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

----------x

In the Matter of :

ROCKET MORTGAGE, LLC :

----------x

CONSENT ORDER

The New York State Department of Financial Services (the "Department" or "DFS") and Rocket Mortgage, LLC ("Rocket Mortgage" or the "Company") are willing to resolve the matters described herein without further proceedings.

WHEREAS, Rocket Mortgage is licensed by the Department to provide mortgage lending in New York;

WHEREAS, August 29, 2017, marked the initial effective date of New York's first-in the-nation cybersecurity regulation, 23 NYCRR Part 500 (the "Cybersecurity Regulation")[1];

WHEREAS, the Cybersecurity Regulation defines clear standards for cooperative

[1] All citations to 23 NYCRR Part 500 herein refer to the Cybersecurity Regulation as it read prior to November 1, 2023.

industry compliance, robust consumer data protection, vital cybersecurity controls, timely reporting of Cybersecurity Events, as defined by 23 NYCRR § 500.1(d), and was promulgated to strengthen cybersecurity and data protection for the industry and consumers;

WHEREAS, Rocket Mortgage experienced seven Cybersecurity Events at the hands of threat actors between December 2019 and August 2021;

WHEREAS, Rocket Mortgage failed to report these Cybersecurity Events to the Department in a timely manner, and the Department first learned of six of the incidents during an onsite supervisory examination of the Company;

WHEREAS, following a supervisory examination the Department initiated an investigation of these Cybersecurity Events and Rocket Mortgage's compliance with the Cybersecurity Regulation; and

WHEREAS, based on the investigation, the Department concluded that Rocket Mortgage violated the following sections of the Cybersecurity Regulation: (1) 23 NYCRR § 500.12, which requires Covered Entities to use effective controls, including multi-factor authentication, to protect against unauthorized access to NPI or Information Systems; (2) 23 NYCRR 500.13, which requires Covered Entities to maintain policies and procedures for the secure disposal on a periodic basis of NPI; and (3) 23 NYCRR §500.17(a) and (b), which require all Covered Entities to notify the Department within 72 hours of determining that a reportable Cybersecurity Event has occurred.

NOW THEREFORE, to resolve this matter without further proceedings pursuant to the Superintendent's authority under Section 408 of the New York Financial Services Law, the Department finds as follows:

THE DEPARTMENT'S FINDINGS

Introduction

1. The Department is the primary regulator of mortgage servicers and lenders for the State of New York, and the Superintendent of Financial Services 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.

2. Among the Superintendent's many obligations to the public is a consumer protection function, which includes the protection of individuals' private and personally sensitive data from exposure by licensees of the Department.

3. To support this critical obligation to consumers, the Superintendent's Cybersecurity Regulation places on all Covered Entities an obligation to establish and maintain a cybersecurity program designed to protect the confidentiality, integrity, and availability of its Information Systems and NPI, as defined in 23 NYCRR §§ 500.1(e) and 500.1(g), respectively.

4. Timely reporting to the Department is essential to promote early awareness of emerging threats to regulated entities and the broader financial system, enabling the Department to assess the potential impact of threats, respond proactively, and provide timely guidance to industry to help mitigate risks before they escalate.

5. The Cybersecurity Regulation further requires Covered Entities to address data privacy and other consumer protection issues with effective controls such as multi-factor

authentication, secure data disposal, and timely notifications of Cybersecurity Events. 23 NYCRR §§ 500.12, 500.13, 500.17(a).

Failure to Timely Report Cyber Events

6. 23 NYCRR § 500.17(a)(1) requires Covered Entities to notify the Department of Cybersecurity Events within 72 hours of a determination that a Cybersecurity Event has occurred, when notice is required to be provided to any government body, self-regulatory agency, or any other supervisory body.

7. On October 4, 2021, examiners from the Department's Cybersecurity Division commenced an examination of Rocket Mortgage for the period of January 1, 2018, through March 31, 2021 (the "review period"). Prior to the DFS examination, Rocket Mortgage was advised that the examination would encompass a general compliance safety and soundness review, as well as compliance with the Cybersecurity Regulation. Furthermore, Rocket Mortgage was advised that the latter review would include review of Rocket Mortgage's cybersecurity program, and the details of any Cybersecurity Events that had occurred during the review period, pursuant to Sections 500.2 and 500.17 of the Cybersecurity Regulation.

8. During the DFS examination, examiners sought to confirm that Rocket Mortgage had submitted all required notices of a Cybersecurity Event to DFS during the review period. In response, and for the first time, the Company reported six of the Cybersecurity Events described below, some of which had occurred nearly 18 months earlier.

9. Each of the seven Cybersecurity Events was caused by a business email compromise conducted by an external threat actor and executed through social engineering of Rocket Mortgage employees to provide email account login credentials. A business email

compromise is a specific type of email fraud that has the goal of stealing funds or critical information from personnel.

10. In three instances, the threat actor obtained access to multiple employees' email accounts. The threat actor then initiated a login attempt, which sent a multi-factor authentication notification to the employee in the form of a phone call with a push-based prompt.[2] The employees approved the multi-factor authentication phone prompts, allowing the threat actor access to their email accounts.

11. In another three instances, the threat actor was able to gain access to the email accounts without going through multi-factor authentication, due to a software migration gap outlined in the following section.

12. Rocket Mortgage did not report six of the Cybersecurity Events to DFS until *after* DFS discovered them during the October 2021 examination and reported the seventh Cybersecurity Event in the course of responding to DFS enforcement investigation requests in May 2022.

13. Below is the list of Cybersecurity Events that Rocket Mortgage failed to report to DFS timely:

a. Cybersecurity Event V96001 began on January 6, 2020, and the last of four affected email inboxes was accessed on January 15, 2020. Rocket Mortgage discovered each instance of unauthorized access within 24 hours of occurrence. The Company notified DFS on October 26, 2021.

[2] Push-based MFA only requires a user to accept an on-screen prompt or press a button in response to an automated phone call. Push-based MFA is more susceptible to human error than token-based MFA. *See* New York Department of Financial Services, *Industry Letter - December 7, 2021: Guidance on Multi-Factor Authentication*, Dec. 7, 2021, https://www.dfs.ny.gov/industry_guidance/industry_letters/il20211207_mfa_guidance.

b. Cybersecurity Event V96002 occurred on April 24, 2020. Rocket Mortgage discovered unauthorized access to two email accounts on the same day. The Company notified DFS on October 26, 2021.

c. Cybersecurity Event V96003 occurred on June 29, 2020. Rocket Mortgage discovered the unauthorized access to a company email inbox on the same day. The Company notified DFS on October 26, 2021.

d. Cybersecurity Event V96004 occurred on January 6, 2021. Rocket Mortgage discovered the unauthorized access to two email inboxes on January 8, 2021. The Company notified DFS on October 26, 2021.

e. Cybersecurity Event V96005 occurred on April 16, 2021, and Rocket Mortgage discovered the unauthorized access to an email inbox the same day. The Company notified DFS on October 26, 2021.

f. Cybersecurity Event V96006 occurred on August 8, 2021, and Rocket Mortgage discovered the unauthorized access to two email inboxes the same day. The Company notified DFS on October 26, 2021.

g. Cybersecurity Event V108403 occurred and was discovered by Rocket Mortgage on December 18, 2019. The Company did not report the event to DFS until May 23, 2022.

Multi-Factor Authentication Gap

14. Section 500.12 of the Superintendent's Cybersecurity Regulation requires Covered Entities to implement multi-factor authentication, or reasonably equivalent or more secure access controls approved in writing by the Covered Entity's Chief Information Security Officer, for any external access to a Covered Entity's internal network. 23 NYCRR §§ 500.1(f),

500.12. Multi-Factor Authentication requires more than one distinct authentication factor for successful access, such that a username and password alone are not sufficient to access an email account and its contents. Multi-factor authentication is an additional layer of security that safeguards against attempts to gain unauthorized access, including those made by threat actors using credentials or other access obtained through phishing emails. Phishing emails are sent by cyber criminals aiming to deceive users into providing personal details or other confidential information, thereby facilitating unauthorized access or causing harm to a protected Information System.

15. In August 2019, Rocket Mortgage completed the implementation of a company-wide upgrade to Microsoft Office 365 ("O365") that had begun in January 2017. Following this migration, the Company acknowledged that, due to configuration issues related to the O365 upgrade by Microsoft, its "system was vulnerable to multi-factor authentication workarounds."

16. Due to configuration issues related to the O365 upgrade by Microsoft, there was a gap in multi-factor authentication usage, and Rocket Mortgage lacked compensating controls during the gap. During this gap, O365 access was not protected by multi-factor authentication or reasonably equivalent or more secure access controls, as required by Section 500.12(b) of the Cybersecurity Regulation. As a result, in the V108403, V96001 and V96004 Cybersecurity Events threat actors were able to gain access to the network without any multi-factor authentication.

Secure Disposal of Nonpublic Information Policy

17. Section 500.13 of the Cybersecurity Regulation requires all Covered Entities to maintain policies and procedures for the secure, periodic disposal of NPI that is no longer necessary for business operations or for other legitimate business purposes of the Covered Entity.

The secure disposal of NPI that is no longer necessary is an important way to minimize the amount of consumer data that is accessible on a company's Information Systems at any given time, thereby limiting the harm of any unauthorized access. Until December 2020, Rocket Mortgage did not have written policies and procedures in place that described the Company's practices for the periodic secure disposal of NPI that was no longer necessary for business operations or other legitimate business purposes, in violation of 500.13.

18. Rocket Mortgage's IT security policy, dated February 14, 2019, did not have a written section detailing procedures for secure disposal of NPI.

19. The IT Security Policy stated "Storage of Sensitive information on Systems must be kept to a minimum. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purpose." The Company's policy was insufficiently detailed on the identification and deletion process of NPI to provide adequate protection to Rocket's systems and the NPI stored therein.

20. Prior to December 2020, Rocket Mortgage's written policy did not provide a process for classifying and purging sensitive data, including NPI, that was no longer necessary to store or provide any guidance on how such data should periodically be disposed of, despite the requirements of 23 NYCRR § 500.13.

Violations of Law and Regulations

21. Rocket Mortgage failed to implement multi-factor authentication or reasonably equivalent or more secure access controls, in violation of 23 NYCRR § 500.12(b).

22. Rocket Mortgage did not have policies and procedures in place for the periodic secure disposal of NPI that was no longer necessary for business operations or other legitimate business purposes, in violation of 23 NYCRR § 500.13.

23. Rocket Mortgage failed to timely notify the Department of the Cybersecurity Events, in violation of 23 NYCRR § 500.17(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

24. 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 two million dollars and 00/100 cents ($2,000,000). The payment shall be in the form of a wire transfer in accordance with instructions provided by the Department.

25. 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.

26. 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.

27. In assessing a penalty for failures in cybersecurity compliance, the Department has taken into account factors that include, without limitation: the material failure of the Company to timely comply with its notice requirements, the repeated nature of the Company's failure to comply with its notice requirements, the number of violations and the length of time over which they occurred, the extent to which the entity has cooperated with the Department in

the investigation of such conduct, the gravity of the violations, and such other matters as justice and the public interest may require.

Remediation

28. The Company shall continue to strengthen its controls to protect its information systems and NPI in accordance with the requirements of the Cybersecurity Regulation. Within ninety (90) days of the Effective Date of this Consent Order, the Company (either itself or through an independent, third-party professional engaged by the Company) shall conduct an audit of current MFA controls related to the: (1) integrated infrastructure in which Rocket Mortgage operates; and (2) shared systems that support Rocket Mortgage's core business functions, such as O365 (the "MFA Audit"). The scope of the MFA Audit must include a review of any MFA exceptions, CISO review of the reasonably equivalent or more secure compensating controls associated with these exceptions, as well as the CISO's written approval of any exceptions.

29. Following the completion of the audit, Rocket Mortgage shall report the results of the MFA Audit ("MFA Audit Report") to the Department. The MFA Audit Report shall include a description of any exceptions to MFA, an explanation of any reasonably equivalent or more secure compensating controls associated with the exceptions, along with the CISO's written approval of any exceptions.

30. To the extent Rocket Mortgage identifies material issues in the MFA Audit, Rocket Mortgage will remediate those issues within a reasonable timeframe agreed to by the Department. Rocket Mortgage will provide proof of remediation to the Department upon completion.

31. The Company shall maintain a written incident response policy that addresses documentation and reporting regarding cybersecurity incidents and related incident response activities, including reporting requirements applicable to the Department.

Full and Complete Cooperation

32. 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

33. 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.

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

Waiver of Rights

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

36. 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

37. 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

38. 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.

39. 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 Banking and Financial Services Laws, and any other applicable laws, and may use any evidence available to the Department in any ensuing hearings, notices, or orders.

Notices

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

For the Department:

Elizabeth A. Farid
Senior Enforcement Counsel
Consumer Protection and Financial Enforcement Division
New York State Department of Financial Services
One State Street
New York, New York 10004

Daniel F. Schiano
Enforcement Counsel
Consumer Protection and Financial Enforcement Division
New York State Department of Financial Services
One State Street
New York, New York 10004

For Rocket Mortgage:

Amy Bishop
Executive Vice President, Deputy Legal Officer - Regulatory Legal, Compliance
Rocket Mortgage
1050 Woodward Avenue,
Detroit, MI 48226

Miscellaneous

41. 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.

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

43. 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.

44. 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.

45. 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.

46. 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.

47. 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.

48. 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 Enforcement Counsel
Consumer Protection and Financial Enforcement

November 19, 2026

By: /s/ Daniel F. Schiano
DANIEL F. SCHIANO
Enforcement Counsel
Consumer Protection and Financial Enforcement

November 19, 2026

By: /s/ Christopher B. Mulvihill
CHRISTOPHER B. MULVIHILL
Deputy Superintendent for Consumer Protection
and Financial Enforcement

November 19, 2026

By: /s/ R. Gabriel D. O'Malley
R. GABRIEL D. O'MALLEY
Executive Deputy Superintendent for Consumer
Protection and Financial Enforcement

November 19, 2026

ROCKET MORTGAGE, LLC

By: /s/ Amy Bishop
AMY BISHOP
Rocket Mortgage, LLC

November 16, 2026

THE FOREGOING IS HEREBY APPROVED. IT IS SO ORDERED.

/s/ Kaitlin Asrow
Kaitlin Asrow
Acting Superintendent of Financial Services

November 19, 2026