

UNITED STATES OF AMERICA
Before the
SECURITIES AND EXCHANGE COMMISSION

SECURITIES EXCHANGE ACT OF 1934
Release No. 83848 / August 15, 2018

INVESTMENT ADVISERS ACT OF 1940
Release No. 4985 / August 15, 2018

ADMINISTRATIVE PROCEEDING
File No. 3-18642

In the Matter of

**Ameriprise Financial Services,
Inc.,**

Respondent.

**ORDER INSTITUTING
ADMINISTRATIVE AND CEASE-AND-
DESIST PROCEEDINGS, PURSUANT TO
SECTION 15(b) 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 (“Commission”) deems it appropriate and in the public interest that public administrative and cease-and-desist proceedings be, and hereby are, instituted pursuant to Section 15(b) of the Securities Exchange Act of 1934 (“Exchange Act”) and Sections 203(e) and 203(k) of the Investment Advisers Act of 1940 (“Advisers Act”) against Ameriprise Financial Services, Inc. (“Ameriprise” 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 Section 15(b) 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 finds¹ that:

A. Introduction

1. This matter concerns the failure of Ameriprise, a dually-registered investment adviser and broker-dealer, to adopt and implement policies and procedures reasonably designed to safeguard retail investor assets against misappropriation by the firm’s representatives. Ameriprise provides investment advisory and brokerage services to advisory clients and brokerage customers (together, “the clients”) through a national network of approximately 9,700 representatives.² From 2011 through 2014 (the “relevant period”), as part of its compliance and supervisory systems, Ameriprise employed certain automated surveillance tools to prevent and detect whether a representative may have engaged in fraud by misappropriating funds from a client account. One system did not function properly and a second faced limitations, thereby preventing Ameriprise from detecting the misappropriation of over \$1 million in client funds by five representatives.

2. The first, known as the Fraud Early Detection System (“FEDS”), was intended, among other things, to identify situations where a representative attempted to change the address associated with a client’s account to an address controlled by the representative (such as his home or business address). Ameriprise considered attempts to replace a client’s address with an address controlled by a representative to be suspicious and indicative of a possible attempt to improperly gain control of the client’s account and misappropriate funds. However, because of a technical error that went undetected until December 2013, FEDS did not function properly. Specifically, it did not identify instances where a representative sought to gain control of a client’s account by improperly changing the address associated with the account to one that the representative controlled. One representative was able to perpetrate a fraud on two of her retail clients without Ameriprise detecting that the representative and her daughter improperly replaced client addresses on the account with their controlled addresses.

¹ The findings herein are made pursuant to Respondent’s Offer of Settlement and are not binding on any other person or entity in this or any other proceeding.

² Ameriprise’s representatives encompass both registered representatives of the broker-dealer and investment adviser representatives associated with the investment adviser (referred to herein collectively as the “representatives”). As of December 31, 2016, Ameriprise’s nationwide advisor network consisted of approximately 9,700 advisors. Approximately 7,700 of those advisors are independent franchisees or employees or contractors of franchisees who operate within the group, Ameriprise Franchise Group (“AFG”). Franchise advisors are not employees of Ameriprise and operate independent businesses under the Ameriprise brand name. A significant number of AFG representatives are located in offices primarily made up of one to three representatives. The remaining 2,000 Ameriprise advisors are employees of the firm (known as employee advisors) and operate within the group, Ameriprise Advisors Group (“AAG”). Franchise and employee advisors were subject to the same supervisory and compliance policies and procedures, including those that relate to the prevention and detection of fraud against clients of the firm.

3. The second, an automated transaction-based analysis tool (hereinafter “Analysis Tool”), was intended to identify, among other things, situations where a representative attempted to direct a cash disbursement from a client account to an address controlled by a representative. Ameriprise viewed such a money movement as an indicator that a representative could be engaged in fraudulent activities. However, during the relevant period, because of a limitation in its design, with respect to cash disbursements via check, the Analysis Tool was unable to detect certain unauthorized disbursements from client accounts to addresses associated with the representative. In addition, the Analysis Tool was not utilized to detect fraudulent money movements where the disbursement was made by wire transfer. Ameriprise relied on a manual process to detect wire transfers to external accounts controlled by a representative. On multiple occasions during the relevant period, Ameriprise did not detect the fraudulent transfer of funds from client accounts to destinations that were controlled by its representatives.

4. Each of the five representatives at issue, who are identified in Part III.C.3, was terminated by Ameriprise for misappropriating client funds (the “Terminated Representatives”). In violation of their fiduciary duties under the Advisers Act to their clients, the Terminated Representatives committed numerous unauthorized acts, including forging client documentation, making unauthorized address changes, and/or submitting requests to disburse client funds without their clients’ knowledge or approval. All of the Terminated Representatives violated Sections 206(1) and 206(2) of the Advisers Act. Moreover, because in some instances, the misappropriation was in connection with the sale of securities, certain of the Terminated Representatives violated Section 10(b) of the Exchange Act and Rule 10b-5 thereunder.

5. As a result of the foregoing, Ameriprise violated Section 206(4) of the Advisers Act and Rule 206(4)-7 thereunder, and failed reasonably to supervise the Terminated Representatives within the meaning of Section 203(e)(6) of the Advisers Act and Section 15(b)(4) of the Exchange Act with a view to preventing and detecting the Terminated Representatives’ violations of Sections 206(1) and 206(2) of the Advisers Act and Section 10(b) of the Exchange act and Rule 10b-5 thereunder.

B. Respondent

6. **Ameriprise Financial Services, Inc. (“Ameriprise”)** is dually registered with the Commission as an investment adviser and broker-dealer. Ameriprise, which is incorporated in the state of Delaware, is a diversified financial services firm with its principal corporate office in Minneapolis, Minnesota. Ameriprise is a wholly owned subsidiary of Ameriprise Financial, Inc., a publicly-traded company. Ameriprise has approximately 9,700 representatives, maintains approximately 3,800 branch offices, and reported assets under management of approximately \$198 billion in its Form ADV dated August 31, 2017.

C. Facts

1. Ameriprise’s Supervisory and Compliance Framework to Prevent Fraud

7. Ameriprise had certain supervisory and compliance responsibilities under the Exchange Act as a broker-dealer, and under the Advisers Act as an investment adviser. As a broker-dealer, Ameriprise was required to establish procedures, and a system for applying such

procedures, to reasonably supervise its associated persons with a view to preventing their violations of the federal securities laws. As an investment adviser, in addition to supervising its associated persons, Ameriprise was required to adopt and implement written compliance policies and procedures that were reasonably designed to prevent its associated persons from engaging in fraudulent activities. In fulfilling these supervisory and compliance responsibilities, Ameriprise considered the possibility of fraud, theft, or misappropriation by its representatives to be a risk area that could impact its business and took steps to address that risk. Ameriprise categorized fraud and the misappropriation of client assets as a prohibited activity and designed and implemented policies, procedures, and controls to prevent and detect such misconduct.

8. As part of its general supervisory and compliance framework, Ameriprise employed a hybrid supervisory system to oversee its geographically-dispersed national network of representatives, in which it combined aspects of a field-based model of supervision and a centralized supervisory model.

9. Front-line supervision of representatives was conducted by a field-based supervisor, known as a registered principal. The registered principal was responsible for monitoring the activities of the representatives within a particular geographic location. The registered principal conducted supervision by direct contact through telephone, e-mail, and occasional in-person reviews. Among other things, registered principals were responsible for supervision to prevent and detect prohibited activities. The registered principal was also responsible for conducting an annual office inspection.

10. In addition to field-based supervision, each representative was also supervised by a Centralized Supervision Unit (“CSU”). The CSU contained over 175 registered principals in Ameriprise’s corporate offices that reviewed securities transactions and certain other activities of the representatives located in the field. CSU’s supervisory authority, unlike field-based registered principals, was not limited to a group of representatives in a particular geographical location. As an example, CSU registered principals supervised new account opening, client securities transactions, sales and other marketing materials, mail and check logs, e-mail, and review of OBAs.

11. In addition to the hybrid supervisory model, during the relevant period, Ameriprise implemented additional policies, procedures, and controls designed to prevent and detect fraud by a representative against a firm client.³ For instance, among the controls designed to prevent and detect fraud by unauthorized money movement was Ameriprise’s cashiering group. This group generally reviewed requests to move client funds and determined whether there was adequate information provided on the form, whether there were sufficient funds to approve the transaction, and whether the signature appeared to be authentic. If the signature appeared to be suspicious, Ameriprise conducted additional investigation of the request to determine if the request was authentic or fraudulent. In addition, Ameriprise maintained an anti-fraud group that was responsible for conducting an initial inquiry into suspicious activity by a representative. If further investigation was warranted, the matter was referred to Ameriprise’s complaints and investigations

³ The procedures relating to money movement controls described in Parts III.C.1 and III.C.2 of this Order were in place during the relevant period. In December 2014, Ameriprise began implementing a new automated money movement system, with the capability to review outgoing wire transfers.

group. Such an investigation could entail contacting potentially impacted clients or the representative suspected of misconduct, as well as review of client account documents.

12. The Terminated Representatives whose conduct is further described in Part III.C.3 *infra* were subject to the foregoing supervisory system for at least certain of their fraudulent acts.

2. Ameriprise's Automated Systems to Prevent and Detect Misappropriation of Retail Client Assets

13. As noted above, Ameriprise considered fraud by its representatives, including the misappropriation or theft of client assets, to be prohibited activities so Ameriprise designed and implemented a compliance and supervisory framework intended to prevent and detect such misconduct. Within that framework, during the relevant period, Ameriprise relied on various manual and automated tools to prevent and detect possible misappropriation. Manual tools involved the direct review, analysis, and investigation of data or information by Ameriprise personnel for the purpose of identifying facts and circumstances that directly or indirectly indicated the possibility of fraud.⁴ Automated tools, by contrast, reviewed large quantities of data to flag, using pre-set criteria and thresholds, suspicious or unusual transactions or events that could be indicative of fraud. Because of the volume of transactions and client activity that Ameriprise processed on a daily basis, the success of Ameriprise's supervisory and compliance framework, both generally and as it related to the detection and prevention of prohibited activities, depended on the effectiveness of both manual and automated tools.

14. During a part of the relevant period, certain aspects of two of Ameriprise's automated tools utilized to detect fraud and misappropriation by a representative did not operate effectively.

a. Controlled address review

15. From time to time, Ameriprise received requests to change the address associated with a client's account. Many of the address change requests were routine, reflecting, for instance, the fact that a client may have moved to a new home. However, Ameriprise considered certain types of address changes to raise heightened concerns and merit additional scrutiny for the purpose of identifying potential misconduct.

16. One such type of address change, involving so-called "controlled addresses," is relevant here. In particular, Ameriprise's Compliance Manual prohibited a representative from controlling a client's address, or receiving mail directly on behalf of a client. Ameriprise prohibited such a practice even if a client had requested that the representative receive mail on his or her behalf. Ameriprise considered a situation where a representative controlled the address on a

⁴ For instance, with respect to certain disbursement requests from client accounts, Ameriprise personnel visually inspected client signatures on forms for evidence of forgery. In making such a determination, reviewers compared signatures on a disbursement request against signatures on other account documents, such as an account opening document. The signature analysis was a manual process, relying principally on the judgment, skill, and thoroughness of the reviewer.

client's account to present a risk of fraud and misappropriation, as the representative could take unauthorized account actions without the client learning of such actions.

17. To prevent a situation where one of its representatives gained control of a client's account through the use of a controlled address, during the relevant period, Ameriprise relied on a surveillance system referred to as FEDS. FEDS, which operated on an automated basis, was used by Ameriprise for numerous purposes, including, as relevant here, to review for unauthorized address changes to a client's account.

18. During the relevant period, FEDS was intended to operate as follows. When Ameriprise received a request for an address change to an existing account, whether over telephone, via online, or via a change of address form, the new address was provided to FEDS, which in turn compared the new address against a "hot list" of information. The "hot list" included personal information, such as addresses, of persons associated with Ameriprise, including the firm's representatives. If the new address submitted as part of the request to change an address matched an address on the "hot list," an alert was generated in FEDS.

19. The alert was then to be forwarded to Ameriprise's anti-fraud group for further inquiry. The anti-fraud group was responsible for reviewing the alert to determine whether the address change was initiated in violation of firm policy. If the anti-fraud group had concerns regarding the representative's conduct, it would work with CSU or the complaints and investigations group to conduct further investigation. Such investigation could involve contacting the client to confirm whether the client had initiated the address change or contacting the representative to clarify whether they controlled the address in question.

20. For most of the relevant period, however, the parameter in FEDS relating to address changes did not operate as intended. Because of a technical error, FEDS did not generate a flag in instances when there was a positive match between a changed address on an existing account and a "controlled address." As a consequence, FEDS did not compare the changed address to addresses associated with Ameriprise representatives and other personnel. Ameriprise was unaware of the error for most of the relevant period. Moreover, until December 2013, Ameriprise did not conduct any system testing that could have uncovered the error.

21. As a result of the flaw in the operation of FEDS, Ameriprise was unable to detect certain misappropriation of client assets by its representatives, Barbara Stark and Susan Walker. Stark and/or Walker changed the addresses of two of their clients to Stark's office address and Walker's home address, respectively. These changes should have been detected by FEDS but were not because of the technical error noted above. After the discovery of the fraud, Ameriprise remedied the technical problem with the operation of FEDS in December 2013.

b. Money movement controls

22. During the relevant period, Ameriprise processed millions of requests to transfer money out of client accounts. A number of such requests were initiated by Ameriprise clients seeking to transfer funds from a client account to another Ameriprise client account or to a third party outside Ameriprise. To initiate such a money movement, an Ameriprise client could take any one of several steps, including completing a written disbursement request or contacting their

representative. The money movement, in turn, could take several forms, including, and of relevance here, a check disbursement or wire transfer.

23. Ameriprise recognized that money movements out of client accounts created a risk of fraud and misappropriation. Ameriprise's policies and procedures prohibited its representatives from misappropriating client funds and from moving funds out of a client account without proper authorization. For instance, the firm's Compliance Manual noted that representatives are prohibited from "mingl[ing] client money with [their] own" and from "deposit[ing] client funds in any bank or other financial institution's account over which [the representative has] control." A purpose of this policy was to prevent a representative from committing fraud or misappropriation against a client of the firm.

24. During the relevant period, Ameriprise designed and implemented a series of money movement controls, both manual and automated, to prevent and detect unauthorized money transfers. A critical component of Ameriprise's money movement controls was an automated, transaction-monitoring tool known as the Analysis Tool. Certain money movement transactions flowed through the Analysis Tool, which contained logic implemented by Ameriprise for the purpose of identifying cash disbursements via check that raised concerns regarding possible fraud. In the event that the Analysis Tool flagged a transaction as potentially problematic, it would trigger a surveillance alert. That alert was then routed to Ameriprise anti-fraud personnel for further investigation.

25. Ameriprise created an alert in the Analysis Tool to identify cash disbursements via check, defined to include a circumstance where the name of the payee or the address of the payee matched to a name or address that Ameriprise knew was associated with or controlled by one of its representatives. The Analysis Tool looked for name and address matches against a database compiled by Ameriprise, known as the "hot list," that contained personal information regarding its representatives. For instance, if Ameriprise received a request to disburse client funds via check to one of its representatives, or to a person with the same address as one of its representatives, the Analysis Tool was supposed to flag such a money movement transaction as suspicious, so that further investigation could be conducted.

26. The Analysis Tool's ability to prevent and detect fraud or misappropriation by its representatives, however, was substantially limited during the relevant period.

27. As it relates to check disbursement requests, the Analysis Tool had a design limitation that impacted its capability to detect certain suspicious disbursements, even where the check was made payable to a payee with an address known by Ameriprise to be associated with a representative. This was because the Analysis Tool required an exact match between the information associated with the disbursement request and the information in the "hot list." In other words, if there was an immaterial difference between the information on a check disbursement request and the "hot list"—for instance, if the address information differed as between "Avenue" and "Ave."—the Analysis Tool would not flag the transaction as suspicious. Because of the exact match requirement, the Analysis Tool was not reasonably designed to flag disbursement transactions that involved a check being made out to a representative or being sent to an address known by Ameriprise to be associated with or controlled by the representative.

28. Moreover, the Analysis Tool was not being used to flag wire disbursements that entailed money being sent from a client account to an account known by Ameriprise to be associated with and controlled by the representative.

29. In light of the foregoing, Ameriprise lacked a reasonable mechanism to prevent and detect situations where a representative sought to misappropriate money from a client account, whether by check or wire. As a consequence, during the relevant period and as noted below, Ameriprise disbursed money from client accounts via third party checks and wires on multiple occasions to payees, addresses, and/or external accounts that it knew or should have known were associated with and controlled by its representatives.

30. Ameriprise's aforementioned failure to design and implement a reasonable mechanism to prevent and detect potentially fraudulent money movements by its representatives occurred after Ameriprise became aware, in 2010, that one of its representatives, Jennifer Guelinas, had perpetrated a fraud on two of the firm's clients during the time period 2006 to 2010.⁵ On at least two occasions, she wired money directly to a personal checking account pursuant to a wire transfer request that identified herself as the recipient. Ameriprise's then-existing money movement controls were unable to prevent or detect her fraudulent wire transfers.⁶

3. Ameriprise Representatives Engaged in Misconduct that Resulted in the Theft of Client Assets

31. During the relevant period, five Ameriprise representatives, discussed below, engaged in misconduct that entailed the misappropriation of client assets. Below are summaries of the fraudulent schemes perpetrated by the Terminated Representatives that resulted in the misappropriation of client assets. The fraudulent schemes entailed various unauthorized acts, including changing the address associated with a client account to an address controlled by the representative, or improperly transferring funds out of a client account to an account controlled by the representative. In addition, in some instances, the misappropriation was in connection with the sale of securities.

32. Ameriprise failed to adopt and implement policies, procedures, and controls that were reasonably designed to prevent and detect the misappropriation of client assets by the firm's representatives.

a. Barbara J. Stark and Susan Walker

33. Barbara J. Stark was a representative for 24 years and continuously from October 2008 to March 2013, when she was terminated. Stark operated as a franchise advisor from an

⁵ Guelinas pled guilty to wire fraud in connection with the misappropriation of funds and sentenced to four years of probation; the probation was later revoked, and she was sentenced to ten months in prison. *United States v. Guelinas*, No. 2:12-CR-00075-JTM-JEM (N.D. Ind. filed Apr. 27, 2012).

⁶ After discovering the misconduct in 2010, Ameriprise implemented several manual processes and reports to monitor for fraudulent wire transfers. Those processes and reports, however, did not prevent or detect the fraudulent wire transfers by one representative whose misconduct is described in Part III.C.3.

office located in Minnesota. She was assisted in that office by her daughter, Susan Walker, who was also a representative.

34. Stark serviced dozens of Ameriprise client accounts from October 2008 to March 2013. During that time, Walker acted as her assistant and called herself a paraplanner. Walker also acted as the formal record keeper of mail intake. Walker's control of the mail intake meant Ameriprise relied on her for accurate record keeping of all mail sent to the Ameriprise office. Stark was further subject to annual reviews by her applicable registered principal.

35. From 2008 and continuing to 2013, Stark and Walker perpetrated a fraud against certain Ameriprise clients. During that period, Stark and Walker engaged in approximately 600 fraudulent transactions and misappropriated \$1 million in client funds.

36. Stark and Walker forged client signatures on dozens of Ameriprise forms, including those to change the address of a client, to disburse funds via check, and to transfer funds by wire. For instance, on at least two occasions, Stark and/or Walker changed the addresses of two clients to Stark's office address and Walker's home address, respectively. Both addresses were known to Ameriprise to be associated with and controlled by Stark and Walker. Nonetheless, Ameriprise's compliance and supervisory policies and procedures failed to detect the unauthorized address changes. As noted above, because of a technical error in the operation of the FEDS, Ameriprise did not detect or prevent the unauthorized address changes by Stark and Walker.

37. Stark and Walker stole client funds through numerous methods, including via check disbursements, wire transfers, and Automated Clearing House (ACH) transactions. They perpetrated their fraud by submitting check disbursement requests to payees and/or addresses known by Ameriprise to be associated with and controlled by Stark and/or Walker. Nonetheless, Ameriprise's compliance and supervisory policies and procedures failed to detect the unauthorized money movements. As noted above, because the Analysis Tool required an exact match between information surrounding the check disbursement and the "hot list" information, and therefore was unable to detect that Stark and Walker had disbursed client funds via check to destinations that were under their control because of slight differences between information associated with the check disbursements and information in the "hot list."

38. In addition, Ameriprise personnel reviewed purported client signatures on a number of documents, including money disbursement forms, that had, in fact, been forged by Stark and/or Walker. However, Ameriprise failed to detect any of the signature forgeries during the period of their fraud. Ameriprise also had a process to send letter confirmations to clients of some significant transactions. The process, however, was ineffective because Ameriprise sent many of the transaction confirmations to Walker's home address (as opposed to the client address), an address known to Ameriprise. Ameriprise further became aware of information suggesting that Walker was improperly conducting an unauthorized OBA that involved providing tax preparation

services to clients. Ameriprise, however, failed to take reasonable steps to follow-up. Ameriprise was not aware that Walker utilized her personal e-mail address to communicate with clients.⁷

39. Ameriprise learned of the fraud by Stark and Walker after state regulatory authorities contacted the firm to inquire about the representatives' activities. After discovering the misconduct, Ameriprise terminated Stark and Walker in March 2013.⁸

b. Jeffrey Scott Davis

40. Jeffrey Scott Davis was a representative of Ameriprise from September 2000 to July 2013, when he was terminated. Davis operated as an Ameriprise franchise advisor from an office located in Virginia.

41. From 2012 to 2013, Davis perpetrated a fraud against five Ameriprise clients. During that period, he engaged in multiple fraudulent transactions and misappropriated \$200,000 in funds from client accounts.

42. In June 2012, Davis twice attempted to wire himself monies from a client account by submitting a facsimile letter providing the necessary details to effectuate a wire transfer. The first wire transfer request was to a recipient bank account in the name of "DGP Group LLC." The second wire transfer request was to a recipient bank account in the name of "D & G Company," although the account number provided was the same for both. Ameriprise knew that Davis had an outside business activity known as "DGP Group LLC," because Davis had previously disclosed it to Ameriprise. Even though it should have been apparent that Davis was attempting to wire money from a client account to an external party under his control, Ameriprise approved the transfer.

43. Notably, the recipient bank rejected the first wire transfer because it contained an incorrect routing number, while the second wire transfer failed because the name on the account did not match the recipient. However, an Ameriprise agent informed Davis of the errors and directed him to correct the mistakes, but failed to notice that Davis was attempting to wire himself money to a destination known by Ameriprise to be associated with and controlled by Davis. Davis ultimately misappropriated client funds through a combination of ACH transactions and forged checks.

⁷ Ameriprise's policies and procedures prohibited its representatives from communicating with clients using personal e-mail addresses. A representative's use of his or her personal e-mail address to communicate with clients limited Ameriprise's ability to monitor the communications for supervisory and compliance purposes.

⁸ FINRA barred Stark and Walker from association with any of its members in July 2013 for failing to appear for testimony before FINRA in connection with the allegations that they misappropriated client funds. FINRA Letter of Acceptance, Waiver and Consent, *In re Barbara J. Stark*, No. 20130365120 (June 13, 2013); FINRA Letter of Acceptance, Waiver and Consent, *In re Susan E. Walker*, No. 20130365117 (June 13, 2013). Walker pled guilty to mail fraud and tax evasion in connection with the misappropriation of funds and sentenced to 88 months in prison and fined \$1 million. *United States v. Walker*, No. 14-CR-00305-MJD (D. Minn. filed Sept. 22, 2014). Stark and Walker were also sanctioned by Minnesota for their misconduct. *In the Matter of Barbara J. Stark and Susan E. Walker*, Minnesota Dept. of Commerce, OAH File No. 80-1005-31355 (Oct. 19, 2014).

44. Davis had been the subject of prior discipline by Ameriprise. In October 2011, Davis received a letter of reprimand from Ameriprise and was fined \$1,000 for, among other things, an unauthorized transaction in a client account. In November 2012, Davis again received a letter of reprimand and was fined \$2,000 for engaging in unauthorized activities in client accounts. As a result, Davis was placed on heightened supervision by Ameriprise. Heightened supervision was a supervisory status that indicated a representative presented additional supervisory and compliance risk, thereby warranting closer scrutiny.⁹ After Davis was placed on heightened supervision, CSU identified a check transaction from a client account to DGP Group, LLC. Even though the check was deposited in an account controlled by Davis and that had been previously disclosed to Ameriprise, Ameriprise still was unable to detect and uncover Davis' fraudulent scheme. During the period that Davis was under heightened supervision, Ameriprise did not detect any of the fraudulent money movements.

45. Davis' fraud was discovered in 2013 after one of the victimized clients complained to Ameriprise about unusual money movement activity in his account.¹⁰ Ameriprise terminated Davis in July 2013.

c. Justin Weseloh

46. Justin Weseloh was a representative of Ameriprise from March 2010 to September 2013, when he was suspended and subsequently resigned while under investigation for misappropriation of client funds. Weseloh was employed by an Ameriprise franchise advisor in an office located in Ohio, where he assisted with the business of another Ameriprise representative.

47. From 2011 to 2013, Weseloh perpetrated a fraud against five Ameriprise clients. During that period, he engaged in multiple fraudulent transactions and misappropriated \$676,000 in funds from client accounts, of which approximately \$373,000 was misappropriated from Ameriprise accounts.

48. Weseloh stole client funds through unauthorized wire transfers. In particular, he submitted wire request forms to transfer funds from client accounts to an external account for an OBA that was controlled by him and the representative that employed him. The OBA and its bank account were known by Ameriprise to be associated with Weseloh. However, as noted previously, Ameriprise lacked a reasonable system to detect wire disbursements from a client account to an account known by Ameriprise to be associated with or controlled by the representative. Accordingly, Ameriprise failed to detect the unauthorized wire transfers by Weseloh.

49. In addition, Weseloh forged client signatures on a number of Ameriprise forms. Several of the relevant forms were flagged by Ameriprise as being irregular, but the firm failed to adequately investigate possible signature irregularities. Moreover, several of the wire requests were

⁹ During the period Davis was on heightened supervision, he was one of nine representatives who held that status.

¹⁰ Davis pled guilty to wire fraud in connection with the misappropriation of funds and sentenced to 54 months in prison. *United States v. Davis*, No. 2:14-CR-00102-RBS-DEM (E.D.Va. filed July 11, 2014).

flagged for further review by Ameriprise for unrelated reasons, but Ameriprise failed to conduct adequate follow up.

50. Weseloh's fraud came to be discovered in September 2013 when an office employee found evidence in a trash can that Weseloh had been attempting to copy the signature of a family member from whom he was attempting to steal funds.¹¹

d. Jennifer Johnson

51. Jennifer R. Johnson was a representative of Ameriprise from October 2009 to March 2016, when she was terminated. Johnson was employed by a franchise advisor in an office located in Minnesota, where she served as an associate financial advisor.

52. In 2014, Johnson perpetrated a fraud against an Ameriprise client and misappropriated \$21,000 in funds.

53. Johnson stole client funds through unauthorized check disbursements. Specifically, on two occasions in 2014, Johnson submitted unauthorized check disbursement forms directing that checks be drawn from an Ameriprise client account and made payable to a third-party business entity, Johnson Builders, and be sent to the OBA's address of record, which was Johnson's home address. Ameriprise knew, however, that Johnson operated an OBA by the same name because she had disclosed it previously to Ameriprise. The Analysis Tool, however, did not detect the improper money movements because there was not an exact match between the information on the check disbursement forms and the information known to Ameriprise regarding Johnson.

54. In both instances, Johnson affixed the client's signature for both of the aforementioned transactions from a previously unused document. Without the client's knowledge or consent, Johnson deposited the checks into the account of her OBA.

55. Johnson's fraud was discovered in February 2016 when Ameriprise's new automated money movement system detected the third attempt by Johnson to wire client funds to an account associated with the same OBA. Johnson was terminated in February 2016.¹²

D. Violations

56. As a result of the conduct described above, Ameriprise willfully violated Section 206(4) of the Advisers Act and Rule 206(4)-7 thereunder, which requires, among other things, that registered investment advisers adopt and implement written policies and procedures reasonably designed to prevent violations, by the investment adviser and its supervised persons, of the

¹¹ FINRA barred Weseloh from association with any of its members. FINRA Letter of Acceptance, Waiver and Consent, *In re Justin M. Weseloh*, No. 2013038611701 (June 17, 2014).

¹² Johnson pled guilty to misconduct arising out of her activities at Ameriprise and was sentenced to five days in prison and five years of probation plus restitution. *State of Minnesota v. Johnson*, No. 62-CR-16-7465 (Dist. Ct. 2d Jud. Dist. filed Nov. 8, 2016). FINRA barred Johnson from association with any of its members. FINRA Letter of Acceptance, Waiver and Consent, *In re Jennifer Rebecca Johnson*, No. 2016049086201 (Apr. 26, 2017).

Advisers Act and rules thereunder. Respondent failed to adopt and implement policies and procedures reasonably designed to prevent and detect the misappropriation of client assets by persons associated with the firm in violation of Sections 206(1) and 206(2) of the Advisers Act.

57. As a result of the conduct described above, Ameriprise failed reasonably to supervise the Terminated Representatives, within the meaning of Section 15(b)(4)(E) of the Exchange Act, with a view to preventing and detecting the Terminated Representatives' violations of Sections 206(1) and 206(2) of the Advisers Act and Section 10(b) of the Exchange Act and Rule 10b-5 thereunder.

58. As a result of the conduct described above, Ameriprise failed reasonably to supervise the Terminated Representatives, within the meaning of Section 203(e)(6) of the Advisers Act, with a view to preventing and detecting the Terminated Representatives' violations of Sections 206(1) and 206(2) of the Advisers Act and Section 10(b) of the Exchange Act and Rule 10b-5 thereunder.

E. Remedial Acts

59. In determining to accept Respondent's offer, the Commission considered the cooperation afforded the Commission's staff by Ameriprise and certain other remedial acts. Ameriprise voluntarily retained a compliance consultant to assess the reasonableness of its policies, procedures, and controls regarding the safeguarding of customer and/or client assets against theft or misappropriation by Ameriprise associated persons by means of the movement of funds through cash disbursements and checks, wire transfers, and ACH transactions. Ameriprise further reimbursed all impacted clients for the losses they incurred due to the misconduct of the Terminated Representatives. Ameriprise also took steps to enhance its policies and procedures designed to safeguard client assets against misappropriation by the firm's representatives, including by implementing a new automated money movement control system.

IV.

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

Accordingly, pursuant to Section 15(b)(4) the Exchange Act and Sections 203(e) and 203(k) of the Advisers Act, it is hereby ORDERED that:

- A. Ameriprise shall 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.
- B. Ameriprise is censured.
- C. Ameriprise shall, within 10 days of the entry of this Order, pay a civil penalty in the amount of \$4,500,000 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 SEC Rule of Practice 600 and 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 Ameriprise as the 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 Fuad Rana, Assistant Director, Division of Enforcement, Securities and Exchange Commission, 100 F Street N.E., Washington, DC 20549-6561A.

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.

Brent J. Fields
Secretary