UNITED STATES OF AMERICA
Before the
SECURITIES AND EXCHANGE COMMISSION

SECURITIES EXCHANGE ACT OF 1934
Release No. 92807 / August 30, 2021

INVESTMENT ADVISERS ACT OF 1940
Release No. 5840 / August 30, 2021

ADMINISTRATIVE PROCEEDING
File No. 3-20495

In the Matter of

KMS FINANCIAL SERVICES, INC.

Respondent.

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 KMS Financial Services, Inc. ("KMS" 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 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 Respondent's Offer, the Commission finds that:

Summary

1. These proceedings arise out of KMS's failure to adopt written policies and procedures reasonably designed to safeguard customer records and information, in violation of Rule 30(a) of Regulation S-P (17 C.F.R. § 248.30(a)) (the "Safeguards Rule").

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. KMS, a dually registered broker-dealer and investment adviser, violated the Safeguards Rule by failing to adopt written policies and procedures reasonably designed to safeguard records and information of its brokerage customers and advisory clients (hereafter "customers"), including personal identifying information ("PII") stored on a cloud-based electronic mail ("email") system, which KMS's registered representatives and registered investment adviser representatives ("financial advisers") used for internal and external communications. Between September 2018 and December 2019, fifteen KMS financial adviser email accounts were accessed by unauthorized third parties resulting in the exposure of customer records and information, including PII,[1] of approximately 4,900 KMS customers. Furthermore, KMS's incident response policy was not reasonably designed to ensure that the email account compromises were remediated in a timely manner to ensure the protection of customer PII. Although KMS discovered the first email account compromise in November 2018, it failed to adopt written policies and procedures requiring additional firm-wide security measures for all KMS email users until May 2020, and did not fully implement those measures until August 2020. This resulted in the exposure of sensitive customer records and information, including PII, of thousands of KMS customers throughout 2019 and the potential exposure of additional customer records and information until August 2020.

Respondent

4. KMS Financial Services, Inc. ("KMS") was a Seattle-based dually registered broker-dealer and investment advisory firm. KMS was registered with the Commission as an investment adviser between April 1976 and November 2020, and as a broker-dealer between January 1970 and January 2021. Between October 2014 and February 2020, KMS was wholly owned by Ladenburg Thalmann Financial Services, Inc. ("Ladenburg"), which was a publicly traded company (NYSE: LTS). In February 2020, Ladenburg merged into Advisor Group

[1] As used in this Order, "exposure of customer records and information, including PII," means that an unauthorized third party has the ability to view (but has not necessarily viewed) the customer records and information, including PII.

Holdings, Inc., the parent company of several subsidiaries, including two affiliates separately registered with the Commission as a broker-dealer (Securities America, Inc.) and as an investment adviser (Securities America Advisors, Inc.). In November 2020, KMS assigned its investment advisory assets to Securities America Advisors, Inc. and merged its broker-dealer into Securities America, Inc. KMS then withdrew its broker-dealer and investment advisory firm registrations.

Background

5. Between September 2018 and August 2020 (the "relevant time period"), KMS offered customers services through a network of more than 400 financial advisers who were independent contractors.[2]

6. KMS employees and independent contractors, including financial advisers, used a cloud-based email system for internal and external communications, regularly received and sent cloud-based emails containing customer PII, and stored customer PII in cloud-based email files.

7. KMS independent contractors, including financial advisers and their assistants, generally used their own computer equipment and networks, including protective infrastructure and software, such as encryption, antivirus protection, and local password storage requirements.

KMS's Written Policies and Procedures

8. During the relevant time period, KMS financial advisers were required to comply with KMS's written Policy Manual. Section 6.8 of the Policy Manual, entitled "Privacy Policy and Required Security Safeguards," required financial advisers to "[c]onduct your business practices in a way that safeguards the confidentiality of your client's identity, including protecting all sensitive client information" and to "[p]eriodically review your internal business policies to make sure they are adequately designed to protect sensitive client information."[3] The KMS Policy Manual stated that financial advisers were obligated to adhere to KMS' Computer and Network Security Policies ("CNSP").

---

[2] The independent contractor representatives were investment adviser representatives of KMS or were associated persons of KMS who were licensed as registered representatives or otherwise qualified to effect transactions in securities on behalf of KMS. 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)").

[3] The KMS Policy Manual identified "[s]ensitive information" as including Social Security or tax identification numbers; account numbers; information identifying account holdings, transactions, or balances; relationships with other individuals or organizations; income, net worth, or other aspects of financial dealings; email addresses; and information received from a consumer reporting agency.

9. The CNSP contained requirements for certain technical security issues, such as maintaining strong passwords, securing wireless networks, using anti-virus and malware protection, securing backup and stored data, and encrypting hard drives. The CNSP recommended, but did not require, the use of multi-factor authentication ("MFA")[4] for accessing sensitive data. The CNSP required KMS financial advisers to notify KMS of any suspected cybersecurity breaches.

Email Account Takeover Activity

10. During the relevant time period, fifteen KMS financial advisers experienced email account takeovers[5] in which unauthorized persons accessed the email accounts of the financial advisers or their assistants and had the ability to take action in the accounts. Collectively, these email account takeovers resulted in the exposure of customer records and information, including PII that falls within the scope of Regulation S-P, for approximately 4,900 KMS customers. In many of these instances, emails containing customer PII were forwarded to unauthorized email addresses outside of KMS. In some instances, customers received "phishing"[6] emails that requested them to: (a) wire funds to a bank account; (b) enter PII (such as a driver's license number or Social Security number) to access a document; or (c) click on a link to view an investment recommendation, which would grant access to the customer's computer.

11. After the email account takeovers were discovered, KMS had the affected financial advisers' email passwords reset, forwarding rules removed, and MFA enabled. However, these security measures were not fully implemented firm-wide until August 2020, which was approximately 21 months after discovery of the first breach, in which approximately 2,700 emails of one KMS financial adviser were exposed for a period of 26 days during which unauthorized third parties forwarded the financial adviser's emails to an email address outside of the firm.

12. KMS also hired two forensic firms to investigate the email account takeovers, including whether customer records and information had been exposed, notified affected customers, and offered credit monitoring services to affected customers. The forensic firms issued an incident report for each email account takeover that summarized the incidents and remedial measures taken, including resetting passwords and enabling MFA on the affected

[4] MFA requires at least one authentication factor in addition to a username and password to log in 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.

[5] 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.

[6] 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.

accounts.[7] Several of the incident reports recommended the expedited enabling of MFA for all KMS independent contractor email addresses.

13. Despite the recommendations for expedited enabling of MFA, KMS failed to adopt written policies and procedures requiring additional firm-wide security measures for all KMS email users, such as MFA, until May 2020, when it issued new policies and procedures. By then, KMS had begun implementing additional security measures, such as MFA, but KMS did not fully implement those measures firm-wide until August 2020. This timeline placed at risk the security of additional customer records and information.

14. KMS lacked its own Incident Response Policy and used an Incident Response Policy tailored to a different Ladenburg subsidiary, which required completion of a particular incident response form but failed to include guidelines on timeframes or schedules for response activities. Written summaries concerning the email account takeovers were not completed until several months after the discovery of the incidents.

15. The fifteen email account takeovers do not appear to have resulted in any unauthorized trades or fund transfers to unauthorized parties for any KMS customer accounts.

Violation

16. As a result of the conduct described above, KMS willfully[8] violated the Safeguards Rule, which requires every broker-dealer and every investment adviser registered with the Commission to adopt written policies and procedures reasonably designed to safeguard customer records and information.

KMS's Remedial Efforts

17. In determining to accept the Offer, the Commission considered remedial acts undertaken by Respondent.

IV.

In view of the foregoing, the Commission deems it appropriate and in the public interest to impose the sanctions agreed to in Respondent KMS's Offer. Accordingly, pursuant to Sections

[7] In July 2018, KMS received an audit report from a third party that recommended a review of remote access systems and consideration of stronger access controls, such as two-factor authentication. Therefore, by the time of the first email account takeover in September 2018, KMS had known for several months that remote access to its systems needed stronger security controls.

[8] "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).

15(b) and 21C of the Exchange Act and Sections 203(e) and 203(k) of the Advisers Act, it is hereby ORDERED that:

A. Respondent KMS 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. Respondent KMS is censured; and

C. Respondent KMS shall, within 10 (ten) business days of the entry of this Order, pay a civil money penalty in the amount of $200,000 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 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 KMS 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: A. Kristina Littman, Cyber Unit Chief, Division of Enforcement, Securities and Exchange Commission, 100 F St., NE, Washington, DC 20549.

D. 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