with their consumer reports, including placing and removing Security Freezes and Locks on consumer reports, placing or removing Fraud Alerts and Active-Duty Alerts on consumer reports, and disputing information on consumer reports. TUI offers various products to consumers, such as credit scores, credit monitoring, and identity theft protection.

5. During the Relevant Period, Respondent TUI has offered or provided a "consumer financial product or service" and is therefore a "covered

person" under the CFPA. 12 U.S.C. §§ 5481(5), (6), (15)(A)(ix). Respondent TUI is a wholly-owned subsidiary of Respondent TULLC.

6. Respondent TULLC is a Delaware limited liability company headquartered in Chicago, Illinois. During the Relevant Period, Respondent TULLC has been an NCRA as defined in the FCRA and Regulation V. 15 U.S.C. § 1681a(p); 12 C.F.R. § 1022.130(h). Respondent TULLC compiles and maintains financial and consumer data, and uses credit information it has collected in consumer credit files to generate consumer reports and makes such information available to its wholly-owned subsidiary, Respondent TUI. Respondent TULLC markets, sells, and provides consumer reports to commercial users, such as lenders, insurance companies, and potential employers. TULLC is responsible for providing and provides the ability for consumers to obtain consumer reports and to take certain actions associated with their consumer reports, including placing and removing Security Freezes and Locks on consumer reports, placing or removing Extended Fraud Alerts and Active-Duty Alerts on consumer reports, and disputing information on consumer reports.

7. During the Relevant Period, both directly and indirectly through its agent and affiliate, Respondent TUI, Respondent TULLC has offered or

provided a "consumer financial product or service." 12 U.S.C. §§ 5481(5), (15)(A)(ix). Respondent TULLC is therefore a "covered person" under the CFPA. 12 U.S.C. § 5481(6).

8. Respondent TransUnion is a publicly traded company that is incorporated in Delaware and headquartered in Chicago, Illinois. Respondent TransUnion is the ultimate parent company of Respondents TUI and TULLC.

9. Respondent TransUnion is a "covered person" and a "related person" under the CFPA. 12 U.S.C. § 5481(6)(B), (25)(B), (C)(i).

10. To help protect their credit reports maintained by the three NCRAs from the threat of identity theft or other misuse of sensitive personal information, consumers rely on Security Freezes, mandated by Federal law beginning in September 2018 to be a free service,[1] or Locks, a feature of certain products. Security Freezes and Locks are intended to block certain third parties from access to consumers' credit reports to prevent a potential identity thief from obtaining credit in those consumers' names. Consumers can remove those Security Freezes and Locks when, for example, applying for credit for themselves. Consumers also can temporarily "lift" Security

[1] Prior to 2018, Respondents offered Security Freezes pursuant to various state laws, including some that allowed Respondents to charge consumers a fee to place or remove a Security Freeze.

Freezes. Thus, the timely and effective placement and removal of Security Freezes and Locks are crucial to the integrity and efficiency of the consumer economy.

11. Since at least 2003, Respondents failed to place or remove Security Freezes and Locks on the credit reports of tens of thousands of consumers in a timely manner. These consumers did not know about this failure, and some were told that their requests had been honored when they had not.

12. These failures, about which Respondents were aware, were caused by issues in Respondents' systems. Rather than resolving the root cause, Respondents attempted to place or remove Security Freezes and Locks manually when the system failed to honor consumers' requests for them (Requests). But Respondents did not keep up with the demand over time; in the wake of the 2017 security breach at Equifax, Inc. (Equifax) Requests increased significantly, and the number of Requests that were not honored timely by Respondents due to the issues with their systems steadily accumulated and were left unresolved for years. Indeed, for certain periods of time, Respondents were not systematically checking for or manually fixing Out of Sync Freeze and Lock Requests.

13. For certain consumers who extended their Active-Duty Alerts or Extended Fraud Alerts, Respondents also failed to continue to exclude those

consumers from marketing lists for prescreened offers. This was due to another problem with Respondents' systems.

14. Finally, Respondents allowed a third-party vendor handling Freeze Requests submitted by mail to process Freeze Requests within five business days rather than the three business days required by law, resulting in the failure to timely process thousands of Freeze Requests.

15. Respondents' failure to place or remove Security Freezes and Locks in a timely manner violated the prohibitions on deception and unfairness in the CFPA and, for free Security Freezes beginning when the applicable revisions to the FCRA took effect in September 2018, Respondents' failures violated the FCRA. Respondents' failure to exclude consumers with Active-Duty Alerts and Extended Fraud Alerts from marketing lists also violated the FCRA.

The "Out of Sync" Issue

16. Since at least 2003, tens of thousands of consumers were unable to timely place or remove Security Freezes or Locks on their TransUnion consumer reports because of longstanding issues with Respondents' databases.

17. Specifically, those consumers experienced an issue that Respondents referred to as "Out of Sync," when two databases would reflect a different status for the same consumer.

18. If a consumer sought to place a Security Freeze but it became Out of Sync, the Security Freeze may not have been placed on the consumer's report, potentially allowing a report to be provided to a third-party user against the consumer's wishes. Conversely, if a consumer sought to remove an existing Security Freeze but it became Out of Sync, the Security Freeze may not have been removed, potentially preventing the consumer's report from being provided to a third-party user.

19. Similarly, when consumers enrolled or unenrolled in products that featured a Lock, certain consumers whose reports were affected by the Out of Sync issue would not have the Lock placed or removed as they intended.

20. Consumers were harmed or were at risk of harm in both of the above scenarios. Consumers, whose reports were not frozen or locked despite their Requests, may have had their consumer reports provided to third-party users against the consumers' wishes, potentially exposing those consumers to identity theft and other harm. Consumers who wanted to remove Security Freezes or Locks from their consumer reports may have been in the process of seeking credit and needed third-party users to be able to pull their TransUnion reports in order to check their credit and approve new credit. Those consumers may have been at risk of harm by

the denial of credit by lenders who were unable to pull their TransUnion consumer reports.

21. Respondents did not tell consumers when their Requests were Out of Sync. In fact, for many consumers, regardless of whether consumers' Requests were successful or Out of Sync, Respondents would send them standard, automatically generated confirmation messages reflecting that their Requests had been successful. Consumers often did not discover until later that there had been an error. For example, many consumers did not learn until they were applying for credit that a Security Freeze or Lock remained on their TransUnion credit reports, and some consumers could not get the Security Freeze or Lock removed without significant effort and extensive communications with Respondents. Consumers complained that they were denied credit or were at risk of being denied credit because of this issue.

22. Respondents failed to adequately investigate, address, or remediate all the root causes of the Out of Sync issue, though some of the root causes were known or suspected by Respondents' employees for years. Respondents' employees proposed various remediation efforts, but some of those proposals, even if initiated, were not prioritized and followed through to successful remediation.

23. Respondents did not adequately prevent Freeze or Lock Requests from becoming Out of Sync in the first place. Instead, Respondents applied a series of after-the-fact and inadequate measures to implement Requests that were already Out of Sync, including by implementing manual measures with insufficient staffing.

24. Because Respondents failed to adequately address the Out of Sync issue, Requests affected by that issue were not honored in a timely fashion. Some were only delayed for days, which meant, at least for Freeze Requests, that although Respondents failed to execute them within timeframes required by law, they were still honored relatively close in time to the deadline.

25. But other Freeze and Lock Requests – amounting to tens of thousands of such Requests – were not honored for months or years.

26. While this was happening, demand for Security Freezes grew over time. In 2016, for example, Respondents received approximately 19,962 requests to place a Security Freeze and 7,551 requests to remove a Security Freeze each month. By 2019, that number increased to approximately 116,623 requests to place a Security Freeze and 35,337 requests to remove a Security Freeze each month. Requests for Locks increased as well. Respondents were increasingly unable to keep up with the volume of

Requests that were not timely implemented because they were Out of Sync.

27. As a result, a backlog of unresolved Requests grew over time. In January 2016, for example, at least 10,094 Freeze Requests were backlogged because they were Out of Sync. By December 2019, that number was at least 29,992.

The 2017 Equifax Data Breach

28. On or about September 7, 2017, Equifax, another NCRA, publicly disclosed a data breach (the Equifax Breach) involving the theft of sensitive consumer personal information from millions of consumers.

29. After the Equifax Breach became public, Respondents experienced a large increase in Freeze Requests from consumers who sought to protect their credit data. Just before the Equifax Breach announcement, in July and August 2017, Respondents received a total of 33,082 Freeze Requests; just after the announcement, in September and October 2017, Respondents received 2,022,240 Freeze Requests. This caused a corresponding increase in Freeze Requests that were Out of Sync and therefore had to be manually implemented, with which Respondents struggled to keep up.

30. After the Equifax Breach, employees of Respondents, specifically noting the massive increase in Requests and the increasing challenge of resolving

all of them manually, again proposed that Respondents prioritize and address the Out of Sync issue, but that did not happen at that time.

31. Thus, the backlog of Requests delayed as a result of being Out of Sync continued to grow in the wake of the Equifax Breach.

Enactment of EGRRCPA

32. Following the Equifax Breach, Congress passed EGRRCPA on May 24, 2018, which amended the FCRA. Among other things, EGRRCPA required consumer reporting agencies to place and remove Security Freezes for free for all United States consumers and required consumer reporting agencies to allow consumers to place Extended Fraud Alerts and Active-Duty Alerts on their consumer reports for free.

33. EGRRCPA sets forth specific timing requirements for the placement and removal of Security Freezes. Specifically, upon a consumer's request, consumer reporting agencies must place a Security Freeze on that consumer's report within one (1) business day if the request is by telephone or secure electronic means, or three (3) business days after receipt if the request is by mail. Similarly, upon a consumer's request, consumer reporting agencies must remove a Security Freeze on that consumer's report within one (1) hour if the request is by telephone or secure electronic means, or three (3) business days after receipt if the

request is by mail. The same timing requirements apply to Freeze Requests placed by representatives of Protected Consumers. These requirements became effective on September 21, 2018.

34. On August 9, 2018, shortly before the timing requirements of EGRRCPA became effective, the Bureau's Office of Supervision sent Respondents a questionnaire asking about Respondents' readiness and ability to comply with EGRRCPA. Specifically, the questionnaire asked whether Respondents had "any concerns with complying with the timing deadlines in Section 301 [of EGRRCPA] or anticipate any operational or other difficulties with the requirements of Section 301 [of EGRRCPA]?"

35. On September 7, 2018, Respondents responded to the Bureau's questionnaire. In response to the question about whether the Respondents had any operational concerns or concerns about complying with the timing requirements of EGRRCPA, Respondents indicated that they expected to be "fully compliant."

36. But Respondents had significant operational and other concerns about their ability to comply with EGRRCPA's timing requirements because of the Out of Sync issue. Respondents' employees expressed concerns that Respondents had repeatedly failed to prioritize fixing or preventing the Out of Sync issue from occurring and expected it to be exacerbated after

EGRRCPA's effective date. This was reported to, and discussed with, certain managers and executives.

37. These employee concerns materialized, and as the number of Freeze Requests increased, the number of backlogged Freeze Requests due to the Out of Sync issue also increased.

38. In other words, Respondents' statement that they expected to be "fully compliant" with EGRRCPA's timing requirements as of September 21, 2018 was not accurate, and they were not compliant by that time.

39. In addition to the Out of Sync issue, Respondents allowed a third-party vendor to process mail requests according to deadlines that were not in compliance with EGRRCPA's timing requirements, causing thousands of mailed Freeze Requests not to be resolved in a timely manner, as discussed below.

Failure to Remediate the Out of Sync Issue Despite its Increasing Impact on Consumers

40. In the months following the effective date of EGRRCPA, Respondents' staff continued fixing Out of Sync accounts manually. As a result, the number of Freeze Requests that remained Out of Sync for an extended period of time, in violation of the EGRRCPA deadlines, continued to increase.

41. During 2019, consumers continued to make large numbers of Freeze Requests, and the long-term backlog of Freeze Requests caused by the Out of Sync issue continued to increase – reaching 29,992 by December 2019.

42. Despite the issue and Respondents' widespread and longstanding awareness of it, Respondents did not take any significant steps to address it until they were notified in early February 2020 that the Bureau intended to examine their compliance with EGRRCPA. Then Respondents began to take action.

43. Over the next several months, Respondents took several steps to resolve the Out of Sync issue. For example, Respondents attempted to improve customer service agents' ability to address Out of Sync errors in real time. In addition, Respondents identified the number of Freeze Requests that were Out of Sync, some of which had been Out of Sync for years at that point.

44. On July 15, 2020, Respondents finally implemented tens of thousands of Freeze Requests backlogged due to the Out of Sync issue on a one-time basis, placing 19,675 Security Freezes and removing 19,068 Security Freezes. Most of those Freeze Requests had been Out of Sync for months or years.

45. Respondents are unable to identify Out of Sync Freeze and Lock Requests that were placed prior to July 15, 2020 and resolved prior to the Sync-Up Process.

46. Although the backlog has now been addressed, a small number of Requests go Out of Sync each month, requiring manual resolution.

The "Unexpired Lift" Issue

47. Another technical issue affected some consumers who enrolled in a product with a Lock feature after December 2019. As a quirk of the feature, Respondents automatically assigned those consumers' credit reports a "lift" that would not expire until the year 2099, even though the consumer had not taken any action to freeze or lock their report, let alone requested that any Security Freeze or Lock be "lifted." If the consumer never took affirmative action to activate the Lock feature and then took one of several steps, including unenrolling and then re-enrolling in the product or attempting to convert the Lock to a Security Freeze, the consumer could not actually place a Lock or Security Freeze because the original unexpired lift was still in place. Thus, despite the fact that consumers thought they had a Lock on their account, the assigned lift would remove or lift the Lock, unbeknownst to the consumers, thereby

allowing third party users to gain access to the consumers' credit files, exposing these consumers to potential financial harm.

48. This issue was resolved by Respondents in October 2022, but not before it affected almost 17,000 consumers who requested a Security Freeze, and about 3,000 consumers who requested a Lock, but did not receive them.

Active-Duty Alerts and Extended Fraud Alerts

49. When an Active-Duty Alert is added to a consumer's file, the consumer reporting agency must also, "during the 2-year period beginning on the date of such request, exclude the active duty military consumer from any list of consumers prepared by the consumer reporting agency and provided to any third party to offer credit or insurance to the consumer as part of a transaction that was not initiated by the consumer, unless the consumer requests that such exclusion be rescinded before the end of such period." 15 U.S.C. § 1681c-1(c)(2). When an Extended Fraud Alert is added to a consumer's file, the consumer reporting agency must also, "during the 5-year period beginning on the date of such request, exclude the consumer from any list of consumers prepared by the consumer reporting agency and provided to any third party to offer credit or insurance to the consumer as part of a transaction that was not initiated by the consumer, unless the consumer or such representative requests that such exclusion be rescinded

before the end of such period." 15 U.S.C. § 1681c-1(b)(1)(B). As a result of a system problem, Respondents did not extend the opt-out from prescreened solicitation lists for some consumers who sought to extend their Active-Duty Alerts or Extended Fraud Alerts.

50. Consumers can make a request directly to Respondents to obtain these alerts, but they can also submit the requests to any one of the NCRAs, and the requests will be forwarded to the other NCRAs through a system called the "Fraud Exchange." Due to a coding error, when certain consumers sought to extend an existing Extended Fraud Alert and Respondents were notified through the Fraud Exchange, Respondents failed to also extend the timeframe during which those consumers would be excluded from the prescreened solicitation lists. Similarly, when certain consumers sought to extend an existing Active-Duty Alert and Respondents were notified through the Fraud Exchange or through a direct consumer request via Respondents' website or telephone interactive voice response system, Respondents failed to also extend the timeframe during which those consumers would be excluded from the prescreened solicitation lists. These errors affected approximately 32,000 consumers.

51. Respondents identified this failure in an audit that culminated in a December 2018 report. However, Respondents determined the issue to be "low risk" and did not remediate it for over a year, until February 2020.

The Vendor Compliance Issue

52. Respondents also failed to timely resolve Freeze Requests because they allowed a third-party vendor handling incoming mail to exceed its deadline, which caused thousands of consumers' Freeze Requests to be delayed, including Requests on behalf of Protected Consumers.

53. EGRRCPA amended the FCRA to make special provision for Freeze Requests made on behalf of Protected Consumers, who are either under 16, incapacitated, or someone for whom a guardian or conservator has been appointed, recognizing they are particularly vulnerable to identity theft. 15 U.S.C. § 1681c-1(j)(1)(B).

54. In 2004, TULLC entered into a contract with a third-party vendor to handle certain incoming mail requests from consumers, including requests for the placement and removal of Security Freezes.

55. In May 2018, EGRRCPA amended the FCRA to specify that mail requests must be resolved within three days of receipt, effective September 21, 2018. Respondents failed to take adequate steps to ensure compliance with these new timing requirements. Although Respondents' contract with its

third-party vendor specified a general three-day turnaround time for certain consumer requests, Respondents did not update the contract or their instructions to the vendor to specifically make clear that a three-day statutory deadline applied to Security Freeze Requests. Respondents also allowed the vendor to exceed the contract-specified three-day turnaround time, including in late 2021, when—due to an increased volume of incoming mail requests—the vendor requested approval to process Security Freeze Requests under a five-day deadline, which Respondents granted.

56. As a result, from September 21, 2018, through October 13, 2022, Respondents, through their third-party vendor, failed to timely resolve approximately 17,000 Freeze Requests submitted by mail, including approximately 12,000 Freeze Requests made by representatives of Protected Consumers. Because Respondents only accepted Freeze Requests for Protected Consumers by mail, nearly all such requests were handled by the third-party vendor.

VIOLATIONS OF THE FCRA

Failure to Place Security Freezes

57. Under 15 U.S.C. § 1681c-1(i)(2), upon the request of a consumer, a Security Freeze must be placed on that consumer's report within certain

time limits: one (1) business day for requests by telephone or secure electronic means and three (3) business days for requests by mail.

58. Since September 21, 2018, for consumers affected by the Out of Sync issue, Respondents failed to place Security Freezes within the time limits set forth in the FCRA.

59. In addition, between December 2019 and October 2022, Respondents failed to place Security Freezes within the time limits set forth in the FCRA because an unexpired lift remained on consumers' accounts.

60. Finally, since September 21, 2018, for consumers who submitted Freeze Requests by mail, Respondents failed to place Security Freezes within the time limits set forth in the FCRA.

61. These failures, as described in Paragraphs 58, 59, 60, were in violation of 15 U.S.C. § 1681c-1(i)(2).

Failure to Place Security Freezes for Protected Consumers

62. Under 15 U.S.C. § 1681c-1(j)(2), within three (3) business days after receipt of a request of a Protected Consumer's representative sent by mail, a Security Freeze must be placed on the Protected Consumer's report.

63. Since September 21, 2018, Respondents failed to place Security Freezes within three days for Protected Consumers whose representatives submitted Freeze Requests by mail.

64. This failure, as described in Paragraph 63, was in violation of 15 U.S.C. § 1681c-1(j)(2).

Failure to Remove Security Freezes

65. Under 15 U.S.C. § 1681c-1(i)(3), upon the request of a consumer, a Security Freeze must be removed from that consumer's report within certain time limits: one (1) hour for requests by telephone or secure electronic means and three (3) business days for requests by mail.

66. Since September 21, 2018, for certain consumers affected by the Out of Sync issue, Respondents failed to remove Security Freezes within the time limits set forth in the FCRA.

67. In addition, since September 21, 2018, for certain consumers who submitted Freeze Requests by mail, Respondents failed to remove Security Freezes within the time limits set forth in the FCRA.

68. These failures, as described in Paragraphs 66 and 67, were in violation of 15 U.S.C. § 1681c-1(i)(3).

Failure to Remove Security Freezes for Protected Consumers

69. Under 15 U.S.C. § 1681c-1(j)(4)(C), within three (3) business days after receipt of a request of a Protected Consumer's representative sent by mail, a Security Freeze must be removed from the Protected Consumer's report.

70. Since September 21, 2018, Respondents failed to remove Security Freezes within three days for certain Protected Consumers whose representatives submitted Freeze Requests by mail.

71. This failure, as described in Paragraph 70, was in violation of 15 U.S.C. § 1681c-1(j)(4)(C).

Failure to Extend Removal from Prescreened Solicitation Lists

72. Under 15 U.S.C. § 1681c-1(b)(1)(B), a consumer must be excluded from prescreened solicitation lists for 5 years following an Extended Fraud Alert placed by that consumer.

73. Under 15 U.S.C. § 1681c-1(c)(2), a consumer must be excluded from prescreened solicitation lists for 2 years following an alert placed by that consumer if the consumer is in active-duty military status.

74. Between September 21, 2018 and February 2020, Respondents failed to extend the removal of certain consumers with Extended Fraud Alerts and Active-Duty Alerts from prescreened solicitation lists.

75. This failure, as described in Paragraph 74, was in violation of 15 U.S.C. §§ 1681c-1(b)(1)(B) and (c)(2).

VIOLATIONS OF THE CFPA

Unfairness (Failure to Place or Remove Security Freezes and Locks Upon Request)

76. 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." 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).

77. Between approximately 2003 and September 21, 2018, consumers in some States were required to pay fees to place Security Freezes. Between approximately 2003 to the present, some consumers have paid fees or agreed to provide their personal data and/or receive marketing communications from Respondents to enroll in products that featured a Lock.

78. Between 2003 and the present, Respondents failed to place or remove certain Security Freezes and Locks within a reasonable time, or the timeframes set forth under state or federal law.

79. For Freeze Requests or Lock Requests affected by the Out of Sync issue, Respondents did not take the requested action for many days or even years.

80. Likewise, for consumers affected by the unexpired lift issue, Respondents did not take the requested action for many days or months.

81. With respect to Respondents' failure to place Security Freezes and Locks:

a. Respondents' conduct caused or was likely to cause substantial injury to consumers. It exposed them to financial risk without their knowledge. Those consumers believed they had a Lock or Security Freeze in place on their credit report when, in fact, they did not. For paid products, consumers additionally did not receive the full benefit of their bargain.

b. Consumers could not reasonably avoid the harm because they had no choice but to seek a Security Freeze or Lock from Respondents if they wanted to protect their TransUnion credit reports.

82. With respect to Respondents' failure to remove Security Freezes or Locks:

a. Respondents' conduct caused or was likely to cause substantial injury to consumers who were seeking to remove their Security Freezes or Locks in order to apply for credit or other opportunities that required production of a credit report because those consumers may have been prevented from doing so when their reports could not be accessed. Those consumers

were also injured, or likely to be injured, by having to repeatedly expend their time and resources to contact Respondents in order to get their Locks or Security Freezes removed.

b. Consumers could not reasonably avoid the harm because they had no choice but to rely on Respondents to remove a Security Freeze or Lock on their TransUnion credit reports.

83. There was no countervailing benefit to consumers or competition in this conduct.

84. Therefore, in this manner, during the Relevant Period, Respondents engaged in unfair acts or practices in violation of the CFPA, 12 U.S.C. §§ 5531(a), (c); 5536(a)(1)(B)).

Deception (Relating to Failure to Place and Remove Security Freezes and Locks on Request)

85. 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.

86. When consumers submitted Freeze Requests or Lock Requests to Respondents, Respondents told consumers that their requests had been

successful. In fact, for tens of thousands of consumers, their requests were Out of Sync and had not been successful.

87. These inaccurate representations were material and consumers, acting reasonably, were misled by them.

88. Therefore, in this manner, during the Relevant Period, Respondents engaged in deceptive acts or practices in violation of the CFPA, 12 U.S.C. §§ 5531(a); 5536(a)(1)(B)).

ORDER

V.

Conduct Provisions

IT IS ORDERED, under §§ 1053 and 1055 of the CFPA, that:

89. Respondents and their officers, agents, servants, employees, and attorneys who receive actual notice of this Consent Order, whether acting directly or indirectly, may not violate (1) the CFPA's prohibition on unfair or deceptive acts and practices, 12 U.S.C. §§ 5531 and 5536, in connection with Security Freezes or Locks, and (2) the FCRA, 15 U.S.C. §§ 1681c-1(i)(2)-(3), (b)(1)(B), (c)(2), (j)(2), and (j)(4)(C).

Affirmative Requirements

90. Respondents must take the following affirmative actions:

a. Establish a committee or utilize an existing committee (the Committee), as follows:

i. The Committee shall:

(1) Assess potential risk to consumers arising from ongoing or recurring technology issues that have caused—or that create a material risk of—violations of this Consent Order or violations of the provisions of the CFPA or FCRA identified in paragraph 89, or any other failure to deliver a product or service to a consumer as required by law (Technology-Related Compliance Risk); and

(2) Direct the development and implementation of any new or revised policies, to be reviewed and approved by the Committee, as well as procedures in order to address Technology-Related Compliance Risk across all Respondents' departments and business units that provide, offer, or support Consumer Financial Products and Services, as defined by 12 U.S.C. §§ 5481(5), (15).

ii. The Committee must be composed of officers and employees best positioned to assess and address Technology-Related Compliance Risk, and include, at a minimum, the Chief Risk

and Compliance Officer and the Chief Technology, Data, and Analytics Officer, or their successor positions.

iii. The Committee shall solicit and assess regular reports that:

(1) Assess the adequacy of Respondents' issue identification, escalation, and tracking policies and procedures for technology issues, including by conducting periodic assessments of information technology ticketing processes and communications with consumers, including consumer complaints, to determine whether technology issues that present Technology-Related Compliance Risk are being appropriately escalated;

(2) Identify and describe any ongoing or recurring technology issues presenting Technology-Related Compliance Risk that exist as of the reporting date;

(3) Explain and evaluate the appropriateness of the current prioritization level for any planned remediation work related to those ongoing or recurring technology issues presenting Technology-Related Compliance Risk, including the reasons for that prioritization level, a description of any work that

has been prioritized ahead of it, and an evaluation of whether the current prioritization level is justified; and

(4) Propose solutions for the outstanding technology issues presenting Technology-Related Compliance Risk identified, including recommendations regarding additional resources needed to address and remediate those issues.

iv. The Committee shall provide regular reports to the Board, or a committee thereof, that include reports related to identified Technology-Related Compliance Risk.

b. Require that Respondents' Global Technology Department or its successor business unit provide regular reports to Respondents' Executives and Board, or a committee thereof, either directly or through the Committee, addressing the progress and issues relating to addressing the root causes for, and the processing of Freeze and Lock Requests affected by, the Out of Sync issue on or after the Effective Date.

c. Review and have processes designed to ensure that:

i. Respondents' contracts with vendors used to meet, in whole or in part, Respondents' FCRA obligations (FCRA-Related Vendors) are consistent with the provisions of FCRA identified in paragraph 89, including with timing and other requirements; and

ii. Respondents' FCRA-Related Vendors are complying with their contractual obligations relating to FCRA.

VI.

Compliance Plan

IT IS FURTHER ORDERED that:

91. Within 90 days of the Effective Date, Respondents must create and implement a comprehensive compliance plan designed to ensure that Respondents' conduct regarding Security Freezes, Locks, Active-Duty Alerts, and Extended Fraud Alerts complies with all applicable laws that the Bureau enforces, including Federal consumer financial laws, and the terms of this Consent Order (Compliance Plan). Respondents must review the Compliance Plan annually and either renew it as written or revise it as appropriate to ensure compliance with this Order. The Compliance Plan must include, at a minimum:

a. Detailed steps for addressing each action required by this Consent Order;
b. A mechanism to ensure that the Board, or a committee thereof, is kept apprised of the status of compliance actions; and
c. Specific timeframes and deadlines for implementation of the steps described above.

92. Respondents must provide the Compliance Plan to the Bureau upon request.

VII.

Role of the Board and Executives

IT IS FURTHER ORDERED that:

93. The Board has the ultimate responsibility for ensuring that Respondent complies with this Consent Order.

94. Respondents' Executives and the Board, or a committee thereof, must review all plans and reports required by this Consent Order, and any submissions to the Bureau prior to such submission.

95. One year after the Effective Date, and yearly thereafter, Respondents must submit to the Supervision Director an accurate written compliance progress report (Compliance Report) that has been approved by the Board, or a committee thereof, the accuracy of which is sworn to under penalty of perjury, and which, at a minimum:

a. Describes the steps that Respondents have taken to reasonably assess whether Respondents are complying with the Redress Plan, the Compliance Plan, and each applicable paragraph and subparagraph of this Consent Order;

b. Describes in detail whether and how Respondents have complied with the Redress Plan, the Compliance Plan, and each applicable paragraph and subparagraph of this Consent Order, including the manner of verification of such compliance and any corrective actions taken to remedy potential non-compliance with the applicable requirement, paragraph, or subparagraph; and

c. Attaches a copy of each Order Acknowledgment obtained under Section XII, unless previously submitted to the Bureau.

96. Respondents' Executives and the Board, or a committee thereof empowered by the full Board with the necessary authority, must:

a. Authorize whatever actions are necessary for Respondents to assess whether Respondents are complying with the Redress Plan, Compliance Plan, and each applicable paragraph and subparagraph of this Consent Order;

b. Authorize whatever actions, including corrective actions, are necessary for Respondents to fully comply with the Redress Plan, the Compliance Plan, and each applicable paragraph and subparagraph of this Consent Order; and

c. Require timely reporting by management to Respondents' Executives and the Board on the status of compliance obligations.

MONETARY PROVISIONS

VIII.

Order to Pay Redress

IT IS FURTHER ORDERED that:

97. Within 10 days of the Effective Date, Respondents must reserve or deposit into a segregated deposit account $3 million for the purpose of providing redress to Affected Consumers, on a pro rata basis, as required by this Section.

98. Within 90 days of the Effective Date, Respondents must submit to the Enforcement Director for review and non-objection a comprehensive written plan for providing redress consistent with this Consent Order (Redress Plan). The Enforcement Director will have the discretion to make a determination of non-objection to the Redress Plan or direct Respondents to revise it. If the Enforcement Director directs Respondents to revise the Redress Plan, Respondents must revise and resubmit the Redress Plan to the Enforcement Director within 30 days. After receiving notification that the Enforcement Director has made a determination of non-objection to the Redress Plan, Respondents must implement and adhere to the steps, recommendations, deadlines, and timeframes outlined in the Redress Plan.

99. Within 30 days of completing the Redress Plan, Respondents must submit to the Bureau a Redress Report detailing the number of consumers and consumer accounts who received redress, the total amount of redress paid to those consumers, and any remainder of funds to be wired to the Bureau pursuant to Paragraph 100.

100. After completing the Redress Plan, if the amount of redress provided to Affected Consumers is less than $3 million, within 30 days of the completion of the Redress Plan, Respondents must pay to the Bureau, by wire transfer to the Bureau or to the Bureau's agent, and according to the Bureau's wiring instructions, the difference between the amount of redress provided to Affected Consumers and $3 million.

101. The Bureau may use these remaining funds to pay additional redress to Affected Consumers. If the Bureau determines, in its sole discretion, that additional redress is wholly or partially impracticable or otherwise inappropriate, or if funds remain after the additional redress is completed, the Bureau will deposit any remaining funds in the U.S. Treasury. Respondents will have no right to challenge any actions that the Bureau or its representatives may take under this Section.

102. Respondents may not condition the payment of any redress to any Affected Consumer under this Consent Order on that Affected Consumer waiving any right.

IX.

Order to Pay Civil Money Penalty

IT IS FURTHER ORDERED that:

103. Under § 1055(c) of the CFPA, 12 U.S.C. § 5565(c), by reason of the violations of law described in Section IV of this Consent Order, Respondents must pay a civil money penalty of $5 million to the Bureau.

104. Within 10 days of the Effective Date, Respondents must pay the civil money penalty by wire transfer to the Bureau or to the Bureau's agent in compliance with the Bureau's wiring instructions.

105. The civil money penalty paid under this Consent Order will be deposited in the Civil Penalty Fund of the Bureau as required by § 1017(d) of the CFPA, 12 U.S.C. § 5497(d).

106. Respondents, for all purposes, must treat the civil money penalty paid under this Consent Order as a penalty paid to the government. Regardless of how the Bureau ultimately uses those funds, Respondents may not:

a. Claim, assert, or apply for a tax deduction, tax credit, or any other tax benefit for any civil money penalty paid under this Consent Order; or

b. Seek or accept, directly or indirectly, reimbursement or indemnification from any source, including but not limited to payment made under any insurance policy, with regard to any civil money penalty paid under this Consent Order.

107. To preserve the deterrent effect of the civil money penalty in any Related Consumer Action, Respondents may not argue that Respondents are entitled to, nor may Respondents benefit by, any offset or reduction of any compensatory monetary remedies imposed in the Related Consumer Action because of the civil money penalty paid in this action or because of any payment that the Bureau makes from the Civil Penalty Fund. If the court in any Related Consumer Action offsets or otherwise reduces the amount of compensatory monetary remedies imposed against Respondents based on the civil money penalty paid in this action or based on any payment that the Bureau makes from the Civil Penalty Fund, Respondents must, within 30 days after entry of a final order granting such offset or reduction, notify the Bureau, and pay the amount of the offset or reduction to the U.S. Treasury. Such a payment will not be considered an additional

civil money penalty and will not change the amount of the civil money penalty imposed in this action.

X.

Additional Monetary Provisions

IT IS FURTHER ORDERED that:

108. In the event of any default on Respondents' obligations to make payment under this Consent Order, interest, computed under 28 U.S.C. § 1961, as amended, will accrue on any outstanding amounts not paid from the date of default to the date of payment, and will immediately become due and payable.

109. Respondents must relinquish all dominion, control, and title to the funds paid to the fullest extent permitted by law and no part of the funds may be returned to Respondents.

110. Respondents acknowledge that their Taxpayer Identification Number(s) (Social Security Number or Employer Identification Number), which Respondents previously submitted to the Bureau, may be used for collecting and reporting on any delinquent amount arising out of this Consent Order, in accordance with 31 U.S.C. § 7701.

111. Within 30 days of the entry of a final judgment, consent order, or settlement in a Related Consumer Action, the affected Respondent(s) must notify the Supervision Director of the final judgment, consent order, or settlement in writing. That notification must indicate the amount of redress, if any, that Respondents paid or are required to pay to consumers and describe the consumers or classes of consumers to whom that redress has been or will be paid.

COMPLIANCE PROVISIONS

XI.

Reporting Requirements

IT IS FURTHER ORDERED that:

112. Respondents must notify the Bureau of any development that may affect compliance obligations arising under this Consent Order, including but not limited to a dissolution, assignment, sale, merger, or other action that would result in the emergence of successor companies; the creation or dissolution of any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Consent Order; the filing of any bankruptcy or insolvency proceeding by or against Respondents; or a change in Respondents' names or addresses. Respondents must provide this notice, if

practicable, at least 30 days before the development, but in any case no later than 14 days after the development.

113. Within 7 days of the Effective Date, Respondents must:

a. designate at least one telephone number and email, physical, and postal addresses as points of contact that the Bureau may use to communicate with each Respondent.

b. designate at least one telephone number and email, physical, and postal addresses as points of contact for consumers with inquiries related to consumer relief under the Consent Order;

114. Respondents must report any change in the information required to be submitted under Paragraph 113 at least 30 days before the change or within 14 days after learning about the change, whichever is sooner.

XII.

Order Distribution and Acknowledgment

IT IS FURTHER ORDERED that:

115. Within 7 days of the Effective Date, Respondents must submit to the Supervision Director an acknowledgment of receipt of this Consent Order, sworn under penalty of perjury.

116. Within 30 days of the Effective Date, Respondents must deliver a copy of this Consent Order to each of their Board members and executive officers, as well as to any business leaders, senior managers, and service providers who have responsibilities related to the subject matter of the Consent Order.

117. For 5 years from the Effective Date, Respondents must deliver a copy of this Consent Order to any business entity resulting from any change in structure referred to in Section XI, any future Board members and executive officers, as well as to any business leaders, senior managers, and service providers who will have responsibilities related to the subject matter of the Consent Order before they assume their responsibilities.

118. Respondents must secure a signed and dated statement acknowledging receipt of a copy of this Consent Order, ensuring that any electronic signatures comply with the requirements of the E-Sign Act, 15 U.S.C. § 7001 *et seq.*, within 30 days of delivery, from all persons receiving a copy of this Consent Order under this Section.

119. Ninety days from the Effective Date, Respondents must submit to the Bureau a list of all persons and their titles to whom this Consent Order was delivered under the Section of this Consent Order titled "Order Distribution and Acknowledgment" and a copy of all signed and dated

statements acknowledging receipt of this Consent Order under Paragraph 118.

XIII.

Recordkeeping

IT IS FURTHER ORDERED that:

120. Respondents must create and retain the following business records:

a. All documents and records necessary to demonstrate full compliance with each provision of this Consent Order, including all submissions to the Bureau.

b. All documents and records pertaining to the Redress Plan, described in Section VIII above.

c. Meeting minutes of the Board, its committees, and the Committee described in paragraph 90 regarding Respondents' compliance with this Consent Order and the Compliance Plan, with sufficient detail to document the substance of all matters discussed.

d. For each individual Affected Consumer: the consumer's name, address, phone number (if provided), email address (if provided), file identification number(s), whether the consumer made a Freeze Request or a Lock Request, date on which the consumer made their Freeze or

Lock Request, and date on which such Request was honored by Respondents.

e. For each consumer who makes a Freeze or Lock Request after the Effective Date, the consumer's name, address, phone number (if provided), email address (if provided), file identification number(s), whether the consumer made a Freeze Request or a Lock Request, the method of the request, the date and time the request was made, and the date and time the request was honored by Respondents;

f. All consumer complaints and refund requests relating to Respondents' failure to timely honor Freeze or Lock Requests (whether received directly or indirectly, such as through a third party) or the failure to remove consumers from prescreened solicitation lists, and any responses to those complaints or requests.

g. For each consumer who places or extends an Extended Fraud Alert or Active-Duty Alert through the Fraud Exchange after the Effective Date, the consumer's name, address, phone number (if provided), email address (if provided), file identification number(s), whether the consumer placed an Extended Fraud Alert or an Active-Duty Alert, the method of the request, the date and time the alert was placed, and the date and time the steps to place or extend such alert or to remove consumers from

prescreened solicitation lists were completed by Respondents;

h. Copies of all internet websites, maintained by or on behalf of Respondents, through which consumers can make a Freeze Request or Lock Request sufficient to demonstrate the experience of consumers on each materially different version of those websites, including confirmation messages, and a record of the date(s) and placements of such information;

i. Copies of all contracts, agreements, or instructions (whether memorialized in a contract or in a more informal manner) with or provided to any FCRA-Related Vendors; and

j. All final audit reports and associated workpapers, and compliance monitoring reports and associated workpapers, if any, regarding Respondents' compliance with the provisions of FCRA identified in paragraph 89.

121. All such documents and records must be maintained in their original electronic format. Data should be centralized, and maintained in such a way that access, retrieval, auditing, and production are not hindered.

122. Respondents must make the documents identified in Paragraph 120 available to the Bureau upon the Bureau's request.

XIV.

Notices

IT IS FURTHER ORDERED that:

123. Unless otherwise directed in writing by the Bureau, Respondents must provide all submissions, requests, communications, or other documents relating to this Consent Order in writing, with the subject line, "*In re* TransUnion, et al., File No. 2023-CFPB-0011," and send them by email to Enforcement_Compliance@cfpb.gov addressed as follows:

ATTN: Supervision Director
Consumer Financial Protection Bureau
ATTENTION: Office of Supervision

ATTN: Enforcement Director
Consumer Financial Protection Bureau
ATTENTION: Office of Enforcement

XV.

Cooperation with the Bureau

IT IS FURTHER ORDERED that:

124. Respondents must cooperate fully to help the Bureau determine the identity and location of, and the amount of injury sustained by, each Affected Consumer. Respondents must provide such information in their

or their agents' possession or control within 14 days of receiving a written request from the Bureau.

XVI.

Compliance Monitoring

IT IS FURTHER ORDERED that:

125. Within 14 days of receipt of a written request from the Bureau, Respondents must submit additional Compliance Reports or other requested information, which must be made under penalty of perjury; provide sworn testimony; or produce documents.

126. Respondents must permit Bureau representatives to interview any employee or other person affiliated with Respondents who has agreed to such an interview regarding: (a) this matter; (b) anything related to or associated with the conduct described in Section IV; or (c) compliance with the Consent Order. The person interviewed may have counsel present.

127. Nothing in this Consent Order will limit the Bureau's lawful use of civil investigative demands under 12 C.F.R. § 1080.6 or other compulsory process.

XVII.

Modifications to Non-Material Requirements

IT IS FURTHER ORDERED that:

128. Respondents may seek a modification to non-material requirements of this Consent Order (*e.g.*, reasonable extensions of time and changes to reporting requirements) by submitting a written request to the Supervision Director.

129. The Supervision Director may, in their discretion, modify any non-material requirements of this Consent Order (*e.g.*, reasonable extensions of time and changes to reporting requirements) if they determine good cause justifies the modification. Any such modification by the Supervision Director must be in writing.

ADMINISTRATIVE PROVISIONS

XVIII.

IT IS FURTHER ORDERED that:

130. The provisions of this Consent Order do not bar, estop, or otherwise prevent the Bureau from taking any other action against Respondents, except as described in Paragraph 131. Further, for the avoidance of doubt, the provisions of this Consent Order do not bar, estop, or otherwise

prevent any other person or governmental agency from taking any action against Respondents.

131. The Bureau releases and discharges Respondents from all potential liability for law violations that the Bureau has or might have asserted based on the practices described in Section IV of this Consent Order, to the extent such practices occurred before the Effective Date and the Bureau knows about them as of the Effective Date. The Bureau may use the practices described in this Consent Order in future enforcement actions against Respondents and their affiliates, including, without limitation, to establish a pattern or practice of violations or the continuation of a pattern or practice of violations or to calculate the amount of any penalty. This release does not preclude or affect any right of the Bureau to determine and ensure compliance with the Consent Order, or to seek penalties for any violations of the Consent Order.

132. This Consent Order is intended to be, and will be construed as, a final Consent Order issued under § 1053 of the CFPA, 12 U.S.C. § 5563, and expressly does not form, and may not be construed to form, a contract binding the Bureau or the United States.

133. This Consent Order will terminate on the later of 5 years from the Effective Date or 5 years from the most recent date that the Bureau

initiates an action alleging any violation of the Consent Order by Respondents, if such action is initiated within 5 years of the Effective Date. If such action is dismissed or the relevant adjudicative body rules that Respondents did not violate any provision of the Consent Order, and the dismissal or ruling is either not appealed or upheld on appeal, then the Consent Order will terminate as though the action had never been filed. The Consent Order will remain effective and enforceable until such time, except to the extent that any provisions of this Consent Order have been amended, suspended, waived, or terminated in writing by the Bureau or its designated agent.

134. Calculation of time limitations will run from the Effective Date and be based on calendar days, unless otherwise noted.

135. Should Respondents seek to transfer or assign all or part of their operations that are subject to this Consent Order, Respondents must, as a condition of sale, obtain the written agreement of the transferee(s) or assignee(s) to comply with all applicable provisions of this Consent Order.

136. The provisions of this Consent Order will be enforceable by the Bureau. For any violation of this Consent Order, the Bureau may impose the maximum amount of civil money penalties allowed under §1055(c) of the CFPA, 12 U.S.C. § 5565(c). In connection with any attempt by the Bureau

to enforce this Consent Order in federal district court, the Bureau may serve Respondents wherever Respondents may be found and Respondents may not contest that court's personal jurisdiction over Respondents.

137. This Consent Order and the accompanying Stipulation contain the complete agreement between the parties. The parties have made no promises, representations, or warranties other than what is contained in this Consent Order and the accompanying Stipulation. This Consent Order and the accompanying Stipulation supersede any prior oral or written communications, discussions, or understandings.

138. Nothing in this Consent Order or the accompanying Stipulation may be construed as allowing Respondents, the Board, officers, or employees to violate any law, rule, or regulation.

IT IS SO ORDERED, this 12th day of October, 2023.

Rohit Chopra

Rohit Chopra
Director
Consumer Financial Protection Bureau