UNITED STATES OF AMERICA
Before the
SECURITIES AND EXCHANGE COMMISSION

SECURITIES EXCHANGE ACT OF 1934
Release No. 92800 / August 30, 2021

INVESTMENT ADVISERS ACT OF 1940
Release No. 5834 / August 30, 2021

ADMINISTRATIVE PROCEEDING
File No. 3-20490

In the Matter of

Cetera Advisor Networks LLC,
Cetera Investment Services LLC,
Cetera Financial Specialists LLC,
Cetera Advisors LLC, and
Cetera Investment Advisers LLC,

Respondents.

ORDER INSTITUTING ADMINISTRATIVE AND CEASE-AND-DESIST PROCEEDINGS PURSUANT TO SECTIONS 15(b) AND 21C OF THE SECURITIES EXCHANGE ACT OF 1934 AND SECTIONS 203(e) AND 203(k) OF THE INVESTMENT ADVISERS ACT OF 1940, MAKING FINDINGS, AND IMPOSING REMEDIAL SANCTIONS AND A CEASE-AND-DESIST ORDER

I.

The Securities and Exchange Commission (the "Commission" or "SEC") deems it appropriate and in the public interest that public administrative and cease-and-desist proceedings be, and hereby are, instituted pursuant to Sections 15(b) and 21C of the Securities Exchange Act of 1934 (the "Exchange Act") and Sections 203(e) and 203(k) of the Investment Advisers Act of 1940 (the "Advisers Act"), against Cetera Advisor Networks LLC, Cetera Advisors LLC, Cetera Investment Services LLC, Cetera Financial Specialists LLC, and Cetera Investment Advisers LLC (together, "Cetera Entities" or "Respondents").

II.

In anticipation of the institution of these proceedings, Respondents have 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 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 them and the subject matter of these proceedings, which are admitted, Respondents consent to the entry of this Order Instituting Administrative and Cease-and-Desist Proceedings Pursuant to Sections 15(b) and 21C of the Securities Exchange Act of 1934 and Sections 203(e) and 203(k) of the Investment Advisers Act of 1940, Making Findings, and Imposing Remedial Sanctions and a Cease-and-Desist Order ("Order"), as set forth below.

III.

On the basis of this Order and Respondents' Offer, the Commission finds[1] that:

Summary

1. These proceedings arise out of Cetera Entities' failure to adopt written policies and procedures reasonably designed to protect customer records and information, in violation of Rule 30(a) of Regulation S-P (17 C.F.R. § 248.30(a)) (the "Safeguards Rule") and, with respect to Cetera Advisors LLC and Cetera Investment Advisers LLC, failure to adopt and implement reasonably designed procedures for review of communications sent to impacted clients in violation of Section 206(4) of the Advisers Act and Rule 206(4)-7 thereunder (17 C.F.R. § 275.206(4)-7).

2. The Safeguards Rule requires every broker-dealer and every investment adviser registered with the Commission to adopt written policies and procedures reasonably designed to: (1) insure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of customer records and information; and (3) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

3. Cetera Entities are registered with the Commission as broker-dealers, investment advisers, or both. Between November 2017 and June 2020, email accounts of over 60 Cetera Entities' personnel were taken over by unauthorized third parties[2] resulting in the exposure of over 4,388 of Cetera Entities' customers' personally identifiable information ("PII") stored in the compromised email accounts.[3] At the time, none of these accounts had multi-factor authentication ("MFA")[4] turned on, even though Cetera Entities' own policies required MFA "wherever possible," beginning in 2018. Although these email account takeovers do not appear to have resulted in any unauthorized trades or transfers in brokerage customers' or advisory clients' (hereinafter "customers") accounts, Cetera Entities violated the Safeguards Rule because their policies and procedures to protect customer information and to prevent and respond to cybersecurity incidents were not reasonably designed to meet these objectives, specifically as applied to independent contractor representatives and offshore contractors. Cetera Entities had a significant number of security tools at their disposal that allowed them to implement controls that would mitigate these higher risks. However, Cetera Entities failed to use these tools in the manner

[1] The findings herein are made pursuant to Respondents' Offer of Settlement and are not binding on any other person or entity in this or any other proceeding.

[2] An email account takeover occurs when an unauthorized third party gains access to the email account and, in addition to being able to view its contents, is also able to take actions of a legitimate user, such as sending and deleting emails or setting up forwarding rules.

[3] As used in this Order, the phrase "exposure of PII" means that an unauthorized third party has the ability to view, but has not necessarily viewed, the PII.

[4] MFA requires at least one authentication factor in addition to a username and password to login to an account. The additional factor is commonly a one-time passcode generated by a hardware token or an application on the user's mobile device or computer, or sent to the user by email or text message.

tailored to their business, exposing their customers' PII to unreasonable risks.

4. Section 206(4) of the Advisers Act and Rule 206(4)-7 thereunder require a registered investment adviser, or an investment adviser required to register, to adopt and implement written compliance policies and procedures reasonably designed to prevent violations, by the adviser or its supervised persons, of the Advisers Act and the rules adopted by the Commission thereunder. Cetera Advisors LLC ("Cetera Advisors") and Cetera Investment Advisers LLC ("Cetera Investment Advisers") violated Section 206(4) of the Advisers Act and Rule 206(4)-7 thereunder by failing to adopt and implement reasonably designed policies and procedures regarding review of communications to advisory clients. This failure resulted in sending breach notifications to the firms' clients that included misleading template language suggesting that the notifications were issued much sooner than they actually were after the discovery of the incidents.

Respondents

5. Cetera Advisor Networks LLC is a Delaware limited liability company headquartered in El Segundo, California, and dually registered as a broker-dealer and investment adviser with the Commission.

6. Cetera Advisors LLC is a Delaware limited liability company headquartered in Denver, Colorado, and dually registered as a broker-dealer and investment adviser with the Commission.

7. Cetera Investment Services LLC is a Delaware limited liability company headquartered in St. Cloud, Minnesota, and dually registered as a broker-dealer and investment adviser with the Commission.

8. Cetera Financial Specialists LLC is a Delaware limited liability company headquartered in Schaumburg, Illinois, and a broker-dealer registered with the Commission.

9. Cetera Investment Advisers LLC is a Delaware limited liability company headquartered in El Segundo, California, and an investment adviser registered with the Commission.

10. All of the above registered entities are direct or indirect wholly-owned subsidiaries of Cetera Financial Group, Inc. ("CFG"), which is not registered with the Commission in any capacity and is not a respondent in this Order. CFG, as corporate parent, provides a variety of centralized business services, including cybersecurity, to Cetera Entities.

Background

11. Cetera Entities are Commission-registered broker-dealers and/or Commission-registered investment advisers that offer a wide range of proprietary and non-proprietary investment products and services through a national network of independent contractor registered representatives and independent contractor investment adviser representatives. From

at least 2017 through 2020 ("the relevant period"), Cetera Entities' personnel, including employees, independent contractor representatives[5] ("contractor representatives"), and offshore contractors ("offshore contractors")[6] used cloud-based email services (i.e., email services hosted on an external server and provided on a subscription basis by a third-party vendor) for internal and external communications. Contractor representatives, offshore contractors, and employees routinely emailed and stored in these email accounts PII of Cetera Entities' customers. Cetera Entities' corporate parent, CFG provisioned and managed all employee and offshore contractor email accounts, but not all contractor representative email accounts. Some of the contractor representative email accounts were provisioned and managed by branch offices where the representatives worked.

12. Starting in February 2018, Cetera Entities' policies required MFA to be turned on "wherever possible." In October 2018, the policies were amended to require MFA "wherever possible, but at a minimum for privileged or high-risk access." Although the policy requiring MFA did not define "privileged" or "high-risk access," another policy in effect since August 2017 included emails and lists containing customers' non-public personal information among "Category I" data subject to highest level of protection.

Email Account Takeover Activity

13. In November and December 2017, 32 email accounts of Cetera Entities' contractor representatives were taken over by unauthorized third parties via phishing,[7] credential stuffing,[8] or other modes of attack. The email account takeovers resulted in the exposure of Cetera Entities' customers' PII stored in the compromised email accounts. None of the compromised email accounts had MFA turned on.

14. Following these email compromises, in January 2018, Cetera Entities turned on

[5] The independent contractor representatives were investment adviser representatives of Cetera Entities or were associated persons of Cetera Entities who were licensed as registered representatives or otherwise qualified to effect transactions in securities on behalf of Cetera Entities. As noted in *Books and Records Requirements for Brokers and Dealers Under the Securities Exchange Act of 1934,* Exchange Act Release No. 44992 (Oct. 26, 2001) 66 FR 55817, 55820 n.18 (Nov. 1, 2001), "[t]he Commission has consistently taken the position that independent contractors (who are not themselves registered as broker-dealers) involved in the sale of securities on behalf of a broker-dealer are 'controlled by' the broker-dealer, and, therefore, are associated persons of the broker-dealer." *See also Rules Implementing Amendments to the Investment Advisers Act of 1940,* Advisers Act Release No. 1633 (May 15, 1997) n. 123 ("the definition of 'supervised person' and the 'other persons who provide investment advice' . . . include persons who may not be employees but assume a similar function (e.g., independent contractors).").

[6] CFG retained the offshore contractors in order to develop and test software used by Cetera Entities, perform quality assurance testing, and support the customer service function.

[7] Phishing is a means of gaining unauthorized access to a computer system or service by using a fraudulent or "spoofed" email to trick a victim into downloading malicious software or entering his or her log-in credentials on a fake website purporting to be the legitimate log-in website for the system or service.

[8] Credential stuffing is a means of gaining unauthorized access to accounts by automatically entering large numbers of pairs of log-in credentials, typically a username or email address together with a password, that were obtained elsewhere.

MFA for employee cloud-based email accounts. Turning on MFA ensured that the users would not be able to use these email accounts without logging in with MFA.

15. Beginning in March 2018, Cetera Entities turned on MFA for 6,650 contractor representatives' email accounts. However, in September 2018, CFG identified approximately 1,500 email accounts used by contractor representatives or their employees that still did not have MFA turned on. In October and December 2018, email accounts of two contractor representatives, which were on the September 2018 list of email accounts without MFA, were taken over by unauthorized persons, resulting in the exposure of PII of 1,831 Cetera Entities' customers. An additional 23 contractor representatives' email accounts were taken over during the first half of 2018, and one additional during the second half of 2018, resulting in the exposure of PII of 199 customers. In 2019, two more contractor representatives' email accounts were taken over, resulting in the exposure of sixteen customers' PII. In the first half of 2020, three more contractor representatives' email accounts were taken over by unauthorized third parties, and one of these incidents resulted in the exposure of 680 customers' PII. None of the compromised email accounts had MFA turned on, despite Respondents' 2018 policies requiring the use of MFA "wherever possible."

16. Cetera Entities also did not implement MFA for offshore contractor email accounts until the end of 2019, even though these email accounts were accessible from any location around the world, rather than only from the secure offshore development facilities. In 2018 and 2019, four email accounts used by offshore contractors were taken over by third parties, and two of the incidents resulted in exposure of 1,662 customers' PII.

17. Cetera Entities' policy requiring MFA for privileged and high-risk access was not reasonably designed to be applied to email accounts of Cetera Entities' contractor representatives and offshore contractors, whose systems and access to sensitive data was generally at the same or higher risk of compromise than the systems and access used by Cetera Entities' employees. Cetera Entities have now implemented MFA for email accounts used by its contractor representatives and offshore contractors.

Breach Notifications to Advisory Clients

18. For each email account takeover where Cetera Entities identified potential customer PII exposure, Cetera Entities issued breach notifications to impacted customers, notifying them that their PII may have been accessed without authorization. Cetera Entities generally engaged outside counsel to prepare and deliver these notifications. While most breach notifications sent by Cetera Entities' outside counsel were accurate, letters sent in 2018 and 2019 to approximately 220 advisory clients regarding takeovers of three Cetera Advisors and Cetera Investment Advisers representatives' email accounts included template language regarding the timing of the incidents that was misleading in light of the circumstances. In particular, the breach notifications referred to the incidents as "recent" and stated that the representatives had "learned that an unauthorized individual gained access" to the recipient's PII two months before the breach notification. Each entity, however, had learned of the underlying breach at least six months earlier. The dates referenced in the letters were the dates the firms completed PII review of compromised email accounts and determined that particular recipient's PII may have been

accessed. This language in the breach notifications created a misleading impression that the incidents had occurred much more recently than they had and that each firm had learned of the incidents and promptly notified its customers. Clients who were misinformed as to when the breaches occurred would not have known to look for or guard against potential misuse of their PII that may have occurred more than two months before they received the misleading notices.

19. At the time these letters were sent, Cetera Advisors' and Cetera Investment Advisers' policies and procedures for responding to cybersecurity incidents required the firms' personnel to review client communications regarding these incidents before the communications were sent to clients. Cetera Advisors and Cetera Investment Advisers failed to implement reasonably designed policies and procedures because that review was conducted in a manner that failed to correct template language that was misleading in light of the circumstances known to the firms at the time of the review.

Violations

20. As a result of the conduct described above, Cetera Entities willfully[9] violated the Safeguards Rule, which requires every broker-dealer and every investment adviser registered with the Commission to adopt written policies and procedures that are reasonably designed to safeguard customer records and information.

21. As a result of the conduct described above, Cetera Advisors and Cetera Investment Advisers willfully violated Section 206(4) of the Advisers Act and Rule 206(4)-7 thereunder (17 C.F.R. § 275.206(4)-7), which require a registered investment adviser, or an investment adviser required to register, to adopt and implement written compliance policies and procedures reasonably designed to prevent violations of the Advisers Act and the rules thereunder.

Cetera Entities' Remedial Efforts

22. In determining to accept the Offer, the Commission considered remedial acts undertaken by Cetera Entities.

IV.

In view of the foregoing, the Commission deems it appropriate and in the public interest to impose the sanctions agreed to in Respondents' Offer. Accordingly, pursuant to Sections 15(b) and 21C of the Exchange Act and Sections 203(e) and 203(k) of the Advisers Act, it is hereby

[9] "Willfully," for purposes of imposing relief under Section 15(b) of the Exchange Act and Section 203(e) of the Advisers Act "'means no more than that the person charged with the duty knows what he is doing.'" *Wonsover v. SEC*, 205 F.3d 408, 414 (D.C. Cir. 2000) (quoting *Hughes v. SEC*, 174 F.2d 969, 977 (D.C. Cir. 1949)). There is no requirement that the actor "also be aware that he is violating one of the Rules or Acts." *Tager v. SEC*, 344 F.2d 5, 8 (2d Cir. 1965). The decision in *The Robare Group, Ltd. v. SEC*, which construed the term "willfully" for purposes of a differently structured statutory provision, does not alter that standard. 922 F.3d 468, 478-79 (D.C. Cir. 2019) (setting forth the showing required to establish that a person has "willfully omit[ted]" material information from a required disclosure in violation of Section 207 of the Advisers Act).

ORDERED that:

A. Cetera Entities cease and desist from committing or causing any violations and any future violations of Rule 30(a) of Regulation S-P (17 C.F.R. § 248.30(a));

B. Cetera Advisors and Cetera Investment Advisers cease and desist from committing or causing any violations and any future violations of Section 206(4) of the Advisers Act and Rule 206(4)-7 thereunder (17 C.F.R. § 275.206(4)-7);

C. Cetera Entities are censured; and

D. Cetera Entities shall, within 10 (ten) business days of the entry of this Order, pay a civil money penalty jointly and severally in the amount of $300,000 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) Cetera Entities may transmit payment electronically to the Commission, which will provide detailed ACH transfer/Fedwire instructions upon request;

(2) Cetera Entities 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) Cetera Entities may pay by certified check, bank cashier's check, or United States Postal Service 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 Cetera Entities as Respondents 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: A. Kristina Littman, Cyber Unit Chief, Division of Enforcement, Securities and Exchange Commission, 100 F St., NE, Washington, DC 20549.

E. 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, Cetera Entities agree that in any Related Investor Action, they shall not argue that they are entitled to, nor shall they benefit by, offset or reduction of any award of compensatory damages by the amount of any part of Cetera Entities' payment of a civil penalty in this action ("Penalty Offset"). If the court in any Related Investor

Action grants such a Penalty Offset, Cetera Entities agree that they 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 Cetera Entities 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