UNITED STATES OF AMERICA
Before the
SECURITIES AND EXCHANGE COMMISSION

SECURITIES ACT OF 1933
Release No. 11343 / December 16, 2024

SECURITIES EXCHANGE ACT OF 1934
Release No. 101928

ADMINISTRATIVE PROCEEDING
File No. 3-22360

In the Matter of **FLAGSTAR BANCORP, INC., now known as "Flagstar Financial, Inc."** **Respondent.**	**ORDER INSTITUTING CEASE-AND-DESIST PROCEEDINGS PURSUANT TO SECTION 8A OF THE SECURITIES ACT OF 1933 AND 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 8A of the Securities Act of 1933 ("Securities Act") and Section 21C of the Securities Exchange Act of 1934 ("Exchange Act"), against Flagstar Bancorp, Inc., now known as "Flagstar Financial, Inc." ("Flagstar" 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 8A of the Securities Act of 1933 and 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 materially misleading statements that Flagstar negligently made regarding a cybersecurity attack on Flagstar's network between November 22, 2021 and December 25, 2021 (the "Citrix Breach"), which resulted in, among other things, the encryption of data, network disruptions, and the exfiltration of the personally identifiable information ("PII") of approximately 1.5 million individuals, including customers, on December 3 and 4, 2021. The risk factors in Flagstar's 2021 Form 10-K, which it filed on March 1, 2022, stated that cybersecurity attacks "may interrupt our business or compromise the sensitive data of our customers," but Flagstar did not disclose that Flagstar had already experienced cybersecurity attacks that resulted in the exfiltration of sensitive customer data and that the Citrix Breach interrupted its business. In a June 17, 2022 notice to customers posted on its website ("Customer Website Notice") and a Form 10-Q filed on August 9, 2022, Flagstar also made materially misleading statements concerning the scope of the Citrix Breach and represented that there was unauthorized "access" to its network and customer data, when Flagstar was aware that the breach disrupted several of its network systems and that customer PII was exfiltrated from its network. Flagstar also failed to maintain disclosure controls and procedures as defined in Exchange Act Rule 13a-15(e).

2. Based on the foregoing conduct, and the conduct described below, Flagstar violated Section 17(a)(2) of the Securities Act and Section 13(a) of the Exchange Act and Rules 12b-20, 13a-1, 13a-13 and 13a-15 thereunder.

Respondent

3. Flagstar Bancorp, Inc., now known as "Flagstar Financial, Inc.", is a Delaware corporation headquartered in Hicksville, New York, whose regional office is in Troy, Michigan. During the relevant period, Flagstar provided commercial and consumer banking services and was one of the nation's largest bank mortgage originators and subservicers of mortgage loans. On December 1, 2022, Flagstar merged with New York Community Bancorp, Inc. ("NYCB") and became known as NYCB.[1] Prior to the merger with NYCB, Flagstar's shares were traded on the National Association of Securities Dealers Automated Quotations ("NASDAQ") from 1997 to 2001 and on the New York Stock Exchange ("NYSE") from 2001 through November 30, 2022 under the ticker symbol FBC. In connection with these listings, Flagstar's common stock was registered under Section 12(b) of the Exchange Act. On or about December 1, 2022, the NYSE filed a notice under Form 25 striking from listing and terminating Flagstar's registration of common shares. Between May 1997 and November 2022, Flagstar was required to file with the Commission annual reports on

[1] NYCB's stock was registered with the Commission under Section 12(b) of the Exchange Act and its shares were traded on the New York Stock Exchange under ticker symbol NYCB from 2001 to October 25, 2024.

Forms 10-K and quarterly reports on Forms 10-Q pursuant to Section 13(a) of the Exchange Act and related rules thereunder. On October 25, 2024, NYCB became known as "Flagstar Financial, Inc."[2]

Facts

The Citrix Breach

4. Between November 22, 2021 and December 25, 2021, Flagstar's network was attacked by a threat actor who, among other things, obtained unauthorized access to Flagstar's platform that enabled users to access Flagstar applications and desktops remotely (the "Citrix environment"), obtained credentials that enabled the threat actor to deploy ransomware that caused encryption on approximately 30% of Flagstar's work stations and servers, and exfiltrated data, including customer PII, from its network.

5. During December 2021, the Citrix Breach intermittently disrupted Flagstar's mortgage business, including impacting the bank's ability to originate, service, and close loans. As a result of the Citrix Breach, Flagstar shut down its network for several hours, rebuilt or restored hundreds of its servers that supported bank-wide business operations, and reset passwords for thousands of Flagstar employees and contractors throughout December 2021. The Citrix Breach also intermittently impacted access to Flagstar's website, certain mobile applications, and Flagstar's customer call center in December 2021.

6. In early December 2021, Flagstar assembled its "Crisis Management Team" and engaged third-party experts to assist with conducting a forensic investigation. In mid-December 2021, the threat actor responsible for the Citrix Breach contacted Flagstar employees and demanded a ransom payment. At the end of December 2021, Flagstar made a ransom payment in exchange for the threat actor's promise to allow Flagstar to delete the exfiltrated data in the threat actor's possession. By March 1, 2022, Flagstar understood that the exfiltrated data included customer PII. In early June 2022, after Flagstar completed its review of the data that the threat actor obtained, Flagstar determined that the number of individuals whose PII was exfiltrated from its network was approximately 1.5 million (approximately a quarter of its active customers across different segments of the bank). During Flagstar's investigation, it engaged a firm to monitor the dark web and, at that time, the firm did not identify evidence that customer data was posted as a result of the Citrix Breach.

Flagstar's Materially Misleading Statements

7. On March 1, 2022, Flagstar filed its Form 10-K for the 2021 fiscal year. In the risk factor section addressing cybersecurity risks, Flagstar represented, "We, and our third-party providers, have been in the past and may in the future be subject to cybersecurity attacks. … Such attacks may interrupt our business or compromise the sensitive data of our customers and employees." By speaking in the hypothetical and mirroring Flagstar's 2020 Form 10-K, these statements were materially misleading by omitting material information, including that Flagstar had experienced cybersecurity attacks that resulted in the exfiltration of the sensitive data of Flagstar

[2] Flagstar Financial, Inc.'s stock is registered with the Commission under Section 12(b) of the Exchange Act and its shares are traded on the New York Stock Exchange under the ticker symbol FLG.

customers. By the time Flagstar filed its 2021 Form 10-K, Flagstar understood that customer PII was exfiltrated during the Citrix Breach and in a separate data breach for which a forensic investigation was completed in March 2021. Flagstar also understood that the Citrix Breach interrupted Flagstar's mortgage business.

8. On June 17, 2022, Flagstar posted the Customer Website Notice containing information about the Citrix Breach on the Customer Data Information Center of its website. Flagstar therein stated, "In December 2021, Flagstar experienced a cyber incident that involved unauthorized access to our network. We want to take a moment to detail what happened, what this means for you, and how you can protect your information." In describing "What happened?" in the Customer Website Notice, Flagstar included no details about the scope or consequence of the Citrix Breach and instead described the steps it took to respond to the Citrix Breach. In the "What is Flagstar doing?" section, Flagstar stated that it was "in the process of notifying individuals who may have been impacted directly via U.S. Mail to extend complimentary credit monitoring services," that "[f]or those impacted, we have no evidence that any of your information has been misused," and that "Flagstar has [established] a call center dedicated to handling inquiries related to [the] incident . . . "

9. Nearly two months later, on August 9, 2022, Flagstar filed its Form 10-Q for the second fiscal quarter of 2022 and disclosed in its Management Discussion & Analysis section as an Operational Risk that "Flagstar recently experienced a cyber incident that involved unauthorized access to our network and other customer data."

10. The Customer Website Notice and Form 10-Q were materially misleading because they represented that there was unauthorized access to Flagstar's network when, in fact, Flagstar was aware that the threat actor exfiltrated the PII of approximately 1.5 million individuals from Flagstar's network. These disclosures were also materially misleading because they minimized the scope of the Citrix Breach by stating that there was unauthorized "access" to its network, when the threat actor had intermittently compromised Flagstar's network between November 22, 2021 and December 25, 2021, and encrypted work stations and servers, causing Flagstar to temporarily take down its network, rebuild or restore hundreds of its servers, and reset thousands of passwords. Furthermore, although the Customer Website Notice stated that it would describe what had happened, the Customer Website Notice was materially misleading because Flagstar omitted material information about the Citrix Breach, such as the number of individuals impacted and that those individuals' PII was exfiltrated. Additionally, the Form 10-Q stated that the cyber incident involved unauthorized access to "other customer data," but omitted material information – that is, that the customer data included customer PII. Lastly, the Form 10-Q was also materially misleading because it stated that the cyber incident took place "recently," when, by the time the Form 10-Q was filed on August 9, 2022, the Citrix Breach took place over eight months earlier in December 2021.

11. During the relevant time period, Flagstar offered and sold stock to its employees through its 2016 Stock Award and Incentive Plan for which a Form S-8 was filed with the Commission on May 24, 2016.

Flagstar's Disclosure Control Failures

12. Exchange Act Rule 13a-15(a) requires issuers such as Flagstar to "maintain disclosure controls and procedures (as defined in paragraph (e) of this section)." Paragraph (e) defines disclosure controls and procedures to include, among other things, "controls and other procedures of an issuer that are designed to ensure that information required to be disclosed by the issuer in the reports that 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." Under the rule, "[d]isclosure controls and procedures include, without limitation, controls and procedures designed to ensure that information required to be disclosed by an issuer in the reports that it files or submits under the [Exchange] Act is accumulated and communicated to the issuer's management . . . as appropriate to allow timely decisions regarding required disclosure."

13. Flagstar failed to maintain disclosure controls and procedures regarding cybersecurity incidents designed to ensure that relevant information to assess materiality was considered by disclosure decision makers to allow timely decisions regarding potentially required disclosure. For example, although Flagstar's disclosure decision makers received regular updates related to the Citrix Breach, Flagstar's cybersecurity procedures and controls lacked guidance on what factors to consider in assessing materiality for purposes of disclosure, which disclosure decision makers were responsible for making the materiality assessment, and how that assessment was to be documented and/or communicated to management. As a result, Flagstar failed to adequately assess relevant information regarding the Citrix Breach from a disclosure perspective.

Violations

14. As a result of the conduct describe above, Flagstar violated Section 17(a)(2) of the Securities Act, which prohibits any person from directly or indirectly obtaining money or property by means of any untrue statement of material fact or any omission to state a material fact necessary in order to make the statements made, in light of the circumstance under which they were made, not misleading. A violation of Section 17(a)(2) does not require scienter and may rest on a finding of negligence. *See Aaron v. SEC*, 446 U.S. 680, 697 (1980).

15. As a result of the conduct describe above, Flagstar violated Section 13(a) of the Exchange Act and Rules 13a-1 and 13a-13 thereunder, which require issuers of a security registered pursuant to Section 12 of the Exchange Act to file with the Commission annual and quarterly reports in conformity with the Commission's rules and regulations. Flagstar also violated Rule 12b-20 of the Exchange Act, which, among other things, requires such issuers to include in their annual and quarterly reports filed with the Commission any material information necessary to make the required statements in the filing not misleading, in light of the circumstances under which they were made.

16. As a result of the conduct describe above, Flagstar violated Exchange Act Rule 13a-15, which requires issuers such as Flagstar with 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 and in the public interest to impose the sanctions agreed to in Respondent Flagstar's Offer.

Accordingly, it is hereby ORDERED that:

A. Pursuant to Section 8A of the Securities Act and Section 21C of the Exchange Act, Respondent Flagstar cease and desist from committing or causing any violations and any future violations of Section 17(a)(2) of the Securities Act and Section 13(a) of the Exchange Act and Rules 12b-20, 13a-1, 13a-13, and 13a-15 thereunder.

B. Respondents shall, within 14 days of the entry of this Order, pay a civil money penalty in the amount of $3,550,000 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 Flagstar 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 Jorge Tenreiro, Acting Chief of the Crypto Assets and Cyber Unit, Division of Enforcement, Securities and Exchange Commission, 100 F St., NE, Washington, DC 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