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

----------x

In the Matter of :

ROCKET MORTGAGE, LLC :
as successor in merger to
NATIONSTAR MORTGAGE LLC d/b/a MR. COOPER :

----------x

CONSENT ORDER

The New York State Department of Financial Services (the "Department" or "DFS") and Rocket Mortgage, LLC as successor in merger to Nationstar Mortgage LLC d/b/a Mr. Cooper ("Mr. Cooper" or the "Company") are willing to resolve the matters described herein without further proceedings.

WHEREAS, Mr. Cooper was licensed by the Department as a mortgage loan servicer and mortgage banker;[1]

[1] Nationstar Mortgage LLC d/b/a Mr. Cooper merged with and into Rocket Mortgage, LLC on February 2, 2026. Mr. Cooper surrendered its licenses on February 4, 2026, as part of this acquisition. It is for that reason that Rocket Mortgage, LLC, as successor by merger to Nationstar Mortgage LLC d/b/a Mr. Cooper, will be executing this consent order.

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"). In April 2020, the Department first amended the Cybersecurity Regulation; the Department again amended the Cybersecurity Regulation on November 1, 2023;[2]

WHEREAS, the Cybersecurity Regulation defines clear standards for cooperative industry compliance, robust consumer data protection, vital cybersecurity controls, and timely notification of reportable 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, the Department has been investigating a Cybersecurity Event experienced by Mr. Cooper, as well as Mr. Cooper's compliance with the Cybersecurity Regulation; and

WHEREAS, based on the investigation the Department has concluded that Mr. Cooper violated the following sections of the Cybersecurity Regulation: (1) 23 NYCRR § 500.2, which requires Covered Entities to design a cybersecurity program sufficient to identify and assess risks to Non-Public Information ("NPI"), use defensive infrastructure, and implement policies and procedures to protect NPI; (2) 23 NYCRR § 500.3(d), which requires Covered Entities to implement and maintain an adequate cybersecurity policy setting forth procedures for the protection of NPI and information systems; (3) 23 NYCRR § 500.9, which requires a Covered Entity to conduct a periodic Risk Assessment sufficient to inform the design of the cybersecurity program; and (4) 23 NYCRR § 500.12, which requires Covered Entities to implement Multi-Factor Authentication ("MFA") or alternative effective controls to prevent unauthorized access to NPI.

[2] Citations and other references to 23 NYCRR Part 500 herein refer to the Cybersecurity Regulation as it read prior to November 1, 2023.

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

THE DEPARTMENT'S FINDINGS[3]

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 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.

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

4. To support this critical obligation, the Cybersecurity Regulation places on all DFS-regulated entities ("Covered Entities"), including Mr. Cooper, an obligation to establish and maintain a cybersecurity program based on a risk assessment and designed to protect the confidentiality, integrity, and availability of its Information Systems and NPI contained therein. 23 NYCRR §§ 500.1(c), 500.1(e), 500.1(g), 500.1(k), 500.2(b).

5. 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 § 500.1(d).

[3] The Department's findings describe events and conduct that occurred prior to Rocket Mortgage, LLC's merger with Nationstar Mortgage, LLC d/b/a Mr. Cooper.

6. The Cybersecurity Regulation requires that Covered Entities identify and assess risks to stored NPI, and implement defensive infrastructure and policies designed to protect against unauthorized access, use, or other malicious acts. 23 NYCRR §§ 500.2(b), 500.3, 500.9.

7. In particular, a Covered Entity's cybersecurity policy must address information security and access controls, in order to protect NPI stored on the Covered Entity's Information Systems from unauthorized access. 23 NYCRR § 500.3(d).

8. A Covered Entity's cybersecurity program and policy shall be based on the Covered Entity's Risk Assessment. 23 NYCRR §§ 500.2, 500.3, 500.9. The Risk Assessment shall be updated as reasonably necessary and must include criteria for the evaluation and categorization of identified cybersecurity risks or threats, criteria for the assessment of the adequacy of controls for the Covered Entity's information systems and NPI in its possession, and requirements describing how risks will be mitigated or accepted and addressed. 23 NYCRR § 500.9.

9. To secure and protect NPI and prevent Cybersecurity Event(s), Covered Entities must "use effective controls, which may include [MFA] or risk-based authentication, to protect against unauthorized access to [NPI] or Information Systems." 23 NYCRR § 500.12(a).

10. MFA requires a minimum of two different categories of authentication methods: (1) knowledge factors, such as a password; (2) possession factors, such as a token; or (3) inherence factors, such as a biometric characteristic. 23 NYCRR § 500.1(f).[4] Two of the same category of authentication factor is insufficient to qualify as MFA.

[4] In the Second Amendment to the Cybersecurity Regulation, this definition has been renumbered 23 NYCRR § 500.1(j).

Events at Issue

The Cybersecurity Event

11. On November 2, 2023, Mr. Cooper filed notice with the Department of an ongoing cybersecurity event involving unidentified threat actors accessing Mr. Cooper's Information Systems (the "Cybersecurity Event"). The notice to the Department indicated that the Cybersecurity Event caused a disruption to Mr. Cooper's business operations.

12. On October 30, 2023, a threat actor (the "Threat Actor"), initiated a series of telephone calls to Mr. Cooper's Help Desk impersonating IT employees, requesting a password reset each time. Eventually, a Help Desk employee reset the password to the impersonated employee's account after the Threat Actor provided the name and last four digits of the employee's Social Security number as identity verification, consistent with Mr. Cooper's written Help Desk procedures then in effect, and verbally shared a new, temporary password with the Threat Actor.

13. Using the impersonated employee's username (a publicly available email address) and the new temporary password, the Threat Actor logged into Zscaler Internet Access ("Zscaler").[5] Logging on to Zscaler caused the Threat Actor's traffic to originate from IP ranges associated with Zscaler that had been configured as trusted locations pursuant to Mr. Cooper's conditional access rules.

14. Once logged on to Zscaler, the Threat Actor accessed LogMeIn, a cloud-hosted remote desktop access application used by Mr. Cooper's IT staff to service other employees' desktops and other endpoints. The compromised employee's account held administrator privileges for LogMeIn. Because the Threat Actor had a Zscaler-associated IP address that was

[5] Zscaler is a cloud security solution used by Mr. Cooper to manage remote access to certain applications.

considered a trusted location, the Threat Actor was granted access to LogMeIn without triggering an MFA check.

15. Once inside Mr. Cooper's Information Systems via LogMeIn, the Threat Actor used social engineering and other methods to gain access to Mr. Cooper's network. The Threat Actor then exfiltrated certain personal data of substantially all of Mr. Cooper's current and former customers before deploying ransomware. In response, Mr. Cooper shut down its Information Systems. Mr. Cooper removed the Threat Actor from its Information Systems on November 2, 2023, and restored full system access on November 4, 2023.

16. Mr. Cooper informed all affected individuals of the Cybersecurity Event, cooperated with the Department's investigation, and worked with various law enforcement agencies.

17. Mr. Cooper's failure to protect NPI stored within its Information Systems resulted in the exposure of millions of individuals' Social Security numbers, dates of birth, and other NPI, including those of hundreds of thousands of New York residents. Additionally, Mr. Cooper's online business operations were disrupted for five days, leaving many customers temporarily without access to their accounts.

Protection of NPI

18. The Cybersecurity Regulation requires a Covered Entity to protect NPI stored on and/or accessible through its Information Systems.

19. Section 500.2(b) of the Cybersecurity Regulation requires that Covered Entities "identify and assess internal and external cybersecurity risks that may threaten the security or integrity of Nonpublic Information" and "use defensive infrastructure and the implementation of policies and procedures to protect… [NPI] stored on [the Covered Entity's] Information

Systems, from unauthorized access." 23 NYCRR § 500.2(b). Additionally, Section 500.3(d) of the Cybersecurity Regulation requires that Covered Entities implement and maintain policies that address access controls and identity management.

20. In further support of the requirements laid out in Section 500.2(b) of the Cybersecurity Regulation, Section 500.12 requires Covered Entities to use "effective controls, which may include [MFA] or risk-based authentication, to protect against unauthorized access to [NPI] or information systems." 23 NYCRR § 500.12(a). Section 500.12(b) further requires that MFA be utilized for any individual's access to an internal network from an external network.

21. To log in to Mr. Cooper's Information Systems at the time of the Cybersecurity Event, a user needed, at minimum, a username, comprised of publicly available employee email addresses, and password.

22. If an employee lost or forgot their password, the employee could contact Mr. Cooper's IT Help Desk for assistance in resetting the password. Before resetting any password, the IT employee staffing the Help Desk was required to verify the identity of the requester by confirming who the employee was and requiring the employee to correctly provide identifying information. Mr. Cooper's written Help Desk procedures in effect at the time of the Cybersecurity Event provided that identity could be verified by confirming the employee's company ID number or the last four digits of the employee's Social Security number. Upon successful authentication, the Help Desk provided the employee with a temporary password.

23. At the time of the Cybersecurity Event, Mr. Cooper's Information Security Policy required MFA for remote access to its corporate network.

24. Mr. Cooper's conditional access rules governing access to certain applications, including LogMeIn, were configured to deny requests originating from external IP addresses.

However, the rules permitted access requests from IP ranges associated with Zscaler. When a user connected through Zscaler, that user's traffic originated from a Zscaler-associated IP address within the trusted ranges. As a result, the conditional access rules identified the user's access requests as originating from a trusted location, and approved them without triggering an MFA prompt.

25. Using the impersonated employee's credentials and administrator privileges for LogMeIn, the Threat Actor accessed LogMeIn and connected to a workstation within Mr. Cooper's corporate network. From that workstation, the Threat Actor used social engineering and other methods, then escalated privileges, moved laterally, and exfiltrated consumer data including names, Social Security numbers, and dates of birth.

Risk Assessments

26. Section 500.9 of the Cybersecurity Regulation requires that "[e]ach Covered Entity . . . conduct a periodic Risk Assessment of the Covered Entity's Information Systems sufficient to inform the design of the cybersecurity program as required by this Part." 23 NYCRR § 500.9(a).

27. Furthermore, Section 500.2(b) of the Cybersecurity Regulation further emphasizes the importance of the Risk Assessment and enumerates additional areas which the Covered Entity's cybersecurity program must address. In relevant part, Section 500.2(b) requires a Covered Entity's cybersecurity program to "(1) identify and assess internal and external cybersecurity risks that may threaten the security or integrity of [NPI] stored on the Covered Entity's Information Systems; [and] (2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the [NPI]

stored on those Information Systems, from unauthorized access, use or other malicious acts." 23 NYCRR § 500.2(b).

28. Mr. Cooper conducted a Cybersecurity Risk Assessment in 2021. The Company began its next Cybersecurity Risk Assessment in 2023 but did not complete it until 2025. The Company attributes the delay in completion to the 2023 Cybersecurity Event. However, a four-year gap between finalized risk assessments falls well short of the "periodic" requirement contained in Section 500.9 of the Cybersecurity Regulation, and is not frequent enough to adequately identify and respond to the cybersecurity risks faced by a company of Mr. Cooper's size.

Violations of Law and Regulations

29. Mr. Cooper failed to maintain a cybersecurity program designed to identify and assess internal and external risks that may threaten the security or integrity of NPI stored on its information systems, and to use defensive infrastructure and implement policies and procedures to protect its NPI stored on its information systems from unauthorized access, in violation of 23 NYCRR § 500.2(b).

30. Mr. Cooper failed to ensure proper implementation of its cybersecurity policy requiring MFA for remote access to its corporate network, in violation of 23 NYCRR § 500.3(d).

31. Mr. Cooper failed to use MFA or other effective controls to protect against unauthorized access to NPI and failed to have MFA in place for external access to the Company's internal network, in violation of 23 NYCRR § 500.12.

32. Mr. Cooper failed to conduct periodic risk assessments, in violation of 23 NYCRR § 500.9.

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

33. 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 New York Financial Services Law § 408 to the Department in the amount of Four Million Seven Hundred and Fifty Thousand Dollars and 00/100 Cents ($4,750,000). The payment shall be in the form of a wire transfer in accordance with instructions provided by the Department.

34. 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.

35. 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.

36. In assessing a penalty for the Company's 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 investigation of such conduct, sanctions imposed by other regulatory agencies, the gravity of the violations, and such other matters as justice and the public interest may require.

37. The Department acknowledges the Company's cooperation with the Department's investigation.

Remediation

38. 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 Mr. Cooper operates; and (2) shared systems that support Mr. Cooper'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.

39. Following the completion of the audit, Mr. Cooper 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 exception.

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

Full and Complete Cooperation

41. 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

42. 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.

43. 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

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

45. 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

46. 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

47. 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.

48. 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

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

For the Department:

Joseph Mineo
Enforcement Counsel
Consumer Protection and Financial Enforcement Division
One Commerce Plaza, 20th Floor
Albany, New York 12257

John Nicosia
Senior Enforcement Counsel
Consumer Protection and Financial Enforcement Division
One State Street, 20th Floor
New York, New York 10004

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

Miscellaneous

50. 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.

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

52. 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.

53. 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.

54. 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.

55. 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.

56. 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.

57. 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").

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/ Daniel Schiano
DANIEL SCHIANO
Enforcement Counsel
Consumer Protection and Financial Enforcement

November 19, 2026

By: /s/ Madeline W. Murphy
MADELINE W. MURPHY
Assistant Deputy Superintendent
Consumer Protection and Financial Enforcement

November 19, 2026

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

November 19, 2026

ROCKET MORTGAGE, LLC, AS SUCCESSOR BY MERGER TO NATIONSTAR MORTGAGE LLC d/b/a MR. COOPER

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

November 17, 2026

THE FOREGOING IS HEREBY APPROVED. IT IS SO ORDERED.

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

November 19, 2026