NEW YORK STATE
DEPARTMENT OF FINANCIAL SERVICES
ONE STATE STREET
NEW YORK, NEW YORK 10004

----------x

In the Matter of :

ONEMAIN FINANCIAL GROUP, LLC :

----------x

CONSENT ORDER

The New York State Department of Financial Services (the "Department" or "DFS") and OneMain Financial Group, LLC ("OneMain" or the "Company") agree to resolve the matters described herein without further proceedings.

WHEREAS, OneMain wholly owns two entities that hold licenses with the Department: OneMain Consumer Loan, Inc., which holds a licensed lender license, and OneMain Mortgage Services, Inc., which holds a mortgage loan servicer license;

WHEREAS, OneMain is a publicly traded company specializing in nonprime lending that operates in 44 states, has more than 6,000 employees and approximately 1,400 branches, manages a combined total of 2.45 million customer accounts, and reported $4.37 billion in annual revenue as of December 31, 2021;

WHEREAS, August 29, 2017, marked the effective date of New York's first-in-the-nation cybersecurity regulation, 23 NYCRR Part 500 (the "Cybersecurity Regulation");

WHEREAS, the Cybersecurity Regulation defines clear standards and guidelines for industry compliance, consumer data protection, cybersecurity controls, and timely reporting of Cybersecurity Events, as defined by 23 NYCRR § 500.01(d), and was promulgated to strengthen cybersecurity and data protection for the industry and consumers, 23 NYCRR § 500.01;

WHEREAS, the Department conducted a full scope examination of OneMain's cybersecurity policies and procedures covering the period December 31, 2016, through March 31, 2020 (the "Examination"), and found deficiencies in compliance, internal controls, management, and technology systems;

WHEREAS, following the Examination, the Department began an enforcement investigation into whether OneMain's compliance programs comply with applicable New York State laws and regulations related to cybersecurity (the "Enforcement Investigation"); and

WHEREAS, through both the Examination and the Enforcement Investigation, the Department found that there were violations of the following sections of the Cybersecurity Regulation: (1) 23 NYCRR § 500.03, which requires all DFS-regulated entities ("Covered Entities") to implement and maintain a cybersecurity policy that is based on the Covered Entity's risk assessment and addresses business continuity and disaster recovery planning and resources; (2) 23 NYCRR § 500.07, which requires Covered Entities to limit user access privileges to electronic information resources ("Information Systems") that provide access to Nonpublic Information ("NPI"); (3) 23 NYCRR § 500.08, which requires Covered Entities to implement and maintain policies and procedures to protect Information Systems and NPI during application development and quality assurance operations; (4) 23 NYCRR § 500.10(a)(3), which requires

Covered Entities to provide cybersecurity personnel with cybersecurity training and verify that key cybersecurity personnel take steps to maintain current knowledge of changing cybersecurity threats and countermeasures; and (5) 23 NYCRR § 500.11(a), which requires Covered Entities to implement written policies and procedures that address, among other things, due diligence processes used to evaluate the adequacy of cybersecurity practices of third-party service providers.

NOW THEREFORE, in connection with an agreement to resolve this matter without further proceedings, the Department finds as follows:

THE DEPARTMENT'S FINDINGS

Introduction

1. The Superintendent of Financial Services is responsible for ensuring the safety and soundness of New York's financial systems and enforcing the various laws and regulations that are applicable to financial services licensees, including the New York Financial Services Law and the various regulations that have been promulgated thereunder.

2. The Department is the primary regulator of mortgage servicers and lenders for the State of New York.

3. The Superintendent has the authority to conduct investigations, bring enforcement proceedings, levy monetary penalties, and order injunctive relief against parties who have violated the relevant laws and regulations.

4. Among the Superintendent's many roles is a consumer protection function, which includes the critical protection of individuals' private and personally sensitive data from careless, negligent, or willful exposure by licensees of the Department.

5. To support this important role, the Superintendent's Cybersecurity Regulation places on each Covered Entity, including OneMain, an obligation to establish and maintain a cybersecurity program that is designed to detect and recover from Cybersecurity Events, as defined below, and protect the confidentiality and integrity of the Covered Entity's Information Systems, as well as any consumer NPI contained therein. 23 NYCRR §§ 500.01(c), 500.01(e), 500.01(g), 500.01(k), 500.02(b).

6. A "Cybersecurity Event" is an act or attempt, whether or not successful, to gain unauthorized access to information stored on an Information System or disrupt or misuse such Information System. 23 NYCRR § 500.01(d).

7. As part of its cybersecurity program, a Covered Entity must limit user access privileges to Information Systems that provide access to NPI and shall periodically review such access privileges. 23 NYCRR § 500.07.

8. Additionally, a Covered Entity shall implement and maintain policies and procedures to protect Information Systems and NPI during application development and quality assurance operations. 23 NYCRR § 500.08.

9. Further, a Covered Entity must use its own qualified cybersecurity personnel, or that of an affiliate or third-party service provider, sufficient to manage the Covered Entity's cybersecurity risks and to perform or oversee the performance of certain core cybersecurity functions. Moreover, a Covered Entity must provide cybersecurity personnel with cybersecurity updates and training and verify that key cybersecurity personnel take steps to maintain current knowledge of changing cybersecurity threats and countermeasures. 23 NYCRR § 500.10(a).

10. Finally, a Covered Entity shall implement written policies and procedures designed to ensure the security of Information Systems and NPI that are accessible to, or held by, third-party service providers. 23 NYCRR § 500.11.

OneMain's Cybersecurity Deficiencies

Cybersecurity Policy

11. Pursuant to 23 NYCRR § 500.03(e), Covered Entities are required to implement and maintain a written policy or policies to address their business continuity and disaster recovery planning and resources ("BCDR").

12. Through both the Examination and the Enforcement Investigation, the Department found that OneMain's BCDR was insufficient. To be adequate, a business impact analysis should document the Information System's requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption. Such documentation is the cornerstone of an effective BCDR strategy because it provides important information such as employee contact lists, emergency contact lists, vendor lists, instructions for performing tests, equipment lists, and technical diagrams of systems and networks. OneMain's BCDR was insufficient as it did not contain all of this information.

Access Privileges

13. Pursuant to 23 NYCRR § 500.07, Covered Entities are required to limit user access privileges to Information Systems that provide access to NPI and shall periodically review such access privileges.

14. In 2018 and 2019, OneMain's internal audit team found a number of issues related to user access privileges. For example, OneMain's Information Security unit manually

conducted privilege access reviews, introducing a high risk of human error that is unacceptable for a network with hundreds of applications and more than 11,000 users. The internal audit team also found that local administrative users shared accounts, compromising the ability to identify malicious actors, and that accounts still used the default password provided by OneMain at the time of user onboarding, increasing the risk of unauthorized access. Additionally, the internal audit team found that passwords were stored on department shared drives, where access was not adequately restricted. Although the file containing the passwords was encrypted and password-protected, it was stored in a folder named "PASSWORDS." Anyone with access to that internal shared drive, which included personnel in OneMain's call center, could rename, move, or delete the folder. This lack of protection could give a malicious actor or software easy access to the Company's Information Systems.

Application Security

15. Pursuant to 23 NYCRR § 500.08, Covered Entities must implement and maintain written policies and procedures to protect Information Systems and NPI during application development and quality assurance operations.

16. For a company like OneMain, which does extensive in-house application development and has its own application programming interfaces, these written policies and procedures must include a formalized methodology providing for all phases of a company's software development life cycle (*e.g.*, the secure design, creation, and maintenance of software, as well as quality assurance processes).

17. At the time of the Examination, OneMain lacked a formalized methodology. Instead, the Company was using a non-formalized project administration framework it had developed in-house that failed to address certain key software development life cycle phases, one

consequence of which was increased vulnerability to the kind of Cybersecurity Event described below in paragraph 25(c).

Cybersecurity Personnel and Intelligence Training

18. Pursuant to 23 NYCRR § 500.10(a)(3), Covered Entities are required to verify that key cybersecurity personnel take steps to maintain current knowledge of changing cybersecurity threats and countermeasures.

19. OneMain does extensive in-house application development and has created its own application programming interfaces. Nevertheless, as of the Examination, OneMain was not providing secure coding training for its developers. Training on secure coding helps developers identify security vulnerabilities in applications being developed and keep pace with the latest security threats.

20. Additionally, at the time of the Examination, OneMain did not effectively track or adequately implement training for its more than 500 information technology employees.

Third-Party Service Provider Security Policy

21. Pursuant to 23 NYCRR § 500.11(a), Covered Entities are required to implement written policies and procedures designed to ensure the security of Information Systems and NPI that are accessible to, or held by, third-party service providers. Such written policies and procedures also must include relevant guidelines for due diligence and contractual protections relating to third-party service providers' use of encryption and multi-factor authentication.

22. Although OneMain has a third-party vendor management policy that requires each of its vendors to undergo an assessment to determine the vendor's risk rating and the appropriate level of due diligence OneMain should perform on the vendor, the Company did not timely conduct due diligence for certain high-risk and medium-risk vendors, effectively

rendering such risk ratings moot for these vendors. For instance, OneMain allowed some of these third-party vendors to begin working at OneMain prior to the completion of OneMain's onboarding security questionnaire and third-party information security risk acceptance. Additionally, OneMain failed to appropriately adjust the risk scores of several vendors after the occurrence of multiple Cybersecurity Events precipitated by the vendors' improper handling of NPI and poor cybersecurity controls. Instead, OneMain simply terminated its relationship with each of the vendors and did so without simultaneously enhancing its own third-party service policies and procedures or due diligence processes.

Cybersecurity Events

23. Through the Examination and Enforcement Investigation, the Department found deficiencies in the Company's cybersecurity program, several of which had been previously identified by its own internal audit unit.

24. Specifically, OneMain's insufficient due diligence process prior to engaging third-party vendors and failure to properly monitor these vendors, as well as the Company's failure to ensure the use of secure development practices for in-house developed applications, made OneMain more vulnerable to instances of unauthorized access to customer NPI.

a. For example, from December 29, 2017, through January 9, 2018, a third-party vendor responsible for processing and managing online debit card payments gave some customers unauthorized access to other customers' NPI. This unauthorized access was a result of the vendor's failure to purge old customer account numbers before those account numbers were assigned to new customers.

b. Additionally, for an unknown duration during 2018, a hacker accessed the emails of OneMain's collections law firm, a third-party vendor, gaining access to emails between the Company and the law firm that contained customer

NPI.

c. And, on July 10, 2020, OneMain, using its online portal, sent a link containing code to hundreds of customers as part of the first stage of a software update roll out. Such code should have been thread safe*, i.e.*, designed and tested to ensure it performs only as intended. This code was not thread-safe, however, and certain customers who logged into their accounts were unintentionally migrated to other account holders' documents. This vulnerability resulted in the unauthorized access of loan documents containing NPI.

Violations of Law and Regulations

25. OneMain failed to implement and maintain written policies that adequately addressed its BCDR planning and resources, in violation of 23 NYCRR § 500.03(e).

26. OneMain failed to maintain and review user access privileges, in violation of 23 NYCRR § 500.07.

27. OneMain failed to implement policies and procedures that protected Information Systems and NPI during application development, in violation of 23 NYCRR § 500.08.

28. OneMain failed to provide its cybersecurity personnel with training sufficient to address relevant cybersecurity risks and failed to verify that key cybersecurity personnel take steps to maintain current knowledge of changing cybersecurity threats and countermeasures, in violation of 23 NYCRR § 500.10.

29. OneMain failed to ensure the security of the NPI that was accessible to, or held by, its third-party service providers, in violation of 23 NYCRR § 500.11(a).

NOW THEREFORE, to resolve this matter without further proceedings, the Department and the Company stipulate and agree to the following terms and conditions:

SETTLEMENT PROVISIONS

Monetary Penalty

30. No later than ten (10) days after the Effective Date (as defined below) of this Consent Order, the Company shall pay a total civil monetary penalty pursuant to Financial Services Law § 408 to the Department in the amount of Four Million, Two Hundred Fifty Thousand U.S. Dollars ($4,250,000.00). The payment shall be in the form of a wire transfer in accordance with instructions provided by the Department.

31. The Company shall not claim, assert, or apply for a tax deduction or tax credit with regard to any U.S. federal, state, or local tax, directly or indirectly, for any portion of the civil monetary penalty paid pursuant to this Consent Order.

32. The Company shall neither seek nor accept, directly or indirectly, reimbursement or indemnification with respect to payment of the penalty amount, including but not limited to, payment made pursuant to any insurance policy.

33. In assessing a penalty for failures in cybersecurity compliance, the Department has taken into account factors that include, without limitation: the extent to which the entity has cooperated with the Department in the Enforcement Investigation of such conduct, the gravity of the violations, and such other matters as justice and the public interest may require.

34. The Department acknowledges OneMain's cooperation throughout this Enforcement Investigation. The Department also recognizes and credits OneMain's ongoing efforts to remediate the shortcomings identified by the Department and to continuously improve

its cybersecurity program. Among other things, OneMain has demonstrated its commitment to remediation by devoting significant financial and other resources to its cybersecurity program.

Remediation

35. OneMain shall continue to strengthen and remediate its controls and procedures to protect its cybersecurity systems and consumers' NPI in accordance with the relevant provisions and definitions of 23 NYCRR Part 500. Within one hundred and eighty (180) days of the date of this Consent Order, OneMain shall have completed the following:

a. implemented a written policy to address BCDR planning and the maintenance of documentation;

b. implemented a plan to properly review and maintain user access privileges;

c. maintained and implemented written policies and procedures for the protection of the Company's Information Systems and the NPI stored on those Information Systems during application development;

d. implemented training procedures sufficient to address relevant cybersecurity risks and verify that key cybersecurity personnel have completed training sufficient to maintain current knowledge of changing cybersecurity threats and countermeasures; and

e. updated its policies and procedures to ensure protection of NPI that is accessible to, or held by, third parties

Action Plan

36. Within sixty (60) days of the completion of the remediation described above, OneMain shall submit the results of said remediation to the Department together with a detailed

Action Plan describing what steps OneMain plans to take to ensure the safety and security of its customers' NPI and compliance with the Cybersecurity Regulation

Full and Complete Cooperation

37. The Company commits and agrees that it will fully cooperate with the Department regarding all terms of this Consent Order.

Further Action by the Department

38. No further action will be taken by the Department against the Company or its successors for the conduct set forth in this Consent Order, or in connection with the remediation set forth in this Consent Order, provided that the Company fully complies with the terms of the Consent Order. Furthermore, no further action will be taken by the Department against the Company for conduct in connection with the Department's Enforcement Investigation.

39. Notwithstanding any other provision in this Consent Order, however, the Department may undertake additional action against the Company for transactions or conduct that were not disclosed in the written materials submitted to the Department in connection with this matter.

Waiver of Rights

40. The Company submits to the authority of the Superintendent to effectuate this Consent Order.

41. The parties understand and agree that no provision of this Consent Order is subject to review in any court, tribunal, or agency outside of the Department.

Parties Bound by the Consent Order

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

Breach of Consent Order

43. In the event that the Department believes the Company to be in material breach of the Consent Order, the Department will provide written notice to the Company, and the Company must, within ten (10) days of receiving such notice, or on a later date if so determined in the Department's sole discretion, appear before the Department to demonstrate that no material breach has occurred or, to the extent pertinent, that the breach is not material or has been cured

44. The Company understands and agrees that its failure to make the required showing within the designated time period shall be presumptive evidence of the Company's breach. Upon a finding that a breach of this Consent Order has occurred, the Department has all the remedies available to it under the New York Financial Services Law and any other applicable laws and may use any evidence available to the Department in any ensuing hearings, notices, or orders.

Notices

45. All notices or communications regarding this Consent Order shall be sent to:

For the Department:

Matthew T. Quinones
Assistant Deputy Superintendent
Consumer Protection and Financial Enforcement
New York State Department of Financial Services
1 State Street,
New York, NY 10004

Justin D. Parnes
Excelsior Fellow
Consumer Protection and Financial Enforcement
New York State Department of Financial Services
1 State Street,
New York, NY 10004

For OneMain Financial Group, LLC:

Joan M. Loughnane
Michal D. Mann
Partners
Sidley Austin LLP
787 Seventh Avenue
New York, NY 10019

Colleen T. Brown
Partner
Sidley Austin LLP
1501 K. Street, N.W.
Washington, D.C. 20005

Miscellaneous

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

47. This Consent Order may not be altered, modified, or changed unless in writing and signed by the parties hereto

48. This Consent Order constitutes the entire agreement between the Department and the Company and supersedes any prior communication, understanding, or agreement, whether written or oral, concerning the subject matter of this Consent Order.

49. Each provision of this Consent Order shall remain effective and enforceable against the Company, its successors, and assigns, until stayed, modified, suspended, or terminated by the Department.

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

51. No promise, assurance, representation, or understanding other than those contained in this Consent Order has been made to induce any party to agree to the provisions of this Consent Order.

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

53. This Consent Order may be executed in one or more counterparts and shall become effective when such counterparts have been signed by each of the parties hereto (the "Effective Date").

[*remainder of this page intentionally left blank*]

IN WITNESS WHEREOF, the parties have caused this Consent Order to be signed on the dates set forth below.

NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES

By: /s/ Elizabeth A. Farid
ELIZABETH A. FARID
Senior Assistant Deputy Superintendent for Consumer Protection and Financial Enforcement

May 18, 2023

By: /s/ Alison L. Passer
ALISON L. PASSER
Deputy Director of Enforcement Consumer Protection and Financial Enforcement

May 18, 2023

By: /s/ Kevin R. Puvalowski
KEVIN R. PUVALOWSKI
Acting Executive Deputy Superintendent for Consumer Protection and Financial Enforcement

May 19, 2023

ONEMAIN FINANCIAL GROUP, LLC

/s/ Micah R. Conrad
MICAH R. CONRAD
Chief Financial Officer, Executive Vice President
OneMain Financial Group, LLC

May 18, 2023

THE FOREGOING IS HEREBY APPROVED. IT IS SO ORDERED.

/s/ Adrienne A. Harris
ADRIENNE A. HARRIS
Superintendent of Financial Services

May 24, 2023