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

----------x

In the Matter of :

FIRST AMERICAN TITLE INSURANCE COMPANY :

----------x

CONSENT ORDER

The New York State Department of Financial Services (the "Department" or "DFS") and First American Title Insurance Company ("First American" or the "Company") are willing to resolve the matters described herein without further proceedings.

WHEREAS, First American is licensed by the Department to sell title insurance in New York State;

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

WHEREAS, the Cybersecurity Regulation defines clear standards for cooperative 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, the Department has been investigating a Cybersecurity Event experienced within First American, as well as First American's compliance with the Cybersecurity Regulation;

WHEREAS, based on the investigation, the Department concluded that First American violated the following provisions of the Cybersecurity Regulation: (1) 23 NYCRR § 500.3, which requires Covered Entities to implement and maintain cybersecurity policies based on the Covered Entity's Risk Assessment with respect to specific areas, including data governance and classification, access controls and identity management, and risk assessment and (2) 23 NYCRR § 500.7, which requires Covered Entities to limit user access privileges to Information Systems that provide access to Nonpublic Information ("NPI");

WHEREAS, on July 21, 2020, the Department filed a Statement of Charges and Notice of Hearing against First American seeking to impose a civil monetary penalty stemming from First American's violations of the Cybersecurity Regulation and an order requiring First American to remedy the violations identified therein; and

WHEREAS, on March 10, 2021, and June 17, 2021, the Department filed an Amended Statement of Charges and Notice of Hearing and a Second Amended Statement of Charges and Notice of Hearing, respectively, against First American.

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 Department is the insurance regulator of the State of New York, and the Superintendent of Financial Services is responsible for ensuring the safety and soundness of New York's insurance industry and promoting the reduction and elimination of fraud, abuse, and unethical conduct with respect to insurance licensees.

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. First American's title insurance products insure the interests of owners or lenders against defects in the title to real property, including adverse ownership claims, liens, encumbrances, or other matters affecting title.

4. In the ordinary course of its business, First American collects, stores and transmits information in connection with real estate transactions, including both publicly available information and the consumer NPI of buyers and sellers of real estate.

5. Among other things, the Superintendent's Cybersecurity Regulation places on all DFS-regulated entities ("Covered Entities"), including First American, an obligation to establish and maintain a cybersecurity program, based on a Risk Assessment and designed to protect the confidentiality and integrity of its Information Systems, as well as any NPI contained therein. 23 NYCRR §§ 500.1(c), (e), (g), and (k), 500.2(b).

6. To do that, the Regulation requires Covered Entities to periodically conduct a Risk Assessment that will inform the design of the cybersecurity program, as well as the written cybersecurity policies. 23 NYCRR §§ 500.2(b), 500.3, 500.9(a). The Risk Assessment must be

updated as necessary to address changes to the Covered Entities' Information Systems, NPI, or business operations. 23 NYCRR § 500.9(a). Each Covered Entity's cybersecurity policy and/or policies must also address data governance and classification, access controls and identity management, systems and network security, and risk assessment, among several other areas. 23 NYCRR § 500.3(b), (d), (g), and (m).

7. The Cybersecurity Regulation also requires Covered Entities to protect against Cybersecurity Events[1] and protect consumer NPI by limiting user access privileges to Information Systems that provide access to NPI, 23 NYCRR § 500.7, and to implement encryption for NPI "held or transmitted by the Covered Entity both in transit over external networks and at rest." 23 NYCRR § 500.15.

The EaglePro Application

8. In connection with the issuance of certain title insurance policies, First American collects documents from customers, real estate agents, and other parties to the real estate transaction, some of which contain personal identifying information, or NPI, of various parties.

9. First American stores the documentation it collects in these transactions in an image repository. As documents are uploaded to the image repository, each individual document is assigned a numbered document ID. When a document is uploaded to the image repository, the individual performing the upload function is supposed to identify whether the document contains NPI, and, if it does, code it appropriately.

10. To provide access to documents from a specific transaction to all necessary parties, First American developed an application called EaglePro. EaglePro is a First American

[1] A "Cybersecurity Event" is defined in the Cybersecurity Regulation as an act or attempt, whether successful, to gain unauthorized access to information stored on an information system or disrupt or misuse such information system. 23 NYCRR § 500.1(d).

proprietary application that enables various parties to a real estate transaction, and their representatives and designees, to render images, such as title searches, title exception documents, and title commitments, viewable to the end user.

11. In October 2014, First American updated EaglePro to include a function that permitted authorized First American employees to create hyperlinks to related images. To share these images with parties to a transaction, a user first selected specific documents from the image repository, EaglePro then emailed the intended recipient a link that allowed the recipient to review the selected documents.

12. The link generated by EaglePro provided access to title-related documents to anyone with the link. Such access was obtained without login or authentication, and until May 24, 2019, EaglePro hyperlinks had no expiration date with respect to accessing documents.

13. EaglePro users were instructed not to transmit documents containing NPI through these hyperlinks, but there were no technical controls in place that prevented users from transmitting documents containing NPI through EaglePro.

Cybersecurity Event

14. On May 24, 2019, a cybersecurity journalist published an article concerning the existence of a vulnerability in the EaglePro application that, according to the cybersecurity journalist, exposed 885 million documents (dating back as far as 2003) to the public. The cybersecurity journalist alleged that he was personally able to view consumer NPI, including social security numbers, drivers' license numbers, and tax and banking information, within some of the impacted documents.

15. The cybersecurity journalist alleged that replacing the document ID in the web page URL of the EaglePro hyperlink with another sequential number allowed access to other non-related documents from the image repository without authentication (the "Vulnerability").

16. Following communications with the cybersecurity journalist, and prior to his publishing of the article, First American shut down external access to EaglePro and disabled all links previously generated by EaglePro.

17. On May 27, 2019, First American notified the Department of the existence of the Vulnerability as required by Section 500.17(a) of the Cybersecurity Regulation. First American also publicly disclosed that it "shut down external access to a production environment with a reported design defect that created the potential for unauthorized access to customer data." Thereafter, in an "Incident Update" addressed to First American's customers on May 31, 2019, First American acknowledged that documents containing NPI were potentially able to be accessed and offered complimentary credit monitoring services to any concerned customer who received a title insurance policy or escrow/closing services from First American on or after January 1, 2003.

Failure to Maintain Reasonable Access Privileges

18. Upon further investigation, the Department learned that First American had discovered the Vulnerability associated with EaglePro prior to the cybersecurity journalist's publication.

19. In December 2018, as part of its routine penetration testing, First American's Cyber Defense Team performed a vulnerability analysis and penetration test of EaglePro. Preliminary findings of the Vulnerability Analysis and Penetration Testing Report for the EaglePro Web Application (the "EaglePro Vulnerability Test Report") were shared with First

American's Vulnerability Remediation Management team and the Application Security team on December 17, 2018. In its report, the Cyber Defense Team expressed that the finding identified in the EaglePro Vulnerability Test report should be "address[ed] as soon as possible."

20. The final EaglePro Vulnerability Test Report was disseminated to First American's IT Application Team and the Vulnerability Remediation Management Team in mid-January 2019.

21. The EaglePro Vulnerability Test Report found that "replacing the document ID in the web page URL" of the EaglePro hyperlink "with another sequential number allow[ed] access to other non-related sessions without authentication." The report further found that "using standard Internet search methods [the Cyber Defense Team was] able to bypass authentication to retrieve documents that were found using Google searches" (emphasis in original).

22. The EaglePro Vulnerability Test Report noted that "[n]o NPI was discovered in the documents that were reviewed for this report," but that "[i]t [was] unknown if any additional documents" were potentially able to be accessed that "contained NPI" and recommended "further investigation by the application owner." No such further investigation or review by senior management was conducted by First American prior to the cybersecurity journalist's publication on May 24, 2019.

23. First American's failure to implement reasonable access controls on the EaglePro application contributed to the potential unauthorized access to NPI and constituted a violation of Section 500.7 of the Cybersecurity Regulation.

Failure to Implement or Maintain Risk-Based Cybersecurity Policies

24. Risk Assessments constitute a core component of a robust cybersecurity program. For example, Section 500.2(b) of the Cybersecurity Regulation requires the cybersecurity

program to be based on the Covered Entity's Risk Assessment, and Section 500.3 of the Cybersecurity Regulation requires the implementation of a written cybersecurity policy and/or policies to be based on the Covered Entity's Risk Assessment.

25. As part of their cybersecurity program, each Covered Entity is required to implement and maintain a written policy or policies, based on the Covered Entity's Risk Assessment, that, among other things, addresses "(b) data governance and classification . . . (d) access controls and identity management . . . (g) systems and network security . . . [and] (m) risk assessment." 23 NYCRR § 500.3(b), (d), (g) & (m).

26. Though First American had many cybersecurity policies and procedures in place, it failed to ensure their full and complete implementation. For example, First American, as part of its risk assessment, incorrectly classified EaglePro as an application that did not contain NPI despite the fact that EaglePro, because of the Vulnerability, could allow access to documents containing NPI. Therefore, First American did not implement an appropriate, risk-based policy governing access controls for EaglePro. These inadequate access controls contributed to the potential unauthorized access to NPI through the EaglePro hyperlinks.

Violations of Law and Regulations

27. First American failed to adequately maintain and implement an effective cybersecurity policy related to access controls and based on its risk assessment. 23 NYCRR § § 500.3(b), (d), and (m).

28. First American failed to implement access controls sufficient to prevent unauthorized users to gain access to NPI through EaglePro, in violation of 23 NYCRR § 500.7.

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

29. 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 one million U.S. dollars ($1,000,000.00). The payment shall be in the form of a wire transfer in accordance with instructions provided by the Department.

30. First American 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.

31. First American 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.

32. In assessing a penalty for failures in First American's 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, the gravity of the violations, and such other matters as justice and the public interest may require.

33. The Department acknowledges First American's cooperation throughout this investigation. The Department also recognizes and credits First American's ongoing efforts to remediate the shortcomings identified in this Consent Order and to enhance their cybersecurity controls to protect NPI and ensure ongoing compliance with the Cybersecurity Regulation.

Remediation

34. Following the Cybersecurity Event, First American remediated the Vulnerability and implemented further procedures to strengthen its Information Security Program. In connection with the parties' discussions to resolve this matter, First American submitted, and the Department approved, a Remediation Overview and Compliance Summary detailing:

a. The remedial steps taken by First American to address the violations identified in this Consent Order; and

b. The enhancements First American has made to its cybersecurity program since the Cybersecurity Event.

Full and Complete Cooperation

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

Disposition of Pending Adjudicatory Proceeding

36. Pursuant to Section 301(5) of the New York State Administrative Procedure Act, the parties agree that this Consent Order shall dispose of the pending adjudicatory proceeding in the matter *In the Matter of: First American Title Insurance Company*, No. 2020-0030-C.

Further Action by the Department

37. No further action will be taken by the Department against the Company or its successors for the conduct set forth in this Consent Order, the Statement of Charges and Notice of Hearing filed in connection with this matter, including any amendments thereto, 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.

38. 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

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

40. 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

41. 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

42. 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.

43. 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 Insurance Law, 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

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

For the Department:

Madeline W. Murphy
Assistant Deputy Superintendent for
Consumer Protection and Financial Enforcement
One Commerce Plaza, 20th Floor
Albany, New York 12257

For First American:

Lisa Cornehl
Chief Legal Officer
First American Financial Corporation
1 First American Way
Santa Ana, CA 92707

Elizabeth Ferrick
Partner
Dentons US LLP
211 N. Broadway, Suite 3000
St. Louis, MO 63102

Miscellaneous

45. 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.

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

47. 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.

48. 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.

49. 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.

50. 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.

51. 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/ Madeline W. Murphy
MADELINE W. MURPHY
Assistant Deputy Superintendent for Consumer Protection and Financial Enforcement

November 27, 2023

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

November 27, 2023

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

November 27, 2023

FIRST AMERICAN TITLE INSURANCE COMPANY

By: /s/ Lisa Cornhel
LISA CORNHEL
Chief Legal Officer

November 17, 2023

THE FOREGOING IS HEREBY APPROVED. IT IS SO ORDERED.

/s/ Joanne A. Berman
JOANNE BERMAN
Acting Superintendent of Financial Services

November 27, 2023