

UNITED STATES OF AMERICA
Before the
SECURITIES AND EXCHANGE COMMISSION

SECURITIES EXCHANGE ACT OF 1934
Release No. 92806 / August 30, 2021

INVESTMENT ADVISERS ACT OF 1940
Release No. 5839 / August 30, 2021

ADMINISTRATIVE PROCEEDING
File No. 3-20496

In the Matter of

**Cambridge Investment Research,
Inc. and Cambridge Investment
Research Advisors, Inc.,**

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”) 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 Cambridge Investment Research, Inc. and Cambridge Investment Research Advisors, Inc. (together, “Cambridge” 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 it 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 that:

Summary

1. These proceedings arise out of Cambridge's 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").

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. Respondents are registered with the Commission as a broker dealer and an investment adviser. From January 2018 through July 1, 2021 (the "Relevant Period"), cloud-based email accounts of over 121 Cambridge independent contractor representatives¹ were taken over² by third parties resulting in the exposure of at least 2,177 customers' personally identifiable information ("PII") stored in the compromised email accounts and potential exposure of another 3,800 customers' PII.³ Although Cambridge discovered the first email account takeover in January 2018, it failed to adopt and implement firm wide enhanced security measures for cloud-based email accounts of its independent representatives in its written policies and procedures, such as the use of multi-factor authentication ("MFA")⁴, for all Cambridge users until 2021. This resulted in the exposure of sensitive customer records and information, including PII, of Cambridge customers

¹ The independent contractor representatives were investment adviser representatives of Cambridge or were associated persons of Cambridge who were licensed as registered representatives or otherwise qualified to effect transactions in securities on behalf of Cambridge. 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))."

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 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.

and the potential exposure of additional customer records and information.

Respondents

4. Cambridge Investment Research, Inc. is an Iowa corporation headquartered in Fairfield, Iowa, and registered as a broker-dealer with the Commission.

5. Cambridge Investment Research Advisors, Inc. is an Iowa corporation headquartered in Fairfield, Iowa, and registered as an investment adviser with the Commission.

Background

6. Respondents are a registered broker-dealer and a registered investment adviser with approximately 4,750 registered representatives and investment adviser representatives (collectively, “representatives”). Approximately 420 of the representatives are based in Cambridge’s home offices in Fairfield, Iowa, Atlanta, Georgia, and Phoenix, Arizona. Approximately 4,330 individuals are registered with FINRA as independent contractors and associated with independent branch offices providing brokerage and investment advisory services throughout the United States (“independent representatives”).

7. Although Cambridge has an information security group at its headquarters that provided its independent representatives with cybersecurity guidance and policies and procedures, each independent representative was responsible for implementing cybersecurity measures. During the Relevant Period, some Cambridge independent representatives used cloud-based electronic mail (“email”) services for internal and external communications and routinely emailed and stored PII of Cambridge’s brokerage customers and advisory clients (hereinafter, “customers”) in these email accounts.

8. Throughout the Relevant Period, Cambridge’s policies recommended, but did not require, independent representatives to implement enhanced security measures, such as MFA, on cloud-based email accounts.

Email Account Takeover Activity

9. During the Relevant Period, Cambridge discovered that email accounts of 121 independent representatives were taken over by unauthorized third parties via phishing,⁵ credential stuffing,⁶ or other modes of attack. Several of the compromises involved emails, some containing PII, being forwarded from the independent representatives’ accounts to unauthorized third parties outside of Cambridge. Other incidents involved phishing, in which customers received

⁵ 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.

⁶ 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.

emails purporting to be from the independent representative requesting that they provide PII or click on a link. Two incidents involved attempts to obtain funds from customer accounts.

10. For certain types of compromises, including those in which an intruder forwarded email from the compromised account to an external third-party account, Cambridge conducted a forensic analysis of the affected email accounts to determine whether customer PII had been exposed. Cambridge determined that PII of at least 2,177 customers had been exposed through such compromises. The independent representatives notified these customers of the compromise and facilitated the offering of identity theft protection services to the affected customers.

11. For other types of compromises, including those in which an intruder used a compromised account to send phishing emails to third parties, Cambridge typically did not conduct a forensic analysis of the compromised email account. For some of these incidents, the independent representatives chose to notify all of their customers that the account had been compromised and that customer PII was potentially exposed. Cambridge notified approximately 3,800 customers of such potential exposure.

12. The email account takeovers do not appear to have resulted in any unauthorized trades or fund transfers to unauthorized parties from any Cambridge customer accounts.

13. After the email account takeovers were discovered, Cambridge suspended the affected independent representatives' accounts and reset the independent representatives' passwords. Cambridge recommended that these independent representatives implement MFA for the affected accounts. Cambridge, however, did not require any other enhanced security measure to prevent similar compromises in the future, such as implementation of MFA, for cloud-based email accounts. Although some of the independent representatives followed Cambridge's recommendation and implemented MFA, many did not. In addition, Cambridge continued its practice of recommending but not requiring the rest of its independent representatives to implement MFA for its cloud-based email accounts.

14. In April 2021, Cambridge revised its policy to require MFA for all cloud-based email accounts, effective July 1, 2021. On May 10, 2021, Cambridge informed its independent representatives of the MFA policy and provided the independent representatives with resources to facilitate implementation of MFA.

Violations

15. As a result of the conduct described above, Cambridge willfully⁷ violated the Safeguards Rule, which requires every broker-dealer and every investment adviser registered

⁷ "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).

with the Commission to adopt written policies and procedures that are reasonably designed to safeguard customer records and information.

Cambridge's Remedial Efforts

16. In determining to accept the Offer, the Commission considered remedial acts undertaken by Cambridge.

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 ORDERED that:

A. Respondents 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));

C. Respondents are censured; and

D. Respondents shall, within 10 (ten) business days of the entry of this Order, pay a civil money penalty jointly and severally in the amount of \$250,000 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) Respondents may transmit payment electronically to the Commission, which will provide detailed ACH transfer/Fedwire instructions upon request;
- (2) Respondents 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) Respondents 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 Cambridge 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, D.C. 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, Respondents 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 Respondents' payment of a civil penalty in this action ("Penalty Offset"). If the court in any Related Investor Action grants such a Penalty Offset, Respondents 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 Respondents 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