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

----------x

In the Matter of: : No. 2020-0030-C

FIRST AMERICAN TITLE INSURANCE COMPANY, :

Respondent. :

----------x

STATEMENT OF CHARGES AND NOTICE OF HEARING

TO THE ABOVE-NAMED RESPONDENT:

PLEASE TAKE NOTICE that a hearing will be held at the office of the New York State Department of Financial Services (the "Department" or "DFS"), One State Street, New York, New York 10004, 6th Floor, on the 26th day of October, 2020, at 10:00 a.m., and continuing thereafter day to day as determined by the Department before a Hearing Officer to be appointed by the Superintendent of Financial Services (the "Superintendent"), to determine whether RESPONDENT has committed violations of §§ 500.02, 500.03, 500.07, 500.09, 500.14 and 500.15 of Part 500 of Title 23 of the New York Codes, Rules, and Regulations, also referred to as the Department's "Cybersecurity Requirements for Financial Services Companies" (hereinafter, 23 NYCRR Part 500 or the "Cybersecurity Regulation"), whether violations should be found for Respondent's persistent failures to safeguard customer information, and whether

civil monetary penalties shall be imposed and other appropriate relief be granted as a result of such findings.

OVERVIEW

1. For more than four years, First American Title Insurance Company ("First American" or "Respondent") exposed tens of millions of documents that contained consumers' sensitive personal information including bank account numbers and statements, mortgage and tax records, Social Security numbers, wire transaction receipts, and drivers' license images.

2. From at least October 2014 through May 2019, due to a known vulnerability on Respondent's public-facing website (the "Vulnerability"), these records were available to anyone with a web browser.

3. The Uniform Resource Locator (the "URL") of a web application is the specific web address that makes it possible to request a document, file, video, or other resource maintained on the web. By permitting a URL on its public website to be vulnerable to manual manipulation, or re-writing, Respondent knowingly laid bare millions of personal datapoints of its customers from hundreds of First American consumer files for access without any login or authentication requirements.

4. The Vulnerability was first introduced during an application software update in May 2014, and went undetected for years.

5. Respondent's mishandling of its own customers' data was compounded by its willful failure to remediate the Vulnerability, even after it was discovered by a penetration test in December 2018.[1] Remarkably, Respondent instead allowed unfettered access to the personal and

[1] A penetration test is an authorized simulated cyberattack on a computer system, performed to evaluate the security system, including the potential for unauthorized parties to gain access to the system's features and data.

financial data of millions of its customers for six more months until the breach and its serious ramifications were widely publicized by a nationally recognized cybersecurity industry journalist.

THE ROLE AND JURISDICTION OF THE DEPARTMENT OF FINANCIAL SERVICES

6. The Department of Financial Services is the insurance regulator in the State of New York. 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 participants.

7. 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.

8. Among her many obligations to the public is the Superintendent's consumer protection function, which includes the protection of individuals' private and personally sensitive data from careless, negligent, or willful exposure by licensees of the Department.

9. To support this critical obligation to consumers, 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 designed to protect the confidentiality, integrity, and availability of its Information Systems and its customers' Nonpublic Information, as defined in 23 NYCRR 500.01(e) and 500.01(g), respectively.

10. To that end, the DFS Cybersecurity Regulation require Covered Entities to implement and maintain cybersecurity policies and procedures to address, to the extent applicable, consumer data privacy and other consumer protection issues with effective controls,

secure access privileges, thorough and routine cybersecurity risk assessments, comprehensive training and monitoring for all employees and other users, and well-grounded governance processes to ensure senior attention to these important protections.

11. Every Covered Entity is required to base its cybersecurity policies and procedures on risk assessments to ensure ongoing evaluation of the risks that continuously threaten the security of Nonpublic Information, including sensitive personal information, and to further safeguard the Information Systems that are accessed or held by Third Party Service Providers. Encryption and multifactor authentication are further controls required under the Cybersecurity Regulation to ensure that Covered Entities thoroughly protect their customers' private data.

12. Respondent, a Nebraska-based stock insurance company, is a licensee of the Superintendent authorized to write title insurance in New York. As such, Respondent is a "Covered Entity" under 23 NYCRR Section 500.01(c) and is therefore subject to the requirements of the Cybersecurity Regulation.

13. Nonpublic Information ("NPI") means all electronic information that is not publicly available and is: (1) Business-related information of a Covered Entity the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the Covered Entity; (2) 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 any one or more of the following data elements: (i) social security number, (ii) drivers' license number or non-driver identification card number, (iii) account number, credit or debit card number, (iv) any security code, access code or password that would permit access to an individual's financial account, or (v) biometric records; and (3) Any information or data, except age or gender, in any form or medium created

by or derived from a health care provider or an individual and that relates to (i) the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family, (ii) the provision of health care to any individual, or (iii) payment for the provision of health care to any individual.

14. Pursuant to Section 404 of the Financial Services Law, the Consumer Protection and Financial Enforcement Division of the Department investigated whether First American was complying with the Superintendent's Cybersecurity Regulation, 23 NYCRR Part 500, which requires that all Department-regulated entities, including First American, have a cybersecurity program that, among other things, protects customer NPI. After such investigation, the Department hereby commences an administrative proceeding alleging that First American has committed the violations described below.

FACTUAL ALLEGATIONS

Respondent's Business Activities

15. Title insurance policies insure the interests of owners or lenders against defects in the title to real property. These defects include adverse ownership claims, liens, encumbrances, or other matters affecting title. Respondent is the second largest title insurance provider in the United States. In 2019, its Title Insurance and Services segment accounted for 91.5% of Respondent's $6.2 billion in consolidated revenue.

16. When a customer seeks to purchase title insurance, Respondent collects personal information from multiple sources in connection with the insurance application. The customer submits NPI in the form of applications and settlement or financial statements. Others involved in the transaction on behalf of the title customer, such as the real estate agent, lender, escrow, or settlement agent and attorney, also submit documents containing sensitive customer information.

In performing the ensuing title search, Respondent obtains, from its own or others' proprietary databases, documents that may also contain personal information such as appraisals, credit reports, escrow account balances, and account numbers. Respondent might also collect documents from public records such as tax assessments and liens to include as part of a title insurance package (the "package" or "title package").

17. Therefore, in the regular course of its business, Respondent collects, stores, and transmits the personal information of millions of buyers and sellers of real estate in the U.S. each year. Respondent stores this information in its main document repository, the FAST image repository, also known as "FAST." Documents can be loaded into FAST by Respondent's employees assigned to any of Respondent's business units. Respondent uses documents stored in FAST to transact title insurance and settlement orders.

18. FAST includes tens of millions of documents with sensitive personal information, such as social security numbers, bank account and wiring information, and mortgage and tax records. In April 2018, for example, FAST contained 753 million documents, 65 million of which had been tagged by Respondent's employees as containing NPI. A random sampling of 1,000 documents that were not tagged showed that 30% of those documents also contained NPI. As of May 2019, FAST contained over 850 million documents.

19. Respondent also created and maintains an application on its network known as EaglePro. EaglePro is a web-based title document delivery system that allows title agents and other Respondent employees to share any document in FAST with outside parties. EaglePro is intended to be used by title agents and others to share the title package with the parties to a real estate transaction. After a party to or a participant in a transaction selects documents from FAST to be shared with another participant of a real estate transaction, EaglePro emails the recipient a

link to a website that allows him or her to access those documents. Anyone who had the link or the URL for the website could access the package without login or authentication.

Respondent's Data Exposure

20. In October 2014, Respondent updated the EaglePro system in a manner that gave rise to the Vulnerability. The URL for each website shared via EaglePro included an ImageDocumentID number, and each document in FAST was assigned a sequentially numbered ImageDocumentID. By changing the ImageDocumentID number in the URL by one or more digits, anyone could view the document corresponding to the revised ImageDocumentID. As a result, by simply typing in any ImageDocumentID, any document in FAST could be accessed regardless of whether the viewer had authorized access to those documents. Until May 2019, the URLs shared via EaglePro had no expiration date.

21. In other words, more than 850 million documents were accessible to anyone with a URL address providing access to a single document in the EaglePro-generated website. The Vulnerability thus led to exposure of a staggering volume of personal and financially sensitive documents, any number of which could be used by fraudsters to engage in identity theft and even outright theft of assets. Moreover, such theft could occur without individuals knowing their information had been stolen from Respondent.

22. In December 2018, First American's Cyber Defense Team discovered the EaglePro Vulnerability during a penetration test of the EaglePro application. The Cyber Defense Team's role was to conduct penetration tests on Respondent's applications — tests that simulated a cyberattack — in order to identify vulnerabilities that could be exploited.

23. In an email on December 17, 2018, a member of the Cyber Defense Team alerted the EaglePro Application Development team to the existence of the EaglePro Vulnerability,

reporting "recently discovered important findings during the reconnaissance phase of our current penetration test of the EaglePro application that should be addressed." The email went on to describe the Vulnerability. Recognizing the urgency of the situation, the manager of the Application Development team responsible for EaglePro replied that the Vulnerability should be "address[ed] as soon as possible."

24. On January 11, 2019, the Cyber Defense Team distributed the final report of the EaglePro penetration test. The report described the Vulnerability in detail, including pages of screenshots demonstrating how the EaglePro website URL could be manipulated to display sensitive documents not intended for widespread viewing. The penetration test report also showed that more than 5,000 documents exposed by EaglePro had been subjected to Google search engine indexing, *i.e.*, collection and storage of data by Google to facilitate later information retrieval in the course of open-source Google searches by the public. Among the key findings in the Cyber Defense Team's report was the following warning: "using standard Internet search methods *we were able to bypass authentication to retrieve documents that were found using Google searches*" (emphasis in the original). The Cyber Defense Team reviewed 10 documents exposed by the Vulnerability, and, although none contained NPI, the Cyber Defense Team strongly recommended that the application team investigate further and determine whether sensitive documents were exposed. Despite this clear warning, this recommendation was ignored, and Respondent failed to conduct follow-up investigation.

25. Even more alarming, in the six months following discovery of the Vulnerability, Respondent failed to correct the Vulnerability even though hundreds of millions of documents were exposed. This lapse was caused by a cascade of errors that occurred substantially due to

flaws in Respondent's vulnerability remediation program. Some of these flaws are illustrated below:

a. Respondent grossly underestimated the level of risk associated with the Vulnerability. During interviews with the Department, several Respondent employees revealed that the Vulnerability was not addressed, in part, because the problem was erroneously classified as "medium severity." The "medium severity" classification, in turn, rested on the mistaken belief that EaglePro could not transmit NPI. Respondent's Chief Information Security Officer, the senior most employee responsible for the security of Respondent's Information Systems, testified that she believed that data accessible in EaglePro was publicly available, and therefore did not constitute NPI. However, anyone with the barest familiarity with EaglePro understood that the application could be used to distribute any documents contained in FAST, including documents of a highly sensitive nature that clearly constituted NPI. Nonetheless, this error was never corrected.

b. Respondent failed to follow its own cybersecurity policies. Respondent's policies required a security overview report for each application and a risk assessment for data stored or transmitted by any application. No security overview or risk assessment was performed for EaglePro.

c. Respondent conducted an unacceptably minimal review of exposed documents, and thereby failed to recognize the seriousness of the security lapse. The Cyber Defense Team reviewed only 10 documents out of the hundreds of millions of documents exposed. While conducting such a preposterously minimal review, the Cyber Defense Team found no NPI in the 10 documents reviewed and thus failed to recognize the seriousness of the

situation. As a result, the team erroneously classified the Vulnerability as merely "medium severity."

d. Respondent failed to heed advice proffered by its own in-house cybersecurity experts. The Cyber Defense Team recommended that the EaglePro application team conduct further review to determine if sensitive documents were exposed by the Vulnerability. No such review was conducted. Moreover, the application team knew that EaglePro could distribute the highly sensitive documents warehoused in FAST but nonetheless conducted no further investigation of the Vulnerability.

e. An apparent administrative error compounded the delay in the timeframe for remediating the Vulnerability. The director of the Cyber Defense Team inadvertently caused additional delay in the remediation by accidently re-classifying the vulnerability from "medium" to "low" severity when it was entered into Respondent's vulnerability tracking system in January 2019. Classified as "low severity," Respondent's policy inaccurately allowed 90 days for the remediation of the Vulnerability.

f. Respondent failed to adhere to its internal policies, and delayed addressing the Vulnerability for six months. Even if Respondent had correctly classified the Vulnerability, which Respondent failed to do by deeming it "low severity," Respondent failed to remediate within 90 days as the policy required even for "low severity " vulnerabilities. Instead, Respondent failed to address the Vulnerability for more than five months after its discovery, and even then, only after the Vulnerability was revealed by a media outlet. This failure occurred despite discovery of the Vulnerability, widespread internal circulation of a detailed report on the Vulnerability, and assignment of a 90-day deadline for remediation. Sworn testimony by

Respondent's employees responsible for data security revealed internal confusion and an alarming lack of accountability with regard to responsibility for remediation of vulnerabilities.

g. Remediation was ineffectively assigned to an unqualified employee. Shortly after the EaglePro penetration test report was circulated on January 11, 2019, responsibility for remediating the Vulnerability was assigned to a new employee with little experience in data security (the "Accountable Remediation Owner"). The newly assigned Accountable Remediation Owner was never given a copy of the EaglePro penetration test detailing the Vulnerability. Moreover, the gravity of the Vulnerability was not highlighted to the employee, who was merely provided with a laundry list of EaglePro application vulnerabilities, mostly minor in nature. In addition, the new Accountable Remediation Owner was not provided with the applicable policies and standards for Respondent's data security and remediation, and was offered little support in performing these new responsibilities.

26. In addition to the failure to promptly detect and then remediate the Vulnerability, EaglePro and FAST generally lacked adequate controls to protect NPI.

27. Respondent knew that its procedure to identify and classify sensitive documents in FAST was significantly flawed. To identify and classify sensitive documents containing NPI, Respondent relied solely on a process in which title agents, in the course of uploading documents, manually added the prefix "SEC" to the name for each file containing NPI. EaglePro users were then instructed not to distribute any documents containing NPI. Moreover, Respondent was fully aware that this methodology — by a wide margin — failed to identify and protect documents containing NPI. For instance:

i. In April 2018, a presentation by senior members of Respondent's IT and information security management teams to the Board of Directors demonstrated that within a

random sample of 1,000 documents stored in FAST, 30% of those documents contained NPI but were not tagged as such. At this error rate, potentially hundreds of millions of documents containing NPI were not designated properly.

ii. A June 1, 2019 email from Respondent's Vice President of Information Security discussing problems with the NPI controls in EaglePro likewise acknowledged that the manual process for designated NPI was "highly prone to error."

28. Despite these widely acknowledged control deficiencies, Respondent's staff responsible for EaglePro's application security — the Director of Vulnerability Remediation Management Team, the Director of Application Security, and the EaglePro Accountable Remediation Owner — testified that they were not aware that NPI was transmitted using EaglePro or that a 2018 sample of documents in FAST had revealed a significant error rate in the tagging of documents with NPI.

29. In June 2019, after a journalist publicized Respondent's data security vulnerabilities, Respondent's information security personnel recommended modifying EaglePro, limiting access to authenticated users. Senior management rejected that recommendation. Respondent's information security personnel then recommended adding two technical controls to protect NPI. First, they recommended disallowing transmission of tagged NPI documents in EaglePro via unsecured links. Second, in recognition of the faulty nature of manually tagging documents, they recommended a scan of FAST for documents containing NPI but not tagged as sensitive. Neither recommendation was implemented.

30. To this day, the sole control preventing EaglePro from being used to transmit NPI is merely an instruction to users not to send NPI. Respondent relies on training to ensure employees follow procedures, delegating responsibility for such training to individual business

units. At the same time, individual business units are left at their own discretion to design and conduct the training. This lack of centralized and coordinated training exists despite Respondent's professed awareness of inadequate controls.

31. When the Department asked Respondent's CISO why additional controls were not adopted to protect NPI, Respondent's CISO disavowed ownership of the issue, stating, among other reasons, that such controls were not the responsibility of Respondent's information security department.

32. Respondent also failed to timely encrypt documents containing NPI as required by the Department's Cybersecurity Regulation. 23 NYCRR Section 500.15 requires, among other things, documents containing NPI be encrypted. While encryption would not have prevented the data exposure of NPI due to the Vulnerability, the encryption requirement of 23 NYCRR Section 500.15 went into effect on September 1, 2018 – 18 months after the Part 500 regulation went into effect. Nonetheless, Respondent did not encrypt the tens of millions of documents tagged as containing NPI until approximately December 2018, months after the relevant provisions of the Cybersecurity Regulation went into effect. Moreover, the remainder of the documents in FAST — which Respondent knew included many documents containing NPI — were not fully encrypted until mid-2019.

Respondent's Data Exposure is Revealed

33. On May 24, 2019, Brian Krebs, a journalist who reports on cybersecurity issues, published an article revealing that Respondent had exposed 885 million documents — dating as far back as 2003 and many containing NPI — by rendering the documents openly accessible to the public. Mr. Krebs himself was easily able to view highly-sensitive consumer data, including

documents that contained NPI such as social security numbers, drivers' licenses, and tax and banking information.

34. In the days leading up to publication of his findings, Mr. Krebs and another individual who had stumbled upon the Vulnerability repeatedly reached out to First American to alert the firm of the Vulnerability.

35. After publication of Mr. Krebs's findings, Respondent reported the incident to the Department, as required under 23 NYCRR 500.17. Respondent 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." In an Incident Update addressed to Respondent's customers on May 31, 2019, Respondent conceded that documents containing NPI were potentially exposed.

36. After the disclosure by Mr. Krebs, Respondent conducted a forensic investigation into data exposure attributable to the Vulnerability but was unable to determine whether records were accessed prior to June 2018. Respondent's forensic investigation relied on a review of web logs retained from June 2018 onward. Respondent's own analysis demonstrated that during this 11-month period, more than 350,000 documents were accessed without authorization by automated "bots" or "scraper" programs designed to collect information on the Internet.

SPECIFICATIONS OF CHARGES

CHARGE I
RESPONDENT VIOLATED 23 NYCRR 500.02

37. The allegations set forth in paragraphs 1 to 36 above are repeated and realleged as if fully set forth herein.

38. Section 500.02 of the Cybersecurity Regulation requires that each Covered Entity maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems. The cybersecurity program must be based on the Covered Entity's Risk Assessment and designed to perform core cybersecurity functions, including identifying and assessing internal and external cybersecurity risks that may threaten the security or integrity of NPI stored on the Covered Entity's Information Systems.

39. Respondent failed to perform risk assessments for data stored or transmitted within its Information Systems, specifically the FAST and EaglePro applications, despite those applications' transmission and storage of NPI. Respondent's acts or practices, for the period beginning on the effective date of this Section, March 1, 2017, through May 24, 2019, constitute a violation of 23 NYCRR 500.02.

CHARGE II
RESPONDENT VIOLATED 23 NYCRR 500.03

40. The allegations set forth in paragraphs 1 to 39 above are repeated and realleged as if fully set forth herein.

41. Section 500.03 of the Cybersecurity Regulation, 23 NYCRR 500.03, requires that a Covered Entity maintain a written policy or policies, approved by a Senior Officer or the board of directors (or an appropriate committee thereof) or equivalent governing body, setting forth the Covered Entity's policies and procedures for the protection of its Information Systems and the NPI stored on those Information Systems. Section 500.03 further requires that the cybersecurity policy shall be based on the Covered Entity's Risk Assessment and address the following areas, among others: data governance and classification, access controls and identity management, and risk assessment. § 500.03(b), (d), and (m).

42. Respondent failed to maintain and implement data governance and classification policies for NPI suitable to its business model and associated risks. Respondent's classification of EaglePro as an application that did not contain or transmit NPI was incorrect given that EaglePro could and did allow access to documents containing NPI.

43. Respondent did not maintain an appropriate, risk-based policy governing access controls for EaglePro. These inadequate access controls failed to prevent the exposure of NPI in millions of documents. Respondent's acts or practices for the period beginning on the effective date of the Section, March 1, 2017, through May 24, 2019, constitute violations of 23 NYCRR 500.03.

CHARGE III
RESPONDENT VIOLATED 23 NYCRR 500.07

44. The allegations set forth in paragraphs 1 to 43 above are repeated and realleged as if fully set forth herein.

45. Section 500.07 of the Cybersecurity Regulation, 23 NYCRR 500.07, requires that a Covered Entity shall limit user access privileges to Information Systems that provide access to NPI and shall periodically review such access privileges.

46. The Vulnerability allowed unauthorized remote users to gain access to NPI in Respondent's FAST system. The Vulnerability existed due to a lack of reasonable access controls. Any person could access sensitive documents stored in FAST simply by altering an EaglePro URL. Respondent's acts or practices, for the period beginning on the effective date of the Section, March 1, 2017, through May 24, 2019, constitute a violation of 23 NYCRR 500.07.

CHARGE IV
RESPONDENT VIOLATED 23 NYCRR 500.09

47. The allegations set forth in paragraphs 1 to 46 above are repeated and realleged as if fully set forth herein.

48. Section 500.09(a) of the Cybersecurity Regulation, 23 NYCRR 500.09(a), requires each Covered Entity to conduct a periodic Risk Assessment of the Covered Entity's Information Systems to inform the design of the cybersecurity program as required by 23 NYCRR Part 500. Such Risk Assessment shall be updated as reasonably necessary to address changes to the Covered Entity's Information Systems, NPI, or business operations. The Covered Entity's Risk Assessment shall allow for revision of controls to respond to technological developments and evolving threats and shall consider the particular risks of the Covered Entity's business operations related to cybersecurity, NPI collected or stored, Information Systems utilized and the availability and effectiveness of controls to protect NPI and Information Systems.

49. Section 500.09(b) requires that the Risk Assessment be carried out in accordance with written policies and procedures and shall be documented. Among other things, such policies and procedures shall include: criteria for the assessment of the confidentiality, integrity, security, and availability of the Covered Entity's Information Systems and Nonpublic Information, including the adequacy of existing controls in the context of identified risks; and requirements describing how identified risks will be mitigated or accepted based on the Risk Assessment and how the cybersecurity program will address the risks.

50. The Risk Assessment was not sufficient to inform the design of the cybersecurity program as required by 23 NYCRR Part 500, as indicated not only by Respondent's failure to identify where NPI was stored and transmitted through its Information Systems, but also its failure to identify the availability and effectiveness of controls to protect NPI and Information

Systems. Respondent's acts or practices, for the period beginning on the effective date of this Section, March 1, 2018, through May 24, 2019, constitute a violation of 23 NYCRR 500.09.

CHARGE V
RESPONDENT VIOLATED 23 NYCRR 500.14(b)

51. The allegations set forth in paragraphs 1 to 50 above are repeated and realleged as if fully set forth herein.

52. Section 500.14(b) of the Cybersecurity Regulation, 23 NYCRR 500.14(b), requires that as part of its cybersecurity program, each Covered Entity is required to provide regular cybersecurity awareness training for all personnel, and such training must be updated to reflect risks identified by the Covered Entity in its Risk Assessment.

53. Respondent did not provide adequate data security training for Respondent's employees and affiliated title agents responsible for identifying and uploading sensitive documents into the FAST system and in using the EaglePro system. This failure was especially significant since both the process of identifying sensitive documents and the only control preventing NPI from being distributed through EaglePro depended solely on employees and users correctly identifying sensitive documents and treating them appropriately. As a result, Respondent did not adopt cybersecurity awareness training that reflected the risks inherent in its operations and led to the Vulnerability reported on May 24, 2019. Respondent's acts or practices, for the period beginning on the effective date of the Section, March 1, 2018, through May 24, 2019, constitute a violation of 23 NYCRR 500.14.

CHARGE VI
RESPONDENT VIOLATED 23 NYCRR 500.15

54. The allegations set forth in paragraphs 1 to 53 above are repeated and realleged as if fully set forth herein.

55. Section 500.15 of the Cybersecurity Regulation requires that Covered Entities implement controls, including encryption, to protect NPI held or transmitted by the Covered Entity both in transit over external networks and at rest. This section allows for the use of effective alternative compensating controls to secure NPI in transit over external networks and at rest if encryption of such is infeasible. Such compensating controls must be reviewed and approved by the Covered Entity's CISO. To the extent that a Covered Entity is utilizing compensating controls, the feasibility of encryption and effectiveness of the compensating controls shall be reviewed by the CISO at least annually.

56. Until the end of 2018, Respondent failed to encrypt documents marked as sensitive within the FAST repository. Other documents that contained sensitive data but were erroneously not marked as sensitive– were not encrypted until mid-2019. Respondent did not implement controls suitable to protect the NPI stored or transmitted by it, both in transit over external networks and at rest, nor did Respondent implement suitable compensating controls approved by the CISO. Respondent's acts or practices, for the period beginning on the effective date of the Section, September 1, 2018, through May 24, 2019, constitute a violation of 23 NYCRR 500.15.

PLEASE TAKE NOTICE THAT, as a result of these charged violations, the Department is seeking the following relief:

a) The imposition of civil monetary penalties against respondent with respect to those violations in which such penalties are authorized; and

b) The issuance of an order upon the Respondent requiring it to remedy the defined violations alleged herein; and

c) Such other relief as is deemed just and appropriate.

PLEASE TAKE FURTHER NOTICE THAT:

(A) Respondent is a person within the meaning of Section 2402 of the Insurance Law, and as such, is within the jurisdiction of the Department for purposes of this hearing, which is brought against the Respondent pursuant to Article 24 of the Insurance Law.

(B) This Notice of Hearing and Statement of Charges is issued to Respondent pursuant to Section 2405 of the Insurance Law and Sections 305 and 306 of the Financial Services Law, and notice of the hearing is given to Respondent in accordance with Section 304 of the Financial Services Law.

(C) Your attention is directed to a statement in plain language, attached hereto as Appendix A, summarizing the provisions of 23 NYCRR Part 2. **This statement contains important information concerning your rights and the Department's hearing procedures and should be read carefully.** A copy of 23 NYCRR Part 2 will be furnished upon request.

(D) Interpreter services shall be made available to deaf persons, at no charge.

(E) Should you fail to appear at the time and place set forth above, or at any subsequent date fixed for the hearing, the hearing will proceed as scheduled and may result in the following:

i. The issuance of a report by the Superintendent finding defined violations of 23 NYCRR Part 500 and the issuance of an order upon the Respondent requiring it to remedy the defined violations; and

ii. The assessment of civil monetary fines against the Respondent pursuant to Financial Services Law Section 408.

Dated: New York, New York
July 21, 2020

NEW YORK STATE
DEPARTMENT OF FINANCIAL SERVICES

By: _____
KATHERINE A. LEMIRE
Executive Deputy Superintendent
Consumer Protection and Financial Enforcement

By: _____
JUSTIN S. HERRING
Executive Deputy Superintendent
Cybersecurity Division

ELIZABETH A. FARID
DESIREE S. MURNANE
MADELINE W. MURPHY
Of Counsel

One State Street
New York, New York 10004
(212) 709-5578