**UNITED STATES OF AMERICA**
**Before the**
**SECURITIES AND EXCHANGE COMMISSION**

**SECURITIES EXCHANGE ACT OF 1934**
**Release No. 92176 / June 14, 2021**

**ADMINISTRATIVE PROCEEDING**
**File No. 3-20367**

| | |
|---|---|
| **In the Matter of**<br><br>**FIRST AMERICAN FINANCIAL CORPORATION,**<br><br>**Respondent.** | **ORDER INSTITUTING CEASE-AND-DESIST PROCEEDINGS PURSUANT TO SECTION 21C OF THE SECURITIES EXCHANGE ACT OF 1934, MAKING FINDINGS, AND IMPOSING A CEASE-AND-DESIST ORDER** |

## I.

The Securities and Exchange Commission ("Commission") deems it appropriate that cease-and-desist proceedings be, and hereby are, instituted pursuant to Section 21C of the Securities Exchange Act of 1934 ("Exchange Act"), against First American Financial Corporation ("First American" or "Respondent").

## II.

In anticipation of the institution of these proceedings, Respondent has submitted an Offer of Settlement (the "Offer") which the Commission has determined to accept. Solely for the purpose of these proceedings and any other proceedings brought by or on behalf of the Commission, or to which the Commission is a party, and without admitting or denying the findings herein, except as to the Commission's jurisdiction over it and the subject matter of these proceedings, which are admitted, Respondent consents to the entry of this Order Instituting Cease-and-Desist Proceedings Pursuant to Section 21C of the Securities Exchange Act of 1934, Making Findings, and Imposing a Cease-and-Desist Order ("Order"), as set forth below.

## III.

On the basis of this Order and Respondent's Offer, the Commission finds that:

### Summary

1. This matter concerns real estate settlement services provider First American's disclosure controls and procedures violations related to disclosures made in connection with a cybersecurity vulnerability involving the company's "EaglePro" application for sharing document images related to title and escrow transactions. First American failed to maintain disclosure controls and procedures designed to ensure that all available relevant information concerning the vulnerability was analyzed for disclosure in the company's reports with the Commission.

2. On the morning of May 24, 2019, a cybersecurity journalist notified First American that its application had a vulnerability exposing over 800 million title and escrow document images dating back to 2003, including images containing sensitive personal data such as social security numbers and financial information. In response, First American issued a statement for inclusion in the cybersecurity journalist's report published on the evening of May 24, 2019, and furnished a Form 8-K to the Commission on May 28, 2019. First American's senior executives responsible for the press statement and Form 8-K were not apprised of certain information concerning the company's information security personnel's prior knowledge of a vulnerability associated with First American's EaglePro system before making those statements—information that would have been relevant to management's assessment of the company's disclosure response to the vulnerability and the magnitude of the resulting risk. In particular, First American's senior executives were not informed that the company's information security personnel had identified a vulnerability several months earlier in a January 2019 manual penetration test of the EaglePro application ("January 2019 Report"), or that the company had failed to remediate the vulnerability in accordance with its policies. As discussed in more detail below, First American did not maintain disclosure controls and procedures designed to ensure that senior management had this relevant information about the January 2019 Report prior to issuing the company's disclosures about the vulnerability.

### Respondent

3. First American Financial Corporation, a Delaware corporation headquartered in Santa Ana, California, provides products and services in connection with residential and commercial real estate transactions, including title insurance and escrow services. First American's common stock is registered with the Commission pursuant to Section 12(b) of the Exchange Act. First American's common stock trades on the New York Stock Exchange.

### Facts

*First American's EaglePro Application*

4. First American's Title Insurance and Services segment includes the company's business issuing title insurance policies on residential and commercial property, and providing

closing and escrow services. The company's services in this segment include the use of real property-related data, which, in certain instances, may contain data regarding purchasers' and sellers' non-public personal information ("NPPI") such as social security numbers and financial information. In 2019, First American derived 91.5% of its consolidated revenues from this segment.

5. First American's proprietary EaglePro application is used to transmit images of certain title and escrow related documents to First American customers through unique uniform resource locators ("URLs") or web addresses. First American launched the EaglePro application in 2013.

6. As of May 24, 2019, First American title and escrow personnel generated and transmitted the EaglePro document packages, which pulled document images from First American's digital repository of escrow and title related document images.

7. As of that date, the repository contained approximately 800 million document images, including both public and non-public information. Document images in the repository containing NPPI were supposed to bear an "SEC" (secure) legend. The process for tagging document images in the repository containing NPPI with the "SEC" legend was performed manually by First American personnel, which lent itself to a number of misclassifications. According to a 2018 internal analysis, the repository potentially contained tens of millions of document images that contained NPPI that were not tagged "SEC."

8. Prior to May 24, 2019, First American personnel could transmit documents to customers through either "secure" or "unsecure" EaglePro packages. Secure packages required password verification by the package recipient. Unsecure EaglePro packages did not require password verification by the recipient, and could be shared by the recipient with third parties without requiring password verification by that third party. For example, a real estate purchaser could share an unsecure EaglePro package URL with the purchaser's agent, which the agent could access without entering a password.

*First American's Failed Remediation of the EaglePro Vulnerability*

9. The EaglePro vulnerability at issue here involved a defect embedded in the application since 2014. Prior to May 24, 2019, a user could take the URL generated as part of an EaglePro package, which could link to an image containing NPPI, and alter the digits in the URL to view other document images to which the user should not have had access. In addition, certain document images transmitted through EaglePro unsecure packages were cached on publicly-available search engines.

10. The company's information security personnel identified the vulnerability months before the May 24, 2019 reporting, but the company did not remediate it according to First American's applicable vulnerability remediation management ("VRM") policies.

11. Between December 2018 and January 2019, First American information security personnel performed a manual penetration test on the EaglePro application, which involved "a security assessment consisting of testing First American's EaglePro Internet facing application."

12. On January 11, 2019, the information security personnel finalized the January 2019 Report. The January 2019 Report identified a "serious" or level "3" vulnerability in the EaglePro application, which information security personnel described as "[a]ccess to PDF's and OrderDetails without authentication." In particular, the January 2019 Report found that "[r]eplacing the document ID in the web page URL with another sequential number allows access to other non-related document sessions without authentication." The January 2019 Report also found that searches of publicly-available search engines "return[] . . . Title related viewable documents within an EaglePo [*sic*] session and give[] direct access to these documents bypassing authentication and present[] additional related documents in the opened session." The January 2019 Report also indicated that "[n]o NPI was discovered in the documents that were reviewed for this report," but that "[i]t is unknown if any additional documents expose [*sic*] contained NPI. This requires further investigation by the application owner."

13. On January 11, 2019, the information security personnel who performed the manual penetration test shared the January 2019 Report with information security managers, VRM personnel, and the EaglePro Accountable Remediation Owner ("ARO"), who under the company's VRM policies was the "individual responsible for remediating vulnerabilities identified via a vulnerability scan and ingested into the VRM Program."

14. Under First American's VRM policies, a vulnerability with a level 3 severity was categorized as "medium risk" and required remediation within 45 days. Rather than recording the vulnerability as a level 3 severity, due to a clerical error the vulnerability was erroneously input as a level "2" or "low risk" severity in First American's automated VRM tracking system.

15. Under First American's VRM policies, a vulnerability with a level 2 severity required remediation within 90 days (rather than 45 days for a level 3 severity). The VRM tracking system, accordingly, calculated the remediation deadline for the EaglePro vulnerability as May 8, 2019 (90 days after the vulnerability was input into the tracking system).

16. Under First American's VRM policies, "[i]f an ARO is unable to remediate based on the timeframes listed above, the ARO must have their management contact Information Security to discuss their remediation plan and proposed time estimate. If it is not technically possible to remediate the vulnerability, or if remediation cost prohibitive, the ARO and their management must contact Information Security to obtain a waiver or risk acceptance approval from the CISO." The ARO did not request a waiver or risk acceptance from the CISO.

*First American's Public Statements About the EaglePro Vulnerability*

17. On the morning of May 24, 2019, a cybersecurity journalist emailed First American's investor relations personnel that First American's web application was "leaking more than 800 million documents from real estate transactions going back from 2003 to the present day. The information in these publicly accessible documents include bank account numbers, mortgage and tax records, Social Security numbers, wire transaction receipts and drivers license images."

18. After the close of trading on May 24, 2019, the cybersecurity journalist published an article on his website, which stated "[m]odifying the document number in [a customer's] link by

numbers in either direction yielded other people's records before or after the same date and time, indicating the document numbers may have been issued sequentially," and wrote that this vulnerability impacted over 800 million document images dating back to 2003.

19. First American provided the cybersecurity journalist the following statement for inclusion in his May 24, 2019 article:

> First American has learned of a design defect in an application that made possible unauthorized access to customer data. At First American, security, privacy and confidentiality are of the highest priority and we are committed to protecting our customers' information. The company took immediate action to address the situation and shut down external access to the application.

The cybersecurity journalist's article quoted First American's statement verbatim, and was made available publicly on the cybersecurity journalist's website. First American also disseminated this same statement to national media outlets, which published the statement on the evening of May 24, 2019.

20. On the morning of May 28, 2019, the first trading day following the May 24, 2019 article's publication, First American furnished a Form 8-K, which attached an additional press release. The May 28, 2019 press release stated that there was "[n]o preliminary indication of large-scale unauthorized access to customer information." The press release also stated:

> 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.

*First American's Senior Executives Were Not Informed About the January 2019 Report Prior to the May 28, 2019 Form 8-K*

21. As described above, First American information security personnel identified the EaglePro vulnerability in the January 2019 Report.

22. Certain of the company's senior technical experts, in particular the CISO and CIO, learned of the January 2019 Report prior to the company furnishing the Form 8-K on May 28, 2019. On the morning of May 24, 2019, shortly after outreach by the cybersecurity journalist, First American's CISO learned about the January 2019 Report for the first time and that the vulnerability had not been timely remediated. First American's CIO likewise learned about the January 2019 Report and the lack of remediation for the first time on May 25, 2019.

23. Subsequent to reviewing the January 2019 Report, First American's CISO and CIO participated in numerous meetings with the company's senior executives responsible for the company's disclosures, including the company's CEO and CFO, between May 24, 2019 and May 28, 2019.

24. Nevertheless, the company's senior executives responsible for the disclosures were not made aware about these facts prior to the company releasing its statement to the press on May 24, 2019 or furnishing the Form 8-K on May 28, 2019.

25. Accordingly, the senior executives responsible for the company's statements in May 2019, did not evaluate whether to disclose the company's prior awareness of, or actions related to the vulnerability. Because these senior executives were not aware of the January 2019 Report, these senior executives did not know about the vulnerability described in the January 2019 Report. Unbeknownst to these senior executives, the company's information security personnel had been aware of the vulnerability for months and the company's information technology personnel did not remediate it, leaving millions of document images exposed to potential unauthorized access for months. Indeed, subsequent to the furnishing of the May 28, 2019 Form 8-K, the company's information security personnel determined that the vulnerability had in fact existed since 2014. These senior executives thus lacked certain information to fully evaluate the company's cybersecurity responsiveness and the magnitude of the risk from the EaglePro vulnerability at the time they approved the company's disclosures.

26. As discussed above, the company's business includes providing services involving data related to real estate transactions. Nevertheless, as of May 24, 2019, First American did not have any disclosure controls and procedures related to cybersecurity, including incidents involving potential breaches of that data.

## Violations

27. As a result of the conduct described above, First American violated Exchange Act Rule 13a-15(a) [17 C.F.R. § 240.13a-15], which requires every issuer of a security registered pursuant to Section 12 of the Exchange Act to maintain disclosure controls and procedures designed to ensure that information required to be disclosed by an issuer in reports it files or submits under the Exchange Act is recorded, processed, summarized, and reported within the time periods specified in the Commission's rules and forms.

## IV.

In view of the foregoing, the Commission deems it appropriate to impose the sanctions agreed to in Respondent First American's Offer.

Accordingly, it is hereby ORDERED that**:**

A. Pursuant to Section 21C of the Exchange Act, Respondent cease and desist from committing or causing any violations and any future violations of Exchange Act Rule 13a-15.

B. Respondent shall, within 14 days of the entry of this Order, pay a civil money penalty in the amount of $487,616 to the Securities and Exchange Commission for transfer to the general fund of the United States Treasury, subject to Exchange Act Section 21F(g)(3). If timely payment is not made, additional interest shall accrue pursuant to 31 U.S.C. §3717.

Payment must be made in one of the following ways:

(1) Respondent may transmit payment electronically to the Commission, which will provide detailed ACH transfer/Fedwire instructions upon request;

(2) Respondent may make direct payment from a bank account via Pay.gov through the SEC website at http://www.sec.gov/about/offices/ofm.htm; or

(3) Respondent may pay by certified check, bank cashier's check, or United States postal money order, made payable to the Securities and Exchange Commission and hand-delivered or mailed to:

Enterprise Services Center
Accounts Receivable Branch
HQ Bldg., Room 181, AMZ-341
6500 South MacArthur Boulevard
Oklahoma City, OK 73169

Payments by check or money order must be accompanied by a cover letter identifying First American as a Respondent in these proceedings, and the file number of these proceedings; a copy of the cover letter and check or money order must be sent to Kristina Littman, Division of Enforcement, Securities and Exchange Commission, 100 F Street, N.E., Washington, District of Columbia 20549.

C. Amounts ordered to be paid as civil money penalties pursuant to this Order shall be treated as penalties paid to the government for all purposes, including all tax purposes. To preserve the deterrent effect of the civil penalty, Respondent agrees that in any Related Investor Action, it shall not argue that it is entitled to, nor shall it benefit by, offset or reduction of any award of compensatory damages by the amount of any part of Respondent's payment of a civil penalty in this action ("Penalty Offset"). If the court in any Related Investor Action grants such a Penalty Offset, Respondent agrees that it shall, within 30 days after entry of a final order granting the Penalty Offset, notify the Commission's counsel in this action and pay the amount of the Penalty Offset to the Securities and Exchange Commission. Such a payment shall not be deemed an additional civil penalty and shall not be deemed to change the amount of the civil penalty imposed in this proceeding. For purposes of this paragraph, a "Related Investor Action" means a private damages action brought against Respondent by or on behalf of one or more investors based on substantially the same facts as alleged in the Order instituted by the Commission in this proceeding.

By the Commission.

Vanessa A. Countryman
Secretary