POMERANTZ LLP
Jennifer Pafiti (SBN 282790)
1100 Glendon Avenue, 15th Floor
Los Angeles, CA 90024
Telephone: (310) 405-7190
jpafiti@pomlaw.com
Counsel for Lead Plaintiff and the Class
(additional counsel listed on signature page)

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

In re First American Financial Corp. Securities Litigation	Case No. CV 20-9781 DSF (Ex) **CLASS ACTION** **AMENDED CLASS ACTION COMPLAINT FOR VIOLATIONS OF THE FEDERAL SECURITIES LAWS** Hon. Dale S. Fischer **JURY TRIAL DEMANDED**

Lead Plaintiff St. Lucie County Fire District Firefighters Pension Trust Fund ("Plaintiff"), individually and on behalf of all other persons similarly situated, by Plaintiff's undersigned attorneys, for Plaintiff's complaint against Defendants, alleges the following based upon personal knowledge as to Plaintiff and Plaintiff's own acts, and information and belief as to all other matters, based upon, *inter alia*, the investigation conducted by and through Plaintiff's attorneys, which included, among other things, conversations with former employees, a review of the First American

Financial Corp.'s ("First American" or "the Company") public documents, conference calls and announcements, United States Securities and Exchange Commission ("SEC") filings, wire and press releases published by and regarding First American, analysts' reports and advisories about the Company, and information readily obtainable on the Internet. Plaintiff believes that substantial additional evidentiary support will exist for the allegations set forth herein after a reasonable opportunity for discovery.

NATURE OF THE ACTION

1. This case arises from Defendants' material misrepresentations to investors between February 17, 2017 through October 22, 2020, both dates inclusive (the "Class Period"), regarding known deficiencies in First American's security practices, policies, and controls, in violation of Sections 10(b) and 20(a) of the Securities Exchange Act of 1934 (the "Exchange Act") and Rule 10b-5 promulgated thereunder. In particular, as detailed herein, Defendants falsely represented to the market that:

- First American had "implement[ed] fundamentally sound security policies" with respect to sensitive consumer data;
- they would "use [their] best efforts to ensure that no unauthorized parties have access to any [customer nonpublic personal] information;
- access to nonpublic personal information would be heavily "restrict[ed]";

- they would "use [their] best efforts … to ensure that your information will be handled responsibly ….";
- "the integrity of the Company's computer systems and the protection of the information that resides on those systems" was "critically important" to First American;
- they "currently maintain[ed] physical, electronic, and procedural safeguards … to guard [customer] nonpublic personal information";
- they "offer[ed] secure, reliable, and affordable records storage"; and
- they applied a heightened "layer of protection …. "to information that belongs to our customers." [*See* ¶¶57, 61, 64, 70, 73, 74, 79, *infra*].

2. These representations were false, and the truth diverged sharply from the rosy picture Defendants painted for investors: First American had, in fact, exposed hundreds 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.

3. Defendants were also misleading when speaking to investors of a potential risk that they may not effectively shield "highly sensitive non-public personal information" from exposure due to increasingly sophisticated "cyber attacks, phishing attacks, and other malicious activity," omitting entirely that such information was

already exposed because First American had ***itself*** published customer personal non-public information ("NPI") without encryption, access controls, or other basic security on its public-facing website. Nor did Defendants disclose that their own information security department disclaimed responsibility for protecting NPI.

4. Specifically, from at least the start of the Class Period through May 2019, Defendants misrepresented their security practices and controls to investors, and concealed the fact that the Company had declined to protect customer data including highly-sensitive NPI records, allowing them to be accessed by anyone with a web browser via First American's public-facing website (the "Breach"). Defendants continued to conceal these crucial, known vulnerabilities even after they were confronted with indisputable evidence documenting the Breach from a penetration test reported internally in December 2018.

5. Rather than come clean to investors, however, Defendants continued to misrepresent the internally-known facts while the personal and financial data of millions of First American customers remained exposed for the taking by hackers and identity thieves for more than six months.

6. Defendants' empty assurances to First American's investors began to crumble on May 24, 2019, when noted cybersecurity expert Brian Krebs reported on his blog, KrebsOnSecurity.com, the massive Breach previously concealed by First

American. In a post that was published after the market closed, Mr. Krebs explained that more than ***850 million*** customer files, dating back sixteen years, were exposed. KrebsOnSecurity further reported that no authentication whatsoever was required to read the exposed documents. In direct response to these revelations, shares of First American fell $3.46, or over 6%, to close at $51.80 on May 28, 2019, the next trading day.

7. Despite the KrebsOnSecurity disclosures, Defendants continued to downplay the severity of the Breach, thereby continuing the deception that existed at the start of the Class Period.

8. On July 22, 2020, the New York State Department of Financial Services ("NYDFS") charged First American with multiple violations of state cybersecurity regulations. After filing its initial charges, NYDFS obtained books and records from First American, which were incorporated into Amended Charges and Notice of Hearing ("NYDFS Amended Charges"). Hearing on those charges has not yet commenced.

9. Then, on October 22, 2020, First American announced it had received a Wells Notice, *i.e.*, a letter from the SEC telling a recipient that the agency is planning to bring enforcement actions.

10. On this news, the price of First American shares fell approximately $4.83 per share, or 9%, to close at $46.75 per share on October 22, 2020.

11. As a result of Defendants' wrongful acts and omissions, several hundreds of millions of dollars of market capitalization were wiped out, causing Plaintiff and other Class members to suffer significant losses and damages.

JURISDICTION AND VENUE

12. The claims asserted herein arise under Sections 10(b) and 20(a) of the Exchange Act, 15 U.S.C. §§ 78j(b) and 78t(a), and Rule 10b-5 promulgated thereunder, 17 C.F.R. § 240.10b-5.

13. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1331 and Section 27 of the Exchange Act, 15 U.S.C. § 78aa.

14. Venue is proper in this District pursuant to Section 27 of the Exchange Act, 15 U.S.C. § 78aa, and 28 U.S.C. § 1391(b). First American is headquartered in this District. Defendants also regularly conduct business in this District, and a significant portion of Defendants' actions including their representations to investors took place within this District.

15. In connection with the acts alleged in this complaint, Defendants, directly or indirectly, used the means and instrumentalities of interstate commerce, including, but not limited to, the mails, interstate telephone communications, and the facilities of the national securities markets.

PARTIES

16. Plaintiff, as set forth in its previously-filed Certification [ECF No. 26-3], acquired First American securities at artificially inflated prices during the Class Period and was damaged upon the corrective disclosures and/or materializations of concealed risks alleged herein.

17. Defendant First American is a Fortune 500 company with over $5 billion in revenue. Through its subsidiaries, First American provides title insurance and other financial services. The Company is incorporated in Delaware and its principal executive offices are located at 1 First American Way, Santa Ana, CA 92707. First American's securities are traded on the New York Stock Exchange under the ticker symbol "FAF."

18. Defendant Dennis J. Gilmore ("Gilmore") was the Chief Executive Officer ("CEO") and a Director of First American throughout the Class Period, and at all times relevant hereto. Defendant Gilmore signed each of First American's Form 10-Q and Form 10-K filings identified herein, and also provided for each a certification pursuant to the Sarbanes-Oxley Act of 2002 certifying the accuracy of the information reported therein.

19. Defendant Mark E. Seaton ("Seaton") was the Chief Financial Officer ("CFO") and Executive Vice President of First American throughout the Class Period, and at all times relevant hereto. Defendant Seaton signed each of First American's

Form 10-Q and Form 10-K filings identified herein, and also provided for each a certification pursuant to the Sarbanes-Oxley Act of 2002 certifying the accuracy of the information reported therein.

20. Defendant Shabnam Jalakian ("Jalakian") was the Chief Information Security Officer ("CISO") of First American throughout the Class Period, and at all times relevant hereto.

21. The Defendants referenced above in ¶¶18-20 are sometimes referred to herein collectively as the "Individual Defendants."

22. The Company and the Individual Defendants are referred to herein collectively as the "Defendants."

23. Defendants Gilmore and Seaton possessed the power and authority to control the contents of the Company's SEC filings, press releases, and other market communications. They were provided with copies of the Company's SEC filings and press releases alleged herein to be misleading prior to or shortly after their issuance and had the ability and opportunity to prevent their issuance or to cause them to be corrected. Likewise, Defendant Jalakian had the power and authority to control the contents of information and statements attributed to her. In addition to their positions with the Company, each had access to material information available to them but not to the public, and consequently knew that the adverse facts specified herein had not been

disclosed to and were being concealed from the public, and that the positive representations being made were then materially false and misleading. The Individual Defendants, in their respective capacities, are liable for the false statements and omissions pleaded herein.

SUBSTANTIVE ALLEGATIONS

Background

24. First American is the second largest title insurance provider in the United States. Title insurance policies insure the interests of owners and lenders against defects in the title to real property. These defects include adverse ownership claims, liens, encumbrances, or other matters affecting title. Title insurers also oversee the financial settlement of residential housing sales transactions at closing, and therefore possess extensive non-public financial information and records about buyers and sellers.

25. In 2019, First American's Title Insurance and Services segment accounted for 91.5% of the Company's $6.2 billion in consolidated revenue. Significantly, the Breach occurred in this core operation, and related to a core function of the core operation—the protection of customer NPI.

26. In performing title searches and facilitating closings, First American obtains from buyers, sellers, and internal and external databases documents that regularly contain highly-sensitive personal non-public information such as credit reports, escrow account balances, Social Security numbers, wire information and

banking and investment account numbers. First American also regularly collects records such as tax assessments and liens to include as part of a title insurance package (the "title package").

27. Defendants have readily and repeatedly acknowledged that protecting consumer data was crucial to First American's business operations, including to its core Title Insurance and Services segment. For example, the Company's annual report filed with the SEC in February 2017 – which was signed by Defendants Gilmore and Seaton – stated that "we are focused on growing our core title insurance and settlement services business, ***strengthening our enterprise through data and process advantages***. . ." (Emphasis added.)

28. Likewise, a 2017 Investor Letter published by Defendant Gilmore stated under "Capital Management" that much of the Company's recent investments had been directed toward technology, including "***the continued enhancement of our title production platform and our customer-facing technologies and enterprise systems***, all of which will improve our customers' experience and our internal process efficiency." (Emphasis added.)

29. In the same letter, Gilmore goes on to state: "Strengthen the enterprise through data and process advantage ... ***These efforts strengthen our control over the key data assets that underlie our products and services and facilitate our efforts to***

manage risk and drive efficiencies throughout the title and settlement process." (Emphasis added.)

30. In the regular course of its business, First American collects, stores, and transmits the personal information of millions of buyers and sellers of real estate in the U.S. each year. First American stores this information in its main document repository, the FAST image repository, also known as "FAST."

31. FAST stores tens of millions of documents with sensitive personal information, such as social security numbers, bank account and wiring information, and mortgage and tax records. Documents can be loaded into FAST by First American's employees assigned to any of First American's business units. First American uses documents stored in FAST to transact title insurance and settlement orders. Defendants conceded understanding during the Class Period that "the protection of the information that resides on those systems are critically important to [First American's] successful operation."

32. On February 16, 2017, one of First American's regulators – the NYDFS – implemented comprehensive cybersecurity requirements effective March 1, 2017. The new cybersecurity requirements, among other things:

- Required First American to maintain a Chief Information Security Officer reporting to the Board of Directors; and

- Required First American to "maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the covered entity's information systems," based on a "risk assessment" that was supposed to have been conducted by First American and "designed to perform the following core cybersecurity functions:"

(1) "identify and assess internal and external cybersecurity risks that may threaten the security or integrity of nonpublic information stored on the covered entity's information systems;"

(2) "use defensive infrastructure and the implementation of policies and procedures to protect the covered entity's information systems, and the nonpublic information stored on those information systems, from unauthorized access, use or other malicious acts;"

(3) "detect cybersecurity events;"

(4) "respond to identified or detected cybersecurity events to mitigate any negative effects;"

(5) "recover from cybersecurity events and restore normal operations and services;" and

(6) "fulfill applicable regulatory reporting obligations."

- Required First American to conduct a periodic risk assessment that is "updated as reasonably necessary to address changes to the covered entity's

information systems, nonpublic information or business operations" and "shall consider the particular risks of the covered entity'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" and

- Required First American to "implement controls, including encryption, to protect nonpublic information…." [*See* NYCRR, Title 23, Part 500].

First American's Longstanding – and Internally-Known – Data Security Issues

33. First American understood the dangers posed by poor data security practices throughout the Class Period. ***Since at least 2017, First American repeatedly identified vulnerabilities and vulnerability management as among its own top risks***. (Emphasis added.)

34. Notwithstanding its understanding about the importance of information security, First American internally acknowledged extensive vulnerabilities that it concealed during the Class Period from investors. As an initial matter, First American withheld from investors that it had identified extensive vulnerabilities and declined to remediate those vulnerabilities as required by its own policies. These deviations were hidden from investors during the Class Period. According to First American's own policies, it was supposed to:

a. scan all information assets for vulnerabilities, and provide a security overview report for each application and a risk assessment for data stored or transmitted by any application;

b. remediate critical or high risk vulnerabilities within 15 days;

c. remediate medium risk vulnerabilities within 45 days; and

d. remediate low risk vulnerabilities within 90 days.

35. Unbeknownst to investors, First American deviated from these policies. ***No security overview or risk assessment was performed for EaglePro***, and tens of thousands of critical or high risk vulnerabilities were permitted to persist for long periods of time without remediation.

36. According to records disclosed in the NYDFS Amended Charges, First American knew about dangerous vulnerabilities both before and throughout the Class Period. Additionally, after interviewing First American's CISO, Defendant Jalakian, and its former Senior Director, Information Security as well as reviewing internal records, the NYDFS determined that "***First American's CISO and senior personnel were fully aware of the disastrous state of First American's vulnerability management***." (Emphasis added.)

37. First American's records confirm that mounting problems were known and quantified internally. For example, as summarized by the NYDFS Amended Charges:

a. In a December 2016 report to the Board Audit Committee, First American's management reported that they conducted a self-assessment of their vulnerability and patching program in Q2 2016, and that they needed to re-engineer the process of vulnerability scanning and patching.

b. A 2017 information security audit identified significant vulnerability management problems. The audit found a failure to assign responsibility for the detailed tracking and performance of vulnerability remediation, and inadequate system for tracking vulnerabilities.

c. By October 3, 2018, internal records tabulated 26,873 critical/high vulnerabilities that were unresolved for more than 90 days, including a staggering 11,000 critical and high-risk vulnerabilities that First American had failed to remediate for more than 3 years. There were an additional 8,782 critical/high vulnerabilities that were left unremediated for 2 to 3 years. ***These were vulnerabilities for which First American's policies required remediation with 15 days.***

d. An early 2018 test of NPI classification indicated that while 65 million of the 753 million documents then in FAST were tagged as

containing NPI, hundreds of millions of documents not tagged were likely misclassified and did in fact contain sensitive NPI that required protection. Specifically, a random sampling of 1,000 non-tagged documents showed that 30% actually contained NPI, a finding that was discussed with the Board of Directors in April 2018. Although Defendants had actual knowledge of this vulnerability, they neither remediated it at the time nor enhanced their boilerplate disclosures.

e. A 2018 internal audit of First American's Vulnerability Management Program ("2018 Audit Report") prepared for First American's management and Board found serious deficiencies and rated the program as "Major Improvement Needed," meaning that the program is "***unlikely to provide reasonable assurance that risks are being managed and objectives are being met***." The audit found that "remediation of known vulnerabilities is not completed timely," AROs were not remediating vulnerabilities in a timely manner, and there was no mechanism to ensure timely remediation.

f. The 2018 audit report also found serious problems throughout First American's remediation management governance, such as a failure to document waivers when vulnerabilities were not remediated

according to policy, incomplete scanning for vulnerabilities, lack of effective reporting to senior management and the board, a lack of analysis of vulnerabilities, and a lack of prioritization of vulnerability remediation.

g. In a March 6, 2019 presentation to the Board, Defendant Jalakian acknowledged that the Company had over 100,000 unremediated critical/high vulnerabilities.

h. By November 11, 2019, First American's records show more than 320,000 high or critical unremediated vulnerabilities. By December 2, 2019, First American had identified an ***additional*** 131,000 high or critical vulnerabilities requiring remediation.

38. Defendant Jalakian regularly discussed with the Board and senior management the security problems that Defendants withheld from investors during the Class Period. As she explained during a panel discussion in the Center for Digital Transformation conference at the University of California-Irvine entitled "Cybersecurity: Is There Such A Thing?" on April 19, 2018: "***I personally meet with the board quarterly with the audit committee, also quarterly. I meet with our CEO monthly, or more often as the need may arise.*** I speak to our shareholders regularly. So, I mean, ***there are a lot of frequent touch points***, which is the lay of the land today."

(Emphasis added.) As a result of these "frequent touch points," there can be no question that the deficiencies known to Defendant Jalakian were also known to Defendant Gilmore and the rest of First American's Board and senior management.

The Data Breach

39. First American 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 First American 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.

40. 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 title package without login or authentication.

41. In October 2014, First American introduced the security flaws into the EaglePro system that gave rise to the Breach. The URL for each website shared via EaglePro included an ImageDocumentID number, and each document in FAST was assigned a sequentially numbered ImageDocumentID. First American did not password protect the documents, and did not control access to documents by ImageDocumentID.

As a result, by changing the ImageDocumentID number in the URL, any document in FAST could be accessed regardless of whether the viewer should have been permitted access. Even worse, scripts could rapidly access thousands if not millions of unauthorized and sensitive documents simply by incrementing the ImageDocumentID. The following is a redacted screenshot of just one of the hundreds of millions of sensitive records exposed by First American's website:

Seller Information

Escrow No. [redacted]

Seller 1 Name: [redacted] **SSN:** [redacted]

Seller 2 Name: **SSN:**

Current Marital Status: Divorced

Telephone Number(s):
Seller 1: [redacted] Home / Work / (Cell) / Fax (circle one)

Seller 2: Home / Work / Cell / Fax (circle one)

Email address:
Seller 1: [redacted]

Seller 2:

Current Mailing Address: [redacted]
Street Address

Scottsdale (City) AZ (State) 85266 (Zip)

Forwarding Address:
(After Sale of Property)
Street Address

City State Zip

Please complete the following information and return as soon as possible:
(Be sure to include pool loans, water softener loans, & equity credit lines)

1st Mortgage: Lender Name: SLS
Address: 8742 Lucent Blvd Suite 300 Highlands Ranch, CO 80129
Loan No: [redacted] Phone No. 800 315 4757

2nd Mortgage: Lender Name:
Or EQUITY Address:
CREDIT LINE Loan No: Phone No.

42. First American compounded this security flaw by refusing to provide any time limitation upon accessing the URLs shared via EaglePro, to which they assigned no expiration date. Due to Defendants' security practices, more than 850 million documents were accessible to anyone with a URL address providing access to a single document in the EaglePro-generated website.

43. Despite widespread characterization of the data exposure event as a vulnerability, which "is a weakness in a system that can be easily exploited ***if found by an attacker***" (emphasis added.), it is properly termed a breach.[1] This is because unlike vulnerabilities, "[b]reaches are successful attacks in which the hacker obtains business/personal data."[2]

44. First American's own analysis demonstrated that during an 11-month period starting in June 2018, more than 350,000 documents ***were in fact accessed*** without authorization by automated "bots" or "scraper" programs designed to collect information on the Internet. Because it is beyond dispute that data was actually taken in the course of First American's data exposure, the event is properly referred to as a breach, and not a vulnerability.

[1] https://blog.digitalwest.com/blog/what-is-the-difference-between-a-security-vulnerability-threat-and-breach

[2] *Id.*

45. The Breach 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 First American.

46. As *Forbes* writer A.J. Dellinger stated on May 26, 2019, two days after the Breach was revealed:

> The trouble with a data exposure like the one at First American is that it's hard to pinpoint exactly how many people are actually affected. If everyone got lucky, this huge cache of sensitive files sat online, undetected and most everyone is in the clear. ***But the worst case scenario is that every last one of those files was captured, saved, and could be used in the future to target individuals and companies***. (Emphasis added.)[3]

47. While the data exposure was unquestionably unknown to Defendants prior to December 2018, *see* ¶¶36, 37(a)-(b), *supra*, the Breach was confirmed that month by a test team during a penetration test of the EaglePro application of the type that the recently-enacted NYDFS regulations required, ¶32, *supra*.

48. On January 11, 2019, the final report of the EaglePro penetration test described the Breach in detail, including pages of screenshots demonstrating how the

[3] *See* https://www.forbes.com/sites/ajdellinger/2019/05/26/understanding-the-first-american-financial-data-leak-how-did-it-happen-and-what-does-it-mean/?sh=38eb720f567f

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 indexed by Google, ***facilitating public searches whether or not the ImageDocumentID was known***. The report further warned that: "using standard Internet search methods we were able to bypass authentication to retrieve documents that were found using Google searches" (emphasis in the original). Although the testers only bothered to review ten (10) exposed documents, they acknowledged that further investigation was immediately required to determine whether sensitive documents were exposed. Despite this clear warning, Defendants neither conducted the necessary review nor informed investors of the Breach. Instead, they continued to hide behind the same boilerplate statements regarding cybersecurity.

49. To identify and classify sensitive documents containing NPI, First American relied solely on a manual process in which title agents, in the course of uploading documents, typed in the prefix "SEC" to the name for each file to be protected; otherwise, the file was not flagged as containing NPI. First American made no effort to confirm the efficacy of this control prior to April 2018, nor implemented any non-manual alternative processes. Defendants were fully aware that this methodology — by a wide margin — failed to identify and protect documents containing NPI. For instance, according to NYDFS:

i. In April 2018, a presentation by senior members of First American'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 misdesignated, and not properly protected.

ii. A June 1, 2019 email from First American'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."

50. Even after a third-party disclosed the Breach concealed by Defendants, senior management vetoed internal recommendations to improve security of EaglePro. In June 2019, First American's information security personnel recommended modifying EaglePro to limit access to authenticated users. Senior management rejected that recommendation. First American'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, recognizing that manual tagging was insufficient, they recommended a comprehensive

scan of FAST for documents not manually tagged to determine whether they actually contained sensitive NPI. Neither recommendation was implemented.

51. When NYDFS asked First American's CISO, Defendant Jalakian, why additional controls were not adopted to protect NPI, she disavowed ownership of the issue, stating, among other reasons, that such controls were not the responsibility of First American's information security department.

52. First American also failed to timely encrypt documents containing NPI as required by NYDFS's Cybersecurity Regulation. In particular, First American 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 First American knew included many documents containing NPI — were not fully encrypted until mid-2019.

53. Former Employee ("FE") 1 worked as a security engineer at First American from July 2016 to November 2020. Based at the company's Santa Ana, CA headquarters, FE1 reported to Cyber Defense Manager Christina Carson.

54. FE1 was alerted to the EaglePro vulnerability when his colleague, Senior Information Security Engineer John Rehagen, documented that sensitive information was accessible outside of the network during a December 2018 penetration test.

55. FE1 said that a high severity incident like the EaglePro vulnerability should have taken priority for remediation. Instead, First American hadn't started remediating the EaglePro vulnerability when KrebsOnSecurity published its article in May 2019.

56. Indeed, FE2, who worked as a director of information security for First American from July 2018 to September 2020 and reported directly to Defendant Jalakian at the time of the Breach, confirms that the Company did not begin to address the Breach until May 24, 2019, the same day that the Krebs article was published.

Materially False and Misleading Statements Issued During the Class Period

57. The Class Period begins on February 17, 2017, when First American filed an annual report on Form 10-K with the SEC for the fiscal year December 31, 2016 (the "2016 10-K"). In the 2016 10-K, which was signed by Defendants Gilmore and Seaton, Defendants stated that:[4]

> ***The Company uses computer systems to receive, process, store and transmit business information, including highly sensitive non-public personal information as well as data from suppliers and other information upon which its business relies. It also uses these systems to manage substantial cash, investment assets, bank deposits, trust assets and escrow account balances on behalf of the Company and its customers, among other activities***. Many of the Company's products, services and solutions involving the use of real property related data are fully reliant on its systems and are only available

[4] Emphasis added throughout, unless otherwise noted.

> electronically. Accordingly, for a variety of reasons, ***the integrity of the Company's computer systems and the protection of the information that resides on those systems are critically important to its successful operation***. The Company's core computer systems are primarily located in two data centers. The Company recently took over management of its primary data center and the secondary data center is maintained and managed by a third party.

58. The statements referenced in ¶57 were materially false and misleading because they omitted the following information necessary to make them not misleading under the circumstances in which they were made: (1) the Company failed to implement basic security standards to protect its customers' sensitive personal information and data from unauthorized access and other malicious acts; (2) the Company disregarded its own information security policies; and (3) as a result of (1) and (2), the Company did not protect but instead exposed tens of millions of documents containing sensitive customer NPI.

59. Defendants further stated that:

> The Company's computer systems and systems used by its agents, suppliers and customers ***have been subject to, and are likely to continue to be the target of, computer viruses, cyber attacks, phishing attacks and other malicious attacks***. These attacks have increased in frequency and sophistication in recent years, and could expose the Company to system-related damage, failures, interruptions, and other negative events. ***Further, certain other potential causes of system damage or other negative system-related events are wholly or partially beyond the Company's control***, such as natural disasters, vendor failures to satisfy service level requirements and power or telecommunications failures. ***These incidents, regardless of their underlying causes, could disrupt the Company's business and could also result in the loss or unauthorized release, gathering, monitoring or***

destruction of confidential, proprietary and other information pertaining to the Company, its customers, employees, agents or suppliers.

60. The statements referenced in ¶59 were materially false and misleading because they omitted the following information necessary to make them not misleading under the circumstances in which they were made: (1) the Company failed to implement basic security standards to protect its customers' sensitive personal information and data from unauthorized access and other malicious acts; (2) the Company disregarded its own information security policies; (3) as a result of (1) and (2), the Company itself – and not cyber attacks or malicious third parties – had exposed non-public information; and (4) the release of confidential customer information that the Company discussed prospectively had in fact already occurred and continued to occur.

61. During 2017, First American's website stated, under the heading "Privacy Information":

> **We Are Committed to Safeguarding Customer Information**
>
> In order to better serve your needs now and in the future, we may ask you to provide us with certain information. We understand that you may be concerned about what we will do with such information – particularly any personal or financial information. ***We agree that you have a right to know how we will utilize the personal information you provide to us***. Therefore, together with our subsidiaries ***we have adopted this Privacy Policy to govern the use and handling of your personal information***.
>
> * * *
>
> **Types of Information**

Depending upon which of our services you are utilizing, the types of nonpublic personal information that we may collect include:

- Information we receive from you on applications, forms and in other communications to us, whether in writing, in person, by telephone or any other means;

- Information about your transactions with us, our affiliated companies, or others; and

- Information we receive from a consumer reporting agency.

Use of Information

We request information from you for our own legitimate business purposes and not for the benefit of any nonaffiliated party. Therefore, ***we will not release your information to nonaffiliated parties except: (1) as necessary for us to provide the product or service you have requested of us; or (2) as permitted by law***. We may, however, store such information indefinitely, including the period after which any customer relationship has ceased. Such information may be used for any internal purpose, such as quality control efforts or customer analysis. We may also provide all of the types of nonpublic personal information listed above to one or more of our affiliated companies. Such affiliated companies include financial service providers, such as title insurers, property and casualty insurers, and trust and investment advisory companies, or companies involved in real estate services, such as appraisal companies, home warranty companies and escrow companies.

* * *

Former Customers

Even if you are no longer our customer, our Privacy Policy will continue to apply to you.

Confidentiality and Security

We will use our best efforts to ensure that no unauthorized parties have access to any of your information. We restrict access to nonpublic personal information about you to those individuals and entities who need to know

that information to provide products or services to you. We will use our best efforts to train and oversee our employees and agents to ensure that your information will be handled responsibly and in accordance with this Privacy Policy and First American's.

Fair Information Values.
We currently maintain physical, electronic, and procedural safeguards that comply with federal regulations to guard your nonpublic personal information.

Information Obtained Through Our Web Site
First American Financial Corporation is sensitive to privacy issues on the Internet ...

Fair Information Values

Fairness We consider consumer expectations about their privacy in all our businesses. We only offer products and services that assure a favorable balance between consumer benefits and consumer privacy.

Public Record We believe that an open public record creates significant value for society, enhances consumer choice and creates consumer opportunity. We actively support an open public record and emphasize its importance and contribution to our economy.

Use ***We believe we should behave responsibly when we use information about a consumer in our business.*** We will obey the laws governing the collection, use and dissemination of data.

Accuracy We will take reasonable steps to help assure the accuracy of the data we collect, use and disseminate. Where possible, we will take reasonable steps to correct inaccurate information. When, as with the public record, we cannot correct inaccurate information, we will take all reasonable steps to assist consumers in identifying the source of theerroneous data so that the consumer can secure the required corrections.

Education ***We endeavor to educate the users of our products and services, our employees and others in our industry about the importance of consumer privacy.*** We will instruct our employees on our fair information values and on the responsible collection and use of data. We will encourage others in our industry to collect and use information in a responsible manner.

Security ***We will maintain appropriate facilities and systems to protect against unauthorized access to and corruption of the data we maintain.***

62. The statements referenced in ¶61 were materially false and misleading because they omitted the following information necessary to make them not misleading under the circumstances in which they were made: (1) the Company failed to implement basic security standards to protect its customers' sensitive personal information and data from unauthorized access and other malicious acts; (2) the Company disregarded its own information security policies; and (3) as a result of (1) and (2), the Company did not protect but instead exposed tens of millions of documents containing sensitive customer NPI.

63. On April 24, 2017, Defendants filed an annual report on Form 10-Q with the SEC for the quarter ending March 31, 2017 (the "2017 Q1 10-Q"). In the 2017 Q1 10-Q, which was signed by Defendants Gilmore and Seaton, Defendants made substantially-similar representations as found in the portions of the 2016 10-K quoted in ¶¶57 & 59 above and which were false and/or misleading for the reasons explained in ¶¶58 & 60 above.

64. Defendants also made misrepresentations in a series of magazines and newsletters that First American disseminated in various markets under the names *Agency Today, Agency Connect, Agent Angle, Florida Legal Eagle, The Pronghorn Press, Illinois Hot Topics, Vermont Spotlight,* and *Big Sky Review*. Feature articles were

replicated word-for-word across the titles. On or around May 3, 2017, Defendant Jalakian stated in such a feature article that:

> ***First American has established a formal information security program, led by the Corporate Information Security office, to continuously oversee and strengthen our security and privacy practices. This is accomplished by implementing fundamentally sound security policies as well as repeatable processes, best-of-breed technology solutions, and regular awareness training.*** *The objective of information security is to support the business and maximize stakeholder benefit while protecting the information assets of both the Company and its customers from all relevant threats*.

See, e.g., "Executive Spotlight: Shabnam Jalakian," Florida Legal Eagle, Vol. VII (May 3, 2017). On information and belief, based upon First American's practice of replicating feature articles across its line of publications, First American also disseminated this article and the misrepresentations contained therein through the other aforementioned First American publications at approximately the same time.

65. Defendant Jalakian further claimed that the Company was "serious" about "the protection of information [consumers] entrust in our care," and encouraged the Company's underwriters "to be security evangelists for our customers and borrowers who may not have the same level of security protections at their disposal" as First American customers supposedly did. *Id.*

66. The statements referenced in ¶¶64-65 were materially false and misleading because: (1) the Company had not "implement[ed] fundamentally sound security

policies"; (2) the Company had not implemented "best-of-breed technology solutions" with respect to crucial NPI and encryption; (3) the Company lacked controls to properly classify or protect non-public information; (4) the Company's Corporate Information Security Office did not "continuously oversee and strengthen…security and privacy practices," and in fact later disclaimed any responsibility for protecting customer NPI; (4) the statements omitted that neither First American, Defendant Jalakian nor the Company's Corporate Information Security Office implemented basic widely-accepted measures necessary to "protect[] the information assets of both the Company and its customers from all relevant threats," which information was necessary to make the statements made not misleading under the circumstances in which they were made.

67. On May 17, 2017, Defendants took part in the Barclays Americas Select Conference. During the conference, Defendant Seaton stated that:

> We spend about $130 million a year in capital expenditures. And that's about as much as we could spend responsibly. So ***we spend that in technology, in customer-facing technology to make it easier for our customers to do business with us. We spend capital on building our databases, to make our business more efficient.*** That's our #1 priority is to continue to build our business organically.

68. The statements referenced in ¶67 were materially false and misleading because they omitted the following material information necessary to make the statements made not misleading under the circumstances in which they were made: (1) the Company failed to implement basic security standards to protect its customers'

sensitive personal information and data from unauthorized access and other malicious acts; (2) the Company lacked controls to properly classify or protect non-public information; and (3) Defendants' technology program compromised not strengthened First American's relationship with its customers by exposing their sensitive data.

69. On July 27 and October 26, 2017, Defendants filed quarterly reports on Form 10-Q with the SEC for the second and third quarters of 2017, respectively. Each was signed and certified by Defendants Gilmore and Seaton, and contained the same misrepresentations identified with respect to the portions of the 2016 10-K quoted in ¶¶57 & 59, above and which were false and/or misleading for the reasons explained in ¶¶58 & 60, above.

70. During 2018, First American's website stated as follows:

> *Post-Closing Document Management*
> ... Let us store your records in our secure facility that is monitored 24-hours a day. And, of course, you always have online access to your and your customers' documents, any time, day or night.
>
> * * *
>
> *Secure Document Storage*
> ***We offer secure, reliable, and affordable records storage solutions for your needs of any size to help you manage active mortgage collateral files.***
>
> Imaged Documents Reviewed for Deficiencies (capture critical data elements, report missing documents & interfile trailing documents)
> State-of-the-art Document Tracking System

Online Access for Document Viewing, Shipping Request Fulfillment & Client-specific Inventory Reports

Secure Facility Monitored 24-hours a day

* * *

Secure access to files which provides our clients with detailed information concerning their REO property closing status

71. The statements referenced in ¶70 were materially false and misleading when made because: (1) access to online documents was not secured; and (2) the statements omitted the following material information necessary to make the statements made not misleading under the circumstances in which they were made: (a) contrary to First American's privacy policy, the Company failed to implement basic security standards to protect its customers' sensitive personal information and data from unauthorized access and other malicious acts; (b) the Company disregarded its own information security policies; and (c) as a result of (a) and (b), the Company did not protect but instead exposed tens of millions of documents containing sensitive customer NPI.

72. On April 19, 2018, Defendant Jalakian spoke at the Center for Digital Transformation at University of California Irvine as part of a panel discussion entitled "Cybersecurity: Is There Such A Thing?" that included Yan Permeh, Co-Founder and

Chief Scientist of Cylance and Scott Zogg, Chief Security Office at Rockwell Collins. At the CDT conference, Defendant Jalakian stated, in relevant part:

> So, the strategy that works for us, we... Again, technical tools, we employ a number of them. We spend millions of dollars a year on technical security, but I think what is really critical is identifying key business processes in a company. So, where does your money come from? Where do you collect data from? So, really understanding the business from the perspective of people who do the work and bring the money and the data in. And then figuring out what are the crown jewels that need the most amount of security. Again, in our case we collect a lot of publicly available data. Okay. ***So the security we apply to that layer of data is clearly different than the layer of security we apply to information that belongs to our customers. That belongs to the lenders that we deal with***.

73. The statements referenced in ¶72 were materially false and misleading because: (1) Defendant Jalakian did not "understand[] the business from the perspective of people who do the work and bring the money and the data in"; (2) the Company did not provide the additional "layer of protection" to customer NPI data that Defendant Jalakian claimed; and (3) the statements omitted the following material information necessary to make the statements made not misleading under the circumstances in which they were made: (a) contrary to First American's privacy policy, the Company failed to implement basic security standards to protect its customers' sensitive personal information and data from unauthorized access and other malicious acts; (b) the Company disregarded its own information security policies; and (c) as a result of (a) and

(b), the Company did not protect but instead exposed tens of millions of documents containing sensitive customer NPI.

74. On February 16, 2018, First American filed an annual report on Form 10-K with the SEC for the fiscal year December 31, 2017 (the "2017 10-K"). In the 2017 10-K, which was signed by Defendants Gilmore and Seaton, Defendants stated that:

> ***The Company uses computer systems to receive, process, store and transmit business information, including highly sensitive non-public personal information as well as data from suppliers and other information upon which its business relies. It also uses these systems to manage substantial cash, investment assets, bank deposits, trust assets and escrow account balances on behalf of the Company and its customers, among other activities***. Many of the Company's products, services and solutions involving the use of real property related data are fully reliant on its systems and are only available electronically. Accordingly, for a variety of reasons, ***the integrity of the Company's computer systems and the protection of the information that resides on those systems are critically important to its successful operation.*** The Company's core computer systems are primarily located in a data center it manages and secondarily in a disaster recovery data center maintained by a third party. The Company is currently engaged in a multi-year process of transitioning to third party cloud-based hosting of its computer systems.

75. The statements referenced in ¶74 were materially false and misleading because they omitted the following information necessary to make them not misleading under the circumstances in which they were made: (1) the Company failed to implement basic security standards to protect its customers' sensitive personal information and data from unauthorized access and other malicious acts; (2) the Company disregarded its own information security policies; and (3) as a result of (1) and (2), the Company did not

protect but instead exposed tens of millions of documents containing sensitive customer NPI.

76. Defendants further stated in the 2017 10-K that:

> The Company's computer systems and systems used by its agents, suppliers and customers ***have been subject to, and are likely to continue to be the target of, computer viruses, cyber attacks, phishing attacks and other malicious attacks***. These attacks have increased in frequency and sophistication in recent years, and could expose the Company to system-related damage, failures, interruptions, and other negative events. ***Further, certain other potential causes of system damage or other negative system-related events are wholly or partially beyond the Company's control***, such as natural disasters, vendor failures to satisfy service level requirements and power or telecommunications failures. ***These incidents, regardless of their underlying causes, could disrupt the Company's business and could also result in the loss or unauthorized release, gathering, monitoring or destruction of confidential, proprietary and other information pertaining to the Company, its customers, employees, agents or suppliers***.

77. The statements referenced in ¶76 were materially false and misleading because they omitted the following information necessary to make them not misleading under the circumstances in which they were made: (1) the Company failed to implement basic security standards to protect its customers' sensitive personal information and data from unauthorized access and other malicious acts; (2) the Company disregarded its own information security policies; (3) as a result of (1) and (2), the Company itself – and not cyber attacks or malicious third parties – had exposed non-public information; and (4) the release of confidential customer information that the Company discussed prospectively had in fact already occurred and continued to occur.

78. On April 26, July 26, and October 25, 2018, Defendants filed quarterly reports on Form 10-Q with the SEC for the first, second and third quarters of 2018, respectively. Each was signed and certified by Defendants Gilmore and Seaton, and contained the same misrepresentations identified with respect to the portions of the 2017 10-K quoted in ¶¶74 & 76 above and which were false and/or misleading for the reasons explained in ¶¶75 & 77 above.

79. On February 20, 2019, First American filed an annual report on Form 10-K with the SEC for the fiscal year December 31, 2018 (the "2018 10-K"). In the 2018 10-K, which was signed by Defendants Gilmore and Seaton, Defendants stated that:

> The Company uses computer systems and other technologies (collectively referred to as "systems"), some of which it owns and manages and some of which are owned and/or managed by third parties, including providers of distributed computing infrastructure platforms commonly known as the "cloud." ***The Company and its agents, suppliers, service providers, and customers use these systems to receive, process, store and transmit business information, including highly sensitive non-public personal information as well as data from suppliers and other information upon which the Company's business relies***. The Company also uses these systems to manage substantial cash, investment assets, bank deposits, trust assets and escrow account balances on behalf of itself and its customers, among other activities. Many of the Company's products, services and solutions involving the use of real property related data are fully reliant on these systems and are only available electronically. ***Accordingly, for a variety of reasons, the integrity of these systems and the protection of the information that resides thereon are critically important to the Company's successful operation***.

80. The statements referenced in ¶79 were materially false and misleading because they omitted the following information necessary to make them not misleading under the circumstances in which they were made: (1) the Company failed to implement basic security standards to protect its customers' sensitive personal information and data from unauthorized access and other malicious acts; (2) the Company disregarded its own information security policies; and (3) as a result of (1) and (2), the Company did not protect but instead exposed tens of millions of documents containing sensitive customer NPI.

81. Defendants further stated in the 2018 10-K that:

> ***These systems have been subject to, and are likely to continue to be the target of, computer viruses, cyber attacks, phishing attacks and other malicious activity. These attacks have increased in frequency and sophistication in recent years.*** Further, certain other potential causes of system damage or other negative system-related events are wholly or partially beyond the Company's control, such as natural disasters, vendor failures to satisfy service level requirements and power or telecommunications failures. ***These incidents, regardless of their underlying causes, could expose the Company to system-related damages, failures, interruptions, and other negative events or could otherwise disrupt the Company's business and could also result in the loss or unauthorized release, gathering, monitoring or destruction of confidential, proprietary and other information pertaining to the Company, its customers, employees, agents or suppliers***.

82. The statements referenced in ¶81 were materially false and misleading because they omitted the following information necessary to make them not misleading under the circumstances in which they were made: (1) the Company failed to implement

basic security standards to protect its customers' sensitive personal information and data from unauthorized access and other malicious acts; (2) the Company disregarded its own information security policies; (3) as a result of (1) and (2), the Company itself – and not cyber attacks or malicious third parties – had exposed non-public information; and (4) the release of confidential customer information that the Company discussed prospectively had in fact already occurred and continued to occur.

83. The 2018 10-K also stated, in pertinent part:

> Certain laws and contracts the Company has entered into require it to notify various parties, including consumers or customers, ***in the event of certain actual or potential data breaches or systems failures***. These notifications can result, among other things, in the loss of customers, lawsuits, adverse publicity, diversion of management's time and energy, the attention of regulatory authorities, fines and disruptions in sales. Further, the Company's financial institution customers have obligations to safeguard their systems and sensitive information and the Company may be bound contractually and/or by regulation to comply with the same requirements. ***If the Company fails to comply with applicable regulations and contractual requirements, it could be exposed to lawsuits, governmental proceedings or the imposition of fines, among other consequences***.

84. The statements referenced in ¶83 were materially false and misleading because they omitted the following information necessary to make them not misleading under the circumstances in which they were made: (1) that the "risk" of First American's failure to notify various parties about the Breach was already in the process of

materializing or had already materialized; and (2) as a result, First American had already exposed itself to regulatory and customer liability.

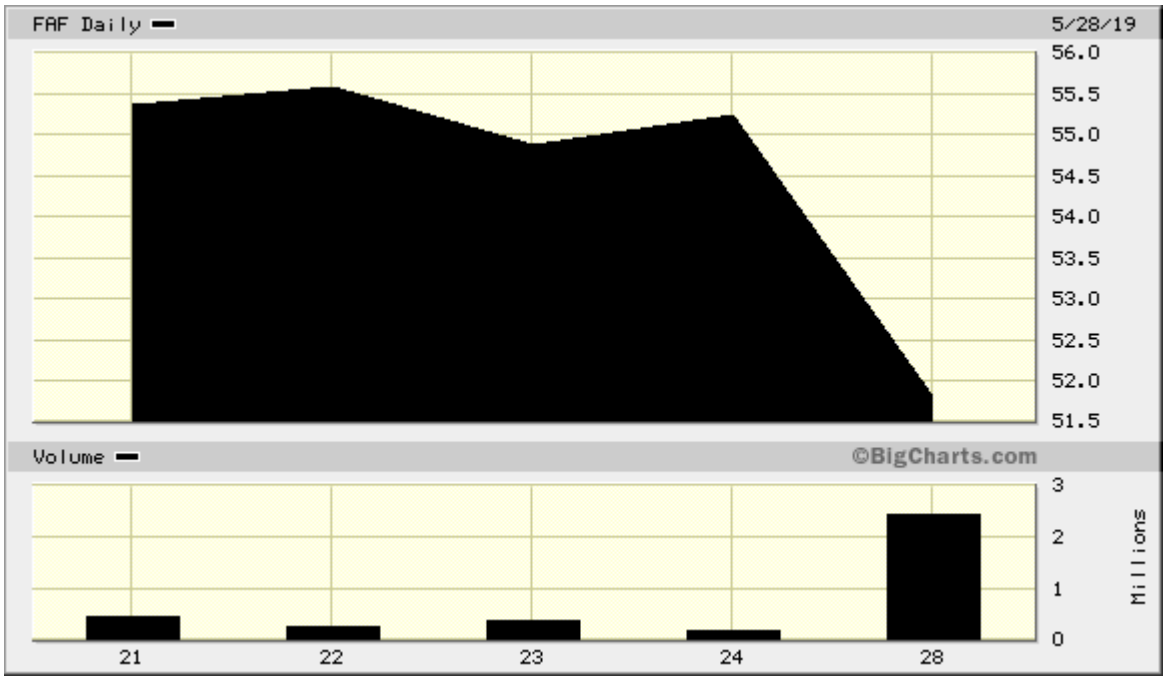
85. On April 25, 2019, Defendants filed a quarterly report on Form 10-Q with the SEC for the first quarter of 2019. The report was signed and certified by Defendants Gilmore and Seaton, and contained the same misrepresentations identified with respect to the portions of the 2018 10-K quoted in ¶¶79, 81, & 83 above and which were false and/or misleading for the reasons explained in ¶¶80, 82, & 84 above.

The Truth Begins to Emerge

86. On May 24, 2019, Brian Krebs, an experienced journalist who reports on cybersecurity issues at KrebsOnSecurity.com, published an article revealing that First American had exposed approximately 850 million documents — dating as far back as 2003 and many containing NPI — by rendering the documents openly accessible to the public.

87. Due to the security Breach that Defendants concealed from investors, 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. In the days leading up to publication of his findings, Mr. Krebs and another individual who had discovered the Breach repeatedly reached out to First American to alert the firm of the Breach.

88. Following publication of the Krebs report, shares of First American fell $3.46, or over 6%, to close at $51.80 on May 28, 2019:



89. After publication of Mr. Krebs's findings, First American filed a report on Form 8-K with the SEC entitled "First American Financial Comments On Its Ongoing Investigation Into Reported Information Security Incident" which stated, in pertinent part:

> **SANTA ANA, Calif., May 28, 2019 –** First American Financial Corporation advises 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. The company is working diligently to address the defect and restore external access***.
>
> An outside forensic firm has been retained to aid in assessing the extent to which any customer information may have been compromised. ***Though the ongoing investigation is in its early stages, at this time there is no indication that any***

> ***large-scale unauthorized access to sensitive customer information occurred***. The company plans to provide updates on its investigation exclusively on its website at https://www.firstam.com/incidentupdate.

90. A report disseminated a few days later by analysts at Stephens interpreted the Company's May 28 statement to mean that "[t]he Company has taken the necessary steps to fix the glitch."

91. The statements referenced in ¶89 were materially false and misleading because: (1) the Breach was not caused by a "design defect," but rather the Company's failure to implement basic security standards to protect its customers' sensitive personal information and data from unauthorized access and other malicious acts; (2) the Company had not just "created the potential for unauthorized access to customer data" but in fact had actually allowed unauthorized access to customer data; (3) the Company was not "working diligently" to address the Breach, and had, in fact, knowingly allowed NPI to be misclassified for years and left customer NPI exposed for many months even after the Breach was flagged internally, all in violation of what it claimed to be its own security protocols; and (4) given that the data exposure had been flagged internally just five months earlier, in December 2019, Defendants knew that millions of records had been left exposed for months, and therefore, that there *was* an "indication that a[] large-scale unauthorized access to sensitive customer information [had] occurred."

92. That same day, May 28, 2019, Barclays published an analyst report titled "Thoughts on Data Issues After a Talk with Management" which communicated the Company's version of events: "[First American] indicated that as soon as the journalist [Mr. Krebs] informed them of the weakness, the database was shut down before the article was published, ***and the issues have since been fixed***." (Emphasis added.)

93. The statements referenced in ¶92 were materially false and misleading and/or failed to disclose that: (1) the Breach issues had not been "fixed"; and (2) sensitive customer information remained exposed as of May 28.

94. In an Incident Update addressed to First American's customers on May 31, 2019, First American belatedly conceded that documents containing NPI were potentially exposed.

95. On February 18, 2020, First American filed an annual report on Form 10-K with the SEC for the fiscal year December 31, 2019 (the "2019 10-K"). In the 2019 10-K, which was signed by Defendants Gilmore and Seaton, Defendants stated with respect to the Breach:

> During the third quarter of 2019, the Company concluded an investigation regarding ***potential unauthorized access to non-public personal information as a result of a vulnerability in one of the Company's applications***. The investigation identified imaged documents containing non-public personal information ***pertaining to 32 consumers*** that likely were accessed without authorization. These ***32 consumers*** were notified and offered complimentary credit monitoring services.

96. The statements referenced in ¶95 were materially false and misleading because: (1) the access to First American customers' NPI was not potential, but actual; (2) First American was subject to a full-blown data breach, and not "potential unauthorized access"; and (3) the more than 350,000 documents that First American admitted were accessed during the Breach is inconsistent with its claim that only 32 consumers were affected.

97. On July 25, 2019, Defendants held an earnings call in connection with First American's quarterly report for the second quarter of 2019 (the "Q2 2019 Earnings Call"). On the Q2 2019 Earnings Call, Defendant Gilmore stated that:

> As we previously announced, we have completed our investigation into the consumer impact of our recent information security incident. ***Though the investigation identified only 32 impacted consumers, we take seriously our responsibility to keep our customers' information secure*** and we regret the concerns this incident caused.

98. The statements referenced in ¶97 were materially false and misleading because: (1) the 350,000 documents that First American admitted were accessed during the Breach is inconsistent with its claim that only 32 consumers were affected; and (2) Defendants were still not "tak[ing] seriously [their] responsibility to keep [their] customers' information secure", as evidenced by the continuing regulatory violations discussed at ¶37 above.

99. On September 19, 2019, Defendant Seaton appeared at the Barclays Global

Financial Services Conference, where he was asked, by analyst Ellis Flannery, "is there anything else on the security incident?" Defendant Seaton's response (a) demonstrated his total disregard for the Breach's impact on First American's investors; (b) acknowledged the Company cared only whether First American's customer had forgotten about the Breach; (c) downplayed the exposure of millions of customers' NPI as "immaterial"; and (d) misrepresented the truth about First American's cybersecurity practices – which were known to him:

> Well, the thing with the information security incidents, I would say from from our customer's perspective, it's really kind of old news, which is really good for us. ***So sort of business as usual from the customer's perspective***. And that was really important for us. We -- ***the regulatory inquiries are just ongoing, and we don't really have a timetable on when, but we think it'll be fairly immaterial, just like the nature of what actually happened***. And so, we continue to work through the regulators. We've answered all their questions. We're being very open, honest about it. And we're really, right now, trying to -- we ***already felt like we had strong information security, but we're taking it to another level internally.*** So, I don't really have a timeline because these things just take a while. So, it's more of along-term issue.

100. The statements referenced in ¶99 were materially false and misleading because they omitted the following information necessary to make them not misleading under the circumstances in which they were made: (1) the Breach, which exposed more than 850 million customer files, with many containing NPI, dating back sixteen years, was not "immaterial" in any sense; (2) the Company, which failed to implement basic security standards to protect its customers' sensitive personal information and data from

unauthorized access and other malicious acts, did not have "strong information security"; (3) the Company was not "taking it to another level internally": less than two months after Defendant Seaton's appearance, First American's records showed more than 320,000 high or critical unremediated vulnerabilities, a figure that climbed the following month, when an additional 131,000 high or critical vulnerabilities requiring remediation. *See* ¶37(h), *supra*.

101. On July 22, 2020, NYDFS announced that First American was the target of their first ever cybersecurity enforcement action in connection with the Breach, with potential penalties of $1000 *per violation*. The NYDFS Amended Charges confirm the accuracy and validity of KrebsOnSecurity's original reporting on the Breach.

102. On July 23, 2020, Defendants held an earnings call in connection with First American's quarterly report for the second quarter of 2020 (the "Q2 2020 Earnings Call"). On the Q2 2020 Earnings Call, Defendant Seaton stated, in pertinent part:

> It has now been a little over a year since the information security incident, and we wanted to take the opportunity to provide you with an update. In March, the Nebraska Department of Insurance, the primary regulator of our Title Insurance Company, led an examination of our information security program as of June 30, 2019 in our response to the information security incident. The resulting report concluded that ***our IT general controls environment is suitably designed and is operating effectively, and that we adequately and appropriately detected, analyzed, contained, eradicated and recovered from a security incident, and that we are in compliance with New York's cyber security requirements for financial services companies***.

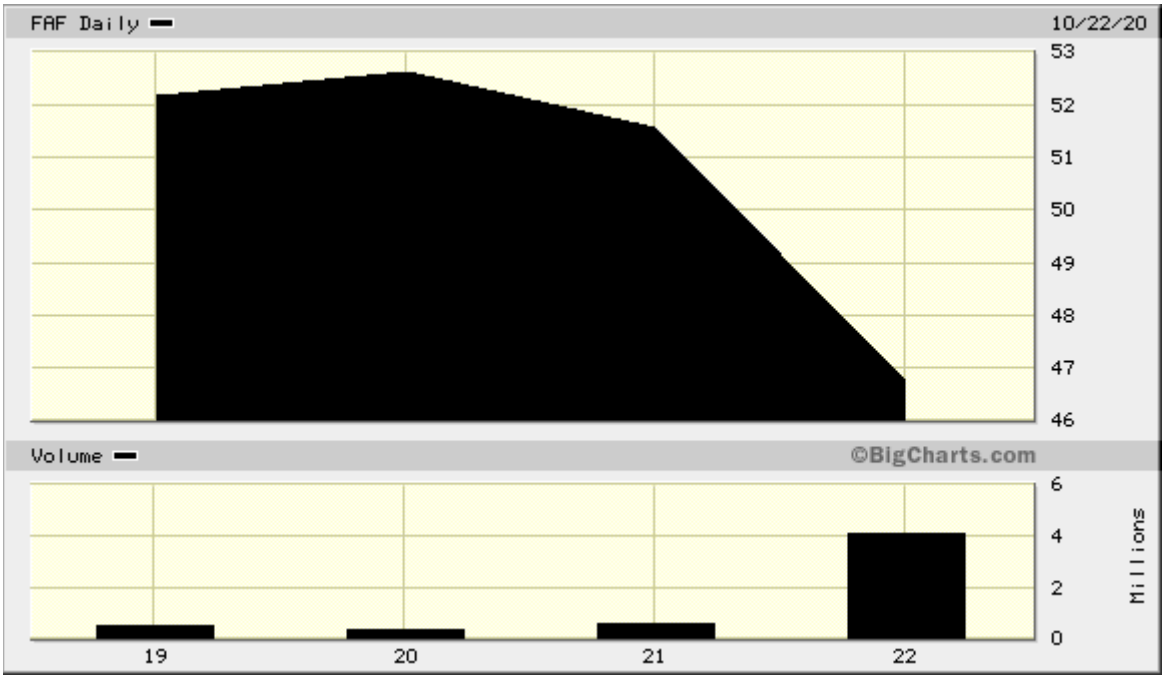
103. The statements referenced in ¶102 were materially false and misleading because they omitted the following information necessary to make them not misleading under the circumstances in which they were made: (1) the Company's IT general controls environment was neither suitably designed nor operating effectively, as evidenced by Defendant Jalakian's March 2019 acknowledgment that First American had over 100,000 unremediated critical/high vulnerabilities, a figure that would expand to 450,000 by year's end; (2) First American had not "adequately and appropriately detected, analyzed, contained, [and] eradicated" the Breach, where it failed to protect its customers' sensitive personal information and data from unauthorized access and other malicious acts even after the Breach had been flagged internally, directly resulting in unauthorized access to more than 350,000 customer documents; (3) as a result of (1) and (2), First American had not " recovered" from the Breach; and (4) as Defendants were well-aware, First American was not in compliance with New York's cyber security requirements for financial services companies.

104. On October 22, 2020, First American filed a quarterly report on Form10-Q with the SEC, announcing that the Company had received a Wells Notice regarding its disclosures to investors regarding its massive security Breach and disclosure controls, stating, in pertinent part:

> Currently, governmental agencies are examining or investigating certain of the Company's operations. ***These exams and investigations***

include two investigations initiated in connection with the information security incident that occurred during the second quarter of 2019, one being conducted by the Securities and Exchange Commission ("SEC") enforcement staff and the other by the New York Department of Financial Services. The SEC enforcement staff is questioning the adequacy of disclosures the Company made at the time of the incident and the adequacy of its disclosure controls. ***In September 2020, the Company received a Wells Notice informing the Company that the enforcement staff has made a preliminary determination to recommend a filing of an enforcement action by the SEC against the Company.***

105. On this news, the price of First American shares fell approximately $4.83 per share, or 9%, to close at $46.75 per share on October 22, 2020:



CLASS ACTION ALLEGATIONS

106. Plaintiff brings this action as a class action pursuant to Federal Rule of Civil Procedure 23(a) and (b)(3) on behalf of a Class, consisting of all those who purchased or otherwise acquired First American securities during the Class Period (the "Class"); and

were damaged upon the (i) revelation of the alleged corrective disclosures and/or (ii) materialization of the concealed risk. Excluded from the Class are Defendants herein, the officers and directors of the Company, at all relevant times, members of their immediate families and their legal representatives, heirs, successors or assigns and any entity in which Defendants have or had a controlling interest.

107. The members of the Class are so numerous that joinder of all members is impracticable. Throughout the Class Period, First American securities were actively traded on the NYSE. While the exact number of Class members is unknown to Plaintiff at this time and can be ascertained only through appropriate discovery, Plaintiff believes that there are thousands of members in the proposed Class. According to the Company's 2017 10-K, right before the Class Period there were 2,487 holders of record. As with most stocks, the overwhelming number of shares are likely held in street name, so the actual number of potential Class members is far higher. Record owners and other members of the Class may be identified from records maintained by First American or its transfer agent and may be notified of the pendency of this action by mail, using the form of notice similar to that customarily used in securities class actions.

108. Plaintiff's claims are typical of the claims of the members of the Class as all members of the Class are similarly affected by the same misrepresentations and

omissions that Defendants made to the market as a whole, and the same wrongful conduct in violation of federal law that is complained of herein.

109. Plaintiff will fairly and adequately protect the interests of the members of the Class and has retained counsel competent and experienced in class and securities litigation. Plaintiff has no interests antagonistic to or in conflict with those of the Class.

110. Common questions of law and fact exist as to all members of the Class and predominate over any questions solely affecting individual members of the Class. Among the questions of law and fact common to the Class are:

- whether the federal securities laws were violated by Defendants' acts as alleged herein;
- whether statements made by Defendants to the investing public during the Class Period misrepresented material facts about the business, operations and management of First American, and in particular its security practices and exposure of sensitive customer NPI;
- whether Defendants Gilmore and Seaton acted as control persons of First American;
- whether Defendants acted knowingly or recklessly in issuing false and misleading public statements;
- whether the prices of First American securities during the Class Period were artificially inflated because of the Defendants' conduct complained of herein; and
- whether the members of the Class have sustained damages and, if so, what is the proper measure of damages.

111. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable. Furthermore, as the damages suffered by individual Class members may be relatively small, the expense and burden of individual litigation make it impossible for members of the Class to individually redress the wrongs done to them. There will be no difficulty in the management of this action as a class action.

112. Plaintiff will rely, in part, upon the presumption of reliance established by the fraud-on-the-market doctrine in that:

- Defendants made public misrepresentations or failed to disclose material facts during the Class Period;
- the omissions and misrepresentations were material;
- First American securities are traded in an efficient market;
- the Company's shares were liquid and traded with moderate to heavy volume during the Class Period;
- the Company traded on the NYSE and was covered by multiple analysts;
- the misrepresentations and omissions alleged would tend to induce a reasonable investor to misjudge the value of the Company's securities; and
- Plaintiff and members of the Class purchased, acquired and/or sold First American securities between the time the Defendants failed to disclose or misrepresented material facts and the time the true facts were disclosed, without knowledge of the omitted or misrepresented facts.

113. Based upon the foregoing, Plaintiff and the members of the Class are entitled to a presumption of reliance upon the integrity of the market.

114. Alternatively, Plaintiff and the members of the Class are entitled to the presumption of reliance established by the Supreme Court in *Affiliated Ute Citizens of the State of Utah v. United States*, 406 U.S. 128, 92 S. Ct. 2430 (1972), as Defendants omitted material information in their Class Period statements in violation of a duty to disclose such information, as detailed above.

COUNT I

(Violations of Section 10(b) of the Exchange Act and Rule 10b-5 Promulgated Thereunder Against All Defendants)

115. Plaintiff repeats and reallege each and every allegation contained above as if fully set forth herein.

116. This Count is asserted against Defendants and is based upon Section 10(b) of the Exchange Act, 15 U.S.C. § 78j(b), and Rule 10b-5 promulgated thereunder by the SEC.

117. During the Class Period, Defendants engaged in a plan, scheme, conspiracy and course of conduct, pursuant to which they knowingly or recklessly engaged in acts, transactions, practices and courses of business which operated as a fraud and deceit upon Plaintiff and the other members of the Class; made various untrue statements of material facts and omitted to state material facts necessary in order to make the statements made,

in light of the circumstances under which they were made, not misleading; and employed devices, schemes and artifices to defraud in connection with the purchase and sale of securities. Such scheme was intended to, and, throughout the Class Period, did: (i) deceive the investing public, including Plaintiff and other Class members, as alleged herein; (ii) artificially inflate and maintain the market price of First American securities; and (iii) cause Plaintiff and other members of the Class to purchase or otherwise acquire First American securities and options at artificially inflated prices. In furtherance of this unlawful scheme, plan and course of conduct, Defendants, and each of them, took the actions set forth herein.

118. Pursuant to the above plan, scheme, conspiracy and course of conduct, each of the Defendants participated directly or indirectly in the preparation and/or issuance of the quarterly and annual reports, SEC filings, press releases and other statements and documents described above, including statements made to securities analysts and the media that were designed to influence the market for First American securities. Such reports, filings, releases and statements were materially false and misleading in that they failed to disclose material adverse information and misrepresented the truth about First American's business operations.

119. By virtue of their positions at First American , Defendants had actual knowledge of the materially false and misleading statements and material omissions

alleged herein and intended thereby to deceive Plaintiff and the other members of the Class, or, in the alternative, Defendants acted with reckless disregard for the truth in that they failed or refused to ascertain and disclose such facts as would reveal the materially false and misleading nature of the statements made, although such facts were readily available to Defendants. Said acts and omissions of Defendants were committed willfully or with reckless disregard for the truth. In addition, each Defendant knew or recklessly disregarded that material facts were being misrepresented or omitted as described above.

120. The Individual Defendants are liable both directly and, with respect to Gilmore and Seaton, indirectly for the wrongs complained of herein. Because of their exercise of control and authority, Gilmore and Seaton were able to and did, directly or indirectly, control the content of the statements of First American, as did Jalakian for the statements she expressly made on behalf of First American. As officers and/or directors of a publicly-held Company, the Individual Defendants had a duty to disseminate timely, accurate, and truthful information with respect to First American businesses, operations, and future prospects. As a result of the dissemination of the aforementioned false and misleading reports, releases and public statements, the market price of First American securities was artificially inflated throughout the Class Period. In ignorance of the adverse facts concerning First American's operational conditions which were concealed

by Defendants, Plaintiff and the other members of the Class purchased or otherwise acquired First American securities at artificially inflated prices and relied upon the price of the securities, the integrity of the market for the securities and/or upon statements disseminated by Defendants, and were damaged thereby.

121. During the Class Period, First American securities were traded on an active and efficient market. Plaintiff and the other members of the Class, relying on the materially false and misleading statements described herein, which the Defendants made, issued or caused to be disseminated, or relying upon the integrity of the market, purchased or otherwise acquired shares of First American securities at prices artificially inflated by Defendants' wrongful conduct. Had Plaintiff and the other members of the Class known the truth, they would not have purchased or otherwise acquired said securities, or would not have purchased or otherwise acquired them at the inflated prices that were paid. At the time of the purchases and/or acquisitions by Plaintiff and the Class, the true value of First American securities was substantially lower than the prices paid by Plaintiff and the other members of the Class. The market price of First American securities declined sharply upon public disclosure of the facts alleged herein to the injury of Plaintiff and Class members.

122. By reason of the conduct alleged herein, Defendants knowingly or recklessly, directly or indirectly, have violated Section 10(b) of the Exchange Act and

Rule 10b-5 promulgated thereunder.

123. As a direct and proximate result of Defendants' wrongful conduct, Plaintiff and the other members of the Class suffered damages in connection with their respective purchases, acquisitions and sales of the Company's securities during the Class Period, upon the disclosure that the Company had been disseminating misrepresented and/or misleading statements to the investing public.

COUNT II

(Violations of Section 20(a) of the Exchange Act Against Defendants Gilmore and Seaton)

124. Plaintiff repeats and reallege each and every allegation contained in the foregoing paragraphs as if fully set forth herein.

125. During the Class Period, the Defendants Gilmore and Seaton participated in the operation and management of First American, and conducted and participated, directly and indirectly, in the conduct of First American business affairs. As discussed above, they knew or recklessly disregarded the adverse non-public information about First American misstatements regarding cybersecurity.

126. As officers and/or directors of a publicly owned Company, the Defendants Gilmore and Seaton had a duty to disseminate accurate and truthful information with respect to First American's results of operations, and to correct promptly any public statements issued by First American which had become materially false or misleading.

127. Because of their positions of control and authority as senior officers, the Defendants Gilmore and Seaton were able to, and did, control the contents of the various reports, press releases and public filings which First American disseminated in the marketplace during the Class Period concerning First American's results of operations. Throughout the Class Period, Defendants Gilmore and Seaton exercised their power and authority to cause First American to engage in the wrongful acts complained of herein.

128. Defendants Gilmore and Seaton therefore, were "controlling persons" of First American within the meaning of Section 20(a) of the Exchange Act. In this capacity, they participated in the unlawful conduct alleged which artificially inflated the market price of First American's securities.

129. Defendants Gilmore and Seaton, therefore, each acted as a controlling person of First American. By reason of their senior management positions and/or being directors of First American, each Defendants Gilmore and Seaton each had the power to direct the actions of, and exercised the same to cause, First American to engage in the unlawful acts and conduct complained of herein. Defendants Gilmore and Seaton each exercised control over the general operations of First American and possessed the power to control the specific activities which comprise the primary violations about which Plaintiff and the other members of the Class complain.

130. By reason of the above conduct, the Defendants Gilmore and Seaton are liable pursuant to Section 20(a) of the Exchange Act for the violations committed by First American.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff demands judgment against Defendants as follows:

A. Determining that the instant action may be maintained as a class action under Rule 23 of the Federal Rules of Civil Procedure, and certifying Plaintiff as the Class representative;

B. Requiring Defendants to pay damages sustained by Plaintiff and the Class by reason of the acts and transactions alleged herein;

C. Awarding Plaintiff and the other members of the Class prejudgment and post-judgment interest, as well as their reasonable attorneys' fees, expert fees and other costs; and

D. Awarding such other and further relief as this Court may deem just and proper.

DEMAND FOR TRIAL BY JURY

Plaintiff hereby demands a trial by jury.

DATED: March 29, 2021

POMERANTZ LLP

s/*Joshua B. Silverman*

Joshua B. Silverman
Louis C. Ludwig
10 South La Salle Street, Suite 3505
Chicago, Illinois 60603
Telephone: (312) 377-1181
jbsilverman@pomlaw.com
lcludwig@pomlaw.com

POMERANTZ LLP
Jennifer Pafiti (SBN 282790)
1100 Glendon Avenue, 15th Floor
Los Angeles, CA 90024
Telephone: (310) 405-7190
jpafiti@pomlaw.com

POMERANTZ LLP
Jeremy A. Lieberman
J. Alexander Hood II
600 Third Avenue, 20th Floor
New York, New York 10016
Telephone: (212) 661-1100
Facsimile: (212) 661-8665
jalieberman@pomlaw.com
ahood@pomlaw.com

Counsel for Lead Plaintiff and the Class

KLAUSNER, KAUFMAN, JENSEN & LEVINSON
Robert D. Klausner
Stuart Kaufman
7080 NW 4th Street Plantation, Florida

33317
Phone: (954) 916-1202
Fax: (954) 916-1232
bob@robertdklausner.com
stu@robertdklausner.com

Additional Counsel for St. Lucie County Fire District Firefighters Pension Trust Fund

CERTIFICATE OF SERVICE

I hereby certify that on March 29, 2021, a copy of the foregoing was filed electronically and served by mail on anyone unable to accept electronic filing. Notice of this filing will be sent by e-mail to all parties by operation of the Court's electronic filing system or by mail to anyone unable to accept electronic filing as indicated on the Notice of Electronic Filing. Parties may access this filing through the Court's CM/ECF System.

/s/Joshua B. Silverman
Joshua B. Silverman