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

NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES

In the Matter of

RESIDENTIAL MORTGAGE SERVICES, INC.

CONSENT ORDER PURSUANT TO NEW YORK BANKING LAW §§ 44 and 44-a

The New York State Department of Financial Services (the "Department" or "DFS"), and Residential Mortgage Services, Inc. ("Residential Mortgage") (together, the "Parties") agree to resolve the matters described herein without further proceedings.

INTRODUCTION

August 29, 2017 marked the effective date of New York's first-in-the-nation cybersecurity regulation, 23 NYCRR 500 ("Cybersecurity Regulation"). The Department's Cybersecurity Regulation was designed to address significant issues of cybersecurity and

protect the financial services industry and consumers from the ever-increasing threat of data breaches and cyberattacks.

The regulation's clearly-defined standards for cooperative industry compliance, robust consumer data protection, vital cybersecurity controls, timely reporting of cybersecurity events (as defined herein), and enforcement were promulgated to strengthen cybersecurity and data protection for industry and consumers.

By agreeing to the terms of this Consent Order the Parties acknowledge that failures to conduct business in accordance with such standards require immediate remediation and imposition of a civil monetary penalty.

BACKGROUND

WHEREAS, Residential Mortgage, headquartered in South Portland, Maine, has been licensed by the Department as a Mortgage Banker since June 5, 2017, pursuant to Article 12D of the New York State Banking Law (the "Banking Law") and, since then, has been subject to the Banking Law's provisions and the provisions of all of its attendant regulations;

WHEREAS, with approval of the Department on December 12, 2018, Residential Mortgage also became an exempt mortgage loan servicer in New York State;

WHEREAS, Residential Mortgage has designated a Chief Information Security Officer ("CISO") to assume responsibility for regulatory compliance. A CISO must have verifiable "knowledge of changing cybersecurity threats and countermeasures" and must, *inter alia,* enact and implement the critical elements of a safe and sound cybersecurity program, including a comprehensive risk assessment and a reporting system for

cybersecurity incidents. Typically, the CISO is designated by a Department licensee to complete an annual certification on behalf of the licensee to confirm that the institution was compliant with the Cybersecurity Regulation during the previous year, and provides DFS with notice of Cybersecurity Events when appropriate and within 72 hours of determining their occurrences;

WHEREAS, on April 3, 2020, to certify compliance during the prior year with all relevant components of the Cybersecurity Regulation, Residential Mortgage's CISO filed a certification of compliance pursuant to 23 NYCRR Part 500.17(b).

WHEREAS, in 2019, Residential Mortgage closed 13,973 residential mortgage loans;

WHEREAS, between March 30 and August 7, 2020, examiners of the Department conducted a safety and soundness examination of Residential Mortgage and discovered significant failures in compliance and reporting required under Sections 44 and 44-a of the Banking Law;

WHEREAS, upon examination and further investigation undertaken by the Department, serious failures in compliance and reporting were discovered in connection with the Department's Cybersecurity Regulation;

NOW THEREFORE the following findings of fact are made:

FINDINGS OF FACT

1. Licensees of the Department, including Residential Mortgage, are subject to routine safety and soundness examinations by the Department to ensure compliance with applicable provisions of the New York State Banking Law, Financial Services Law, and

their attendant regulations. Prior to examination, a so-called First-Day Letter provides notice to licensees of the particular areas of compliance to be examined. A First-Day Letter provides licensees with notice of the scope of an impending examination and permits institutions to prepare for the examiners' questions and requests for supporting documentation.

The DFS Examination

2. On March 30, 2020, examiners of the Department's Mortgage Banking Division commenced examination of Residential Mortgage for the period of January 1, 2017 through December 31, 2019 (the "Review Period"). Prior to the DFS examination, Residential Mortgage was advised the examination would encompass a general compliance safety and soundness review, as well as compliance with the Cybersecurity Regulation. Furthermore, Residential Mortgage was advised the latter would include review of Residential Mortgage's cybersecurity risk assessment(s), and the details of any Cybersecurity Events that had occurred during the review period, pursuant to Sections 500.09, and 500.17 of the Cybersecurity Regulation.

3. 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). Licensees must file notice of a Cybersecurity Event with the Department pursuant to the requirements of 23 NYCRR 500.17(a)(1) and (a)(2). In particular, Part 500.17(a)(1) requires notice to the Superintendent, within 72 hours of determining there has been a Cybersecurity Event, when notices are "required to be provided to any government body, self-regulatory agency or any other supervisory body."

4. During the DFS examination, examiners sought to confirm that Residential Mortgage had not submitted any notice of a Cybersecurity Event with DFS during the Review Period. In response, and for the first time, Residential Mortgage's CISO disclosed to the DFS examiners an apparent Cybersecurity Event which occurred nearly 18 months earlier. The Cybersecurity Event, described more fully below, was an email compromise, or unauthorized access to an employee's Residential Mortgage email account. Residential Mortgage, by its own admission, never fully investigated this Cybersecurity Event.

The March 5, 2019 Cybersecurity Event

5. On March 6, 2019, Residential Mortgage learned that the email account of an employee who collects a substantial amount of sensitive personal data from mortgage loan applicants ("Employee"), was compromised by an unauthorized intruder the prior day. On the afternoon of March 5, Employee had responded to a phishing email, one bearing the false appearance of originating from a business partner.

6. In its simplest form, a phishing email is one sent by a cyber criminal to deceive a user into providing personal details or other confidential information, such as a password, to permit unauthorized access or harm to a protected information system. In the instant case, the phishing email contained a hyperlink to a malicious website, which Employee "clicked on," or "followed." Upon arrival at the malicious website, Employee was prompted to provide her Residential Mortgage email credentials (*i.e.,* the username and password required to log in to her Residential Mortgage email account), and she did.

7. To protect staff email accounts from unauthorized access, such as those that follow successful phishing attempts, Residential Mortgage had instituted multi-factor authentication ("MFA"). MFA requires more than one distinct authentication factor for

successful access. Accordingly, Employee's username and password alone were not sufficient to provide the cyber criminal with remote access to her email account and its contents. To allow access, Employee also had to provide a second means of authentication. In this instance, Employee did so by tapping the screen of her smartphone to give her approval in response to an alert from an MFA application on her phone; notice that someone was seeking approval to login to her email account.

8. On the evening of March 5, 2019, Employee tapped her phone screen four times to provide authentication and permit remote access to her email account. Employee granted access even though her workday was over and she was not, herself, attempting to access her own email account. The following day, after the fifth such prompt for authentication, Employee notified Residential Mortgage's Information Technology ("IT") staff of the anomalous activity.

Residential Mortgage's Failures to Investigate and Provide Requisite Notice

9. The internal investigation conducted by Residential Mortgage in response to the Cybersecurity Event was inadequate. Residential Mortgage's IT staff immediately determined that a cyber intruder had accessed Employee's email account on four occasions between March 5 and 6, 2019, nominally from an IP address originated in South Africa,[1] and blocked further access. The IT staff then failed to conduct any further inquiry after concluding that the unauthorized access was limited to Employee's email account. This failure was especially egregious given Employee's daily handling of the private data of

[1] An Internet Protocol address, or IP address, is a unique set of numbers that can identify an internet device, such as a phone or computer. An IP address can be used to obtain an IP Geolocation, which identifies the geographical location from which the internet device is communicating. Cyber criminals, however, frequently hide their true IP addresses and geolocations by routing communication through a VPN, or Virtual Private Network. In this manner, a true IP address can be concealed.

mortgage loan consumers, including social security numbers and bank account numbers, via her breached email account.

10. A majority of U.S. states, including New York and Maine, where Residential Mortgage is headquartered, impose data breach notifications on companies that maintain consumers' private data, such as social security numbers, passports, and bank account numbers. New York, Maine, and other states require prompt notification of unauthorized access of consumers' private data. *See, e.g.*, 10 Me. Rev. Stat. § 1346 *et. seq*. (Maine); N.Y. Gen Bus. Law§ 899-aa, *et. seq*. (New York); M.G.L. Ch. 93A §1 (Massachusetts). In New York, Department licensees must notify DFS within 72 hours of a determination that a Cybersecurity Event requiring notice to another agency has occurred. 23 NYCRR 500.17(a)(1).

11. Residential Mortgage failed to take appropriate action to satisfy these notification requirements. More specifically, Residential Mortgage failed to (1) identify whether Employee's mailbox contained private consumer data during the breach, (2) identify which consumers were impacted, and (3) apply the applicable state notice requirements triggered by the breach.

12. In failing to conduct an appropriate investigation, Residential Mortgage was unable to provide a data breach notice to any consumer, nor to any state agency – including the Department within 72 hours as required by the Cybersecurity Regulation. Rather, in September 2020, nearly 18 months after the breach, and only after prompting by the Department, Residential Mortgage undertook an appropriate investigation and considered which consumer and state breach notices were required by law.

Failure to Have a Comprehensive Cybersecurity Risk Assessment

13. Also discovered at the time of examination was that Residential Mortgage was missing a comprehensive cybersecurity risk assessment. The Cybersecurity Regulation requires licensees to identify and evaluate periodically vulnerability to cybersecurity risks and threats, analogous to the manner in which companies customarily identify and evaluate business risks in order to mitigate those risks. A cybersecurity risk assessment is the foundation of the risk-based cybersecurity program required by the Cybersecurity Regulation. Each DFS regulated entity must understand the specific risks it faces and design a cybersecurity program to address those risks. In conducting a risk assessment, a company is better able to shape a cybersecurity program to mitigate those threats. Here, a cybersecurity risk assessment should have led to the periodic evaluation of controls designed to protect Nonpublic Information and information systems.[2] See 23 NYCRR 500.09(a). In other words, a cybersecurity risk assessment should serve as a means to evaluate cybersecurity risks, and to protect the company's information systems and data, as well as the personal information of its customers. In sum, a cybersecurity risk assessment should result in thoughtful cybersecurity programs specifically tailored to safeguard the confidentiality of company and consumer data.

[2] Nonpublic Information includes "any information concerning an individual which because of name, number, personal mark, or other identifier can be used to identify such individual, in combination with" of any of the following: social security number; driver's license number, or non-driver identification card number; account number, credit or debit card number; any security code, access code or password that would permit access to an individual's financial account, or biometric records. 23 NYCRR 500.01(g)(2).

14. Residential Mortgage's forgoing failures directly undermine the accuracy of the CISO's 2020 filing of a Certification of Compliance attesting to Residential Mortgage's compliance with the Cybersecurity Regulation for the 2019 calendar year.

Actions Taken by Residential Mortgage

15. In the fall of 2020, after the conclusion of the DFS examination and the Department's subsequent investigation of the March 5, 2019 Cybersecurity Event, Residential Mortgage engaged outside counsel who specialize in data privacy, as well as a cybersecurity consultant, to assist in the search of the contents of Employee's email account.

16. To ensure notification of the March 5, 2019 Cybersecurity Event was made to all impacted consumers, Residential Mortgage reviewed every email which traveled through Employee's email account from her first day of employment through March 6, 2019, when Residential Mortgage blocked the unauthorized access.

17. By the last week of December 2020, Residential Mortgage and its team of experts identified all personal consumer data elements that could have been accessed by the threat actor during the unauthorized intrusion. The company then made the notifications required by law to the appropriate state agencies and impacted customers. These customers were offered a credit monitoring and identity theft protection package for a period of time consistent with the states' legal requirements.

18. The Department acknowledges the utility of the cybersecurity controls in place at Residential Mortgage at the time of the March 5, 2019 Cybersecurity Event. Residential Mortgage had implemented MFA for remote access and other network access through an authenticator device. It had also imposed network access control measures via Active Directory, requiring strong, complex passwords. The company also had installed

antivirus and end-point protection software on end-user devices. The company also had implemented automated detection rules for the improper transmission of certain private consumer data including social security numbers, as well as the automatic blocking of e-mail redirects by unauthorized actors.

19. After the March 5, 2019 Cybersecurity Event, Residential Mortgage implemented additional defenses to further mitigate the risks associated with phishing, including: automatic warning labels on emails sent from an external source; automatic warning and filtering to identify phishing emails prior to reaching end-users; IP filtering and analysis to prevent access from suspicious locations; and periodic penetration and other defense testing by third-party consultants.

20. Residential Mortgage has also provided the Department with its commitment to further remediation to ensure that its cybersecurity controls and protocols and procedures continue to be enhanced.

SETTLEMENT PROVISIONS

Civil Monetary Penalty

21. Residential Mortgage shall pay a penalty to the Department pursuant to Banking Law §§ 44 and 44-a in the amount of $1,500,000.00. It shall pay the entire amount within ten (10) days of executing this Consent Order.

22. In assessing a penalty for failures in compliance and required reporting, 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,

the financial resources and good faith of the entity, the gravity of the violation, and such other matters as justice and the public interest may require. B.L. §§ 44, 44-a.

23. The Department acknowledges Residential Mortgage's commendable cooperation throughout the DFS examination and the ensuing investigation by the Department. The Department also recognizes and credits Residential Mortgage's ongoing efforts to remediate the shortcomings identified in this Consent Order. Among other things, Residential Mortgage has demonstrated its commitment to remediation by devoting significant financial and other resources to enhance its cybersecurity program, including through changes now underway to its policies, procedures, systems, governance structures, and personnel.

Remediation

24. Residential Mortgage shall continue to strengthen its controls to protect its cybersecurity systems and the private data of consumers and shall, in accordance with the relevant provisions and definitions of 23 NYCRR 500:

a. Cyber Security Incident Response Plan. Within ninety (90) days of the date of this Order, Residential Mortgage shall submit to the Department a comprehensive written Cybersecurity Incident Response Plan consistent with 23 NYCRR 500.16. The Cybersecurity Incident Response Plan shall, at a minimum:

i. contain a plan designed to promptly respond to, and recover from, any Cybersecurity Event materially affecting the confidentiality, integrity or availability of Residential Mortgage's information systems or the continuing functionality of any aspect of the Residential Mortgage's business or operations;

ii. codify the internal processes for responding to a Cybersecurity Event;

iii. address the goals of the Cybersecurity Incident Response Plan; define clear roles, responsibilities and levels of decision-making authority;

iv. provide a plan for external and internal communications and information sharing;

v. identify requirements for the remediation of any identified weaknesses in information systems and associated controls;

vi. address documentation and reporting regarding Cybersecurity Events and related incident response activities; and

vii. address the evaluation and revision as necessary of the incident response plan following a Cybersecurity Event.

b. Cybersecurity Risk Assessment. Within ninety (90) days of the date of this Order, Residential Mortgage shall submit to the Department a comprehensive Cybersecurity Risk Assessment of its information systems consistent with 23 NYCRR 500.09, which shall:

i. be updated as reasonably necessary to address changes to Residential Mortgage's Information Systems, Nonpublic Information or business operations;

ii. allow for revision of controls to respond to technological developments and evolving threats, and shall consider the particular risks of Residential Mortgage's business operations related to cybersecurity, Nonpublic Information collected or

stored, Information Systems utilized and the availability and effectiveness of controls to protect Nonpublic Information and Information Systems;

iii. Contain accompanying written policies and procedures to include:

a. criteria for the evaluation and categorization of identified cybersecurity risks or threats facing Residential Mortgage;

b. criteria for the assessment of the confidentiality, integrity, security and availability of Residential Mortgage's information systems and Nonpublic Information, including the adequacy of existing controls in the context of identified risks; and

c. requirements describing how identified risks will be mitigated or accepted based on the Risk Assessment and how the cybersecurity program will address the risk.

c. Training and Monitoring. Within ninety (90) days of the date of this Order, Residential Mortgage shall submit to the Department, the following materials consistent with 23 NYCRR 500.14:

i. its risked-based policies, procedures and controls designed to: (a) monitor the activity of Authorized Users and (b) detect unauthorized access or use of, or tampering with, Nonpublic Information by such Authorized Users; and

ii. its most recent cybersecurity awareness training for all personnel, updated to reflect risks identified by Residential Mortgage in its Cybersecurity Risk Assessment.

Full and Complete Cooperation

25. Residential Mortgage commits and agrees that it will fully cooperate with the Department regarding all terms of this Consent Order, and as noted above, Residential Mortgage has already provided substantial cooperation in this matter.Waiver of Rights

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

Parties Bound by the Consent Order

27. This Consent Order is binding on the Department, Residential Mortgage Services, and its branches, as well as any of their successors and assigns. This Consent Order does not bind any federal or other state agency or any law enforcement authority.

28. No further action will be taken by the Department against Residential Mortgage for the conduct set forth in this Consent Order provided that Residential Mortgage complies with the terms of this Consent Order.

29. In the event that the Department believes any party to this Consent Order to be in material breach of the Consent Order, the Department will provide written notice to the party, and the party must, within ten (10) business 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. The Parties understand and agree that Residential Mortgage's failure to make the required showing within the designated time period shall be presumptive evidence of that party's breach. Upon a finding that a breach of this Consent Order has occurred, the Department has all the remedies available to it under New York

Banking and Financial Services Law and may use any evidence available to the Department in any ensuing hearings, notices, or orders.

Miscellaneous

30. Each provision of this Consent Order shall remain effective and enforceable until stayed, modified, suspended, or terminated by the Department.

31. 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 the Consent Order.

Notices

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

For the Department:

Sarah Walls
Senior Assistant Deputy Superintendent for Enforcement
New York State Department of Financial Services
One State Street
New York, NY 10004

For Residential Mortgage Services:

William E. Saufley
Senior Vice President & General Counsel
Residential Mortgage Services, Inc.
24 Christopher Toppi Drive
South Portland, ME 04106

Amanda R. Lawrence
Buckley LLP
2001 M Street, N.W. Suite 500
Washington, DC 20036

IN WITNESS WHEREOF, the parties have caused this Consent Order to be signed this ___ day of , 2021.

NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES

By: /s
SARAH WALLS
Senior Assistant Deputy Superintendent
Consumer Protection & Financial Enforcement Division

By: /s
KATHERINE A. LEMIRE
Executive Deputy Superintendent
Consumer Protection & Financial Enforcement Division

By: /s
LINDA A. LACEWELL
Superintendent of Financial Services

RESIDENTIAL MORTGAGE SERVICES, INC.

By: /s
JOHN GRAY
Senior Executive Vice President,
Chief Operating Officer & Chief Financial Officer