UNITED STATES OF AMERICA
Before the
SECURITIES AND EXCHANGE COMMISSION

SECURITIES EXCHANGE ACT OF 1934
Release No. 84288 / September 26, 2018

INVESTMENT ADVISERS ACT OF 1940
Release No. 5048 / September 26, 2018

ADMINISTRATIVE PROCEEDING
File No. 3-18840

In the Matter of **Voya Financial Advisors, 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") 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 Voya Financial Advisors, Inc. ("VFA" 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 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 Exchange Act, and Sections 203(e) and 203(k) of the Advisers Act, 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 VFA'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"), and VFA's failure to develop and implement a written Identity Theft Prevention Program as required by Rule 201 of Regulation S-ID (17 C.F.R. § 248.201) (the "Identity Theft Red Flags Rule").

2. VFA is a dually registered broker-dealer and investment adviser. From at least 2013 through October 2017 (the "relevant period"), VFA gave its independent contractor representatives[1] ("contractor representatives") access to its brokerage customer and advisory client (hereinafter, "customer") information through a proprietary web portal. Through the portal, the contractor representatives accessed the personally identifiable information ("PII") of VFA customers and managed the customers' brokerage accounts. The portal was serviced and maintained by VFA's parent company, Voya Financial, Inc. ("Voya"). The contractor representatives generally used their own IT equipment and their own networks to access the portal. Voya's service call centers serviced support calls from VFA's customers and VFA's contractor representatives.

3. Over six days in April 2016, one or more persons impersonating VFA contractor representatives called VFA's technical support line and requested a reset of three representatives' passwords for the web portal used to access VFA customer information, in two instances using phone numbers Voya had previously identified as associated with prior fraudulent activity. The prior activity also involved attempts to impersonate VFA contractor representatives in calls to Voya's technical and customer support lines. Voya's technical support staff reset the passwords and provided temporary passwords over the phone, and on two of the three occasions, they also provided the representative's username.

4. Three hours after the first fraudulent reset request, the targeted contractor representative notified a technical support employee that he had received an email confirming the password change, but he had not requested such a change. Although VFA took certain steps to respond to the intrusion, those steps did not prevent the intruders from obtaining passwords and gaining access to VFA's portal by impersonating two additional representatives over the next several days. Nor did VFA terminate the intruders' access to the three representatives'

[1] The independent contractor representatives were associated persons of VFA who were licensed as registered representatives or otherwise qualified to effect transactions in securities on behalf of VFA, and some of them were also investment adviser representatives of VFA. 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), "The 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."

accounts due to deficient cybersecurity controls and an erroneous understanding of the operation of the portal.

5. The intruders used the VFA contractor representatives' usernames and passwords to log in to the portal and gain access to PII for at least 5,600 of VFA's customers, and subsequently to obtain account documents containing PII of at least one Voya customer. The intruders also used customer information to create new Voya.com customer profiles, which gave them access to PII and account information of two additional customers. There have been no known unauthorized transfers of funds or securities from VFA customer accounts as a result of the attack.

6. The Safeguards Rule requires every broker-dealer and every investment adviser registered with the Commission to adopt written policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information. Those policies and procedures must be 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.

7. VFA violated the Safeguards Rule because its policies and procedures to protect customer information and to prevent and respond to cybersecurity incidents were not reasonably designed to meet these objectives. Among other things, VFA's policies and procedures with respect to resetting VFA contractor representatives' passwords, terminating web sessions in its proprietary gateway system for VFA contractor representatives, identifying higher-risk representatives and customer accounts for additional security measures, and creation and alteration of Voya.com customer profiles, were not reasonably designed. In addition, a number of VFA's cybersecurity policies and procedures were not reasonably designed to be applied to its contractor representatives.

8. The Identity Theft Red Flags Rule requires certain financial institutions and creditors, including broker-dealers and investment advisers registered or required to be registered with the Commission, to develop and implement a written Identity Theft Prevention Program that is designed to detect, prevent, and mitigate identity theft[2] in connection with the opening of a covered account or any existing covered account.[3] An Identity Theft Prevention Program must include reasonable policies and procedures to: identify relevant red flags for the covered accounts and incorporate them into the Identity Theft Prevention Program; detect the red flags that have been incorporated into the Identity Theft Prevention Program; respond appropriately to

[2] The rule defines "identity theft" as a fraud committed or attempted using the identifying information of another person without authority. *See* 17 C.F.R. § 248.201(b)(9).

[3] The rule defines a "covered account" to include an account that a broker-dealer or investment adviser offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a brokerage account with a broker-dealer. *See* 17 C.F.R. § 248.201(b)(3).

any red flags that are detected pursuant to the Identity Theft Prevention Program; and ensure that the Identity Theft Prevention Program is updated periodically to reflect changes in risks to customers from identity theft.

9. Although VFA adopted a written Identity Theft Prevention Program in 2009, VFA violated the Identity Theft Red Flags Rule because it did not review and update the Identity Theft Prevention Program in response to changes in risks to its customers or provide adequate training to its employees. In addition, the Identity Theft Prevention Program did not include reasonable policies and procedures to respond to identity theft red flags, such as those that were detected by VFA during the April 2016 intrusion.

Respondent

10. VFA is a Minnesota corporation headquartered in Des Moines, Iowa, and dually registered as a broker-dealer and investment adviser with the Commission. VFA has approximately 13 million customers and approximately $11 billion in regulatory assets under management. It is an indirect wholly-owned subsidiary of Voya.

Background

11. VFA offers a wide range of proprietary and non-proprietary investment products and services through a national network of independent contractor registered representatives. VFA has over 1,000 employees, including registered representatives, who work in its home and branch offices, as well as 3,800 other associated persons, including contractor representatives who work out of their own offices in approximately 1,200 locations throughout the United States. The contractor representatives make up the largest part of VFA's workforce and provide brokerage and investment advisory services to VFA's customers. In the course of providing these services, VFA contractor representatives regularly collect and access account information for VFA customers that contains PII.

12. During the relevant period, while VFA employees generally used information technology ("IT") equipment and IT systems provided by Voya, VFA contractor representatives generally used their own IT equipment and operated over their own networks.

13. During the relevant period, VFA contractor representatives typically accessed VFA customer information through a proprietary web portal called Voya for Professionals or VPro. By entering login credentials consisting of a username and password into VPro, the contractor representatives gained access to a number of web applications, including third-party applications such as SmartWorks, which is a customer and prospect relationship management system that contained PII and account information for VFA customers and prospects, and a customer account management system that enabled VFA employees and contractor representatives to, among other things, execute trades and initiate cash distributions.

VFA's Policies and Procedures Prior to the Intrusion Were Deficient

14. VFA had no cybersecurity staff of its own and outsourced most of its

cybersecurity functions and some of its information technology functions to its parent company, Voya. Voya staff also serviced support call centers for VFA's customers and contractor representatives. Voya's Financial Application Support Team ("FAST") was responsible for responding to VFA contractor representatives' requests for assistance with respect to VPro and SmartWorks, among other systems.

15. Prior to the intrusion, over a dozen Voya policies and procedures relating to cybersecurity were supposed to govern the conduct of VFA. Among other things, these policies and procedures required: (a) manual account lock-outs for a user suspected of being involved in a security incident from web applications containing critical data, including customer PII; (b) a session timeout after 15 minutes of user inactivity in web applications containing customer PII; (c) a prohibition of concurrent web sessions by a single user in web applications containing customer PII; (d) multi-factor authentication ("MFA")[4] for access to applications containing customer PII; (e) annual and ad-hoc review of cybersecurity policies; and (f) cybersecurity awareness training and updates for VFA employees and contractors.

16. VFA implemented these policies and procedures for the systems used by its associated persons that it classified as employees, including when those associated persons worked remotely.

17. Even though these policies and procedures were applicable to VFA's associated persons that it classified as independent contractors, including those working out of remote offices, these policies and procedures were not reasonably designed to apply to the systems they used. For example, VFA allowed its contractor representatives to maintain concurrent VPro sessions and did not apply 15-minute inactivity timeouts[5] to VPro sessions. In addition, VFA did not have a procedure for terminating an individual VFA contractor representative's remote session. Further, VFA contractor representatives' web access to VPro was subject to MFA that required the user to answer previously-set security questions when a new device was connecting to the relevant VPro account. This form of MFA was rendered ineffective when users called the FAST team to request a reset of VPro passwords and FAST staff reset the security questions, which was what happened during the intrusion.

18. The password reset procedures for VPro allowed FAST staff to provide users who could not remember their passwords with a temporary password by phone, after the user provided at least two pieces of his or her PII. Temporary passwords were not required to be sent via secure email. Although these procedures did not authorize FAST staff to provide VPro usernames (in addition to passwords) to these users, the procedures did not explicitly prohibit it. These procedures remained in place at the time of the intrusion even though VFA was aware of prior

[4] MFA requires at least one factor in addition to username and password for login authentication. The additional factor is commonly a token, randomly-generated by an app on the user's mobile device or sent to the user via SMS/text to a pre-registered phone number. VFA used such token-based MFA for its employees, but a different, less secure form of MFA (discussed in the text) for contractor representatives.

[5] The VPro inactivity timeout was set to 60 minutes. VPro was exempted from the 15-minute timeout requirement without formal documentation.

fraudulent activity at Voya that involved attempts to impersonate its contractor representatives using their PII in calls to technical and customer support lines.

19. Voya kept a "monitoring list" of phone numbers suspected of having been used in connection with prior fraudulent activity at Voya. However, there was no written policy or procedure that required FAST and customer support call centers to use this list when responding to requests for password resets or other calls from the phone numbers on this list. Although Voya adopted an informal, unwritten procedure providing for the next-business-day review of phone calls from numbers on the "monitoring list" in January 2016, that procedure did not prevent someone from fraudulently obtaining access to confidential customer information at the time that the call was occurring, and the procedure was not consistently applied.

20. The contractor representatives' personal computers were supposed to be scanned for the existence of antivirus software, encryption, and certain software updates, but these scans were scheduled to occur only three times per year, and representatives often failed to take the actions that were necessary for the scans to occur. A third-party service provider scanned VFA contractor representatives' computers after a representative clicked a link sent by the service provider via email. However, some representatives failed to click the link for extended periods of time, if at all. Among the computers that were scanned, the fail rate in each of 2015 and 2016 was approximately 30%, with half of those exhibiting critical failures, such as lack of encryption and antivirus software. VFA conducted no review or follow-up on failures of representatives to scan their computers or on the scans that identified security deficiencies.

21. The policies and procedures for protecting VFA customers' Voya.com profiles, which included the customers' personal and account information and provided users with the ability to change email and physical addresses of record as well as to document delivery preferences, were not reasonably designed. VFA did not provide notice to a customer when an initial profile was created for that customer and when contact information and document delivery preferences were changed for that customer. As a result, intruders could create and change customer profiles without customer detection, and they did so during the April 2016 attack.

22. VFA's policies and procedures to respond to a breach and mitigate identity theft in connection with an intrusion into VPro and SmartWorks were also not reasonably designed. They largely consisted of Voya's incident response procedures, which were not reasonably designed to deny or limit an unauthorized person's access to VFA customers' PII. For example, although incident response procedures required in general terms that potentially compromised user accounts be disabled or the relevant applications be shut down to prevent additional compromise, VFA's policies and procedures were not reasonably designed to accomplish these directives. Specifically, Voya IT security staff, who were responsible for responding to security incidents, were not provided with adequate training regarding the operation of VPro and erroneously believed that resetting a VPro password for a user would terminate that user's existing sessions. In fact, resetting VPro passwords did not terminate sessions, and existing sessions continued to proceed after password resets. VFA's incident response procedures also failed to ensure that the FAST and customer-facing call center staff were notified about an ongoing intrusion.

23. VFA's policies and procedures for designating compromised representatives' and

customers' accounts for additional security measures during calls to support centers for VFA contractor representatives and customers they serviced were not reasonably designed. Although in January 2016, VFA informally adopted a procedure to place flags on such contractor representatives and customer accounts in the system, unbeknownst to the relevant security staff, such flags were erased from the system periodically in connection with unrelated automated system activities.

24. In 2009, before the Dodd-Frank Act of 2010 transferred to the Commission the rulemaking responsibility and enforcement authority under Section 615(e) of the Fair Credit Reporting Act with respect to the entities subject to its enforcement authority, VFA adopted an Identity Theft Prevention Program to comply with the then-applicable Red Flags Rule of the Federal Trade Commission (16 C.F.R. § 681.1). VFA's Identity Theft Prevention Program required VFA to oversee the implementation and administration of the Identity Theft Prevention Program, to train its staff on the Identity Theft Prevention Program, and to have in place policies and procedures to periodically update the Identity Theft Prevention Program in response to changes in risks to VFA's customers.

25. Despite significant changes in external cybersecurity risks[6] and in VFA's own risk profile, VFA did not substantively update the Identity Theft Prevention Program after 2009 and VFA's board of directors or a designated member of VFA's management did not administer and oversee the Identity Theft Prevention Program, as required by the Identity Theft Red Flags Rule. As a result, VFA's cyber incident response procedures were not reasonably designed to respond to identity theft red flags, such as those that were detected by Voya's staff prior to and during the April 2016 intrusion. For example, once VFA discovered that intruders had obtained access to the VPro system and customer PII, VFA did not have reasonable procedures to change security codes, employ other security devices, or modify existing procedures in order to deny unauthorized persons' access to VFA customer accounts. In addition, VFA failed to conduct training specific to the Identity Theft Prevention Program.[7]

The Intrusion and VFA's Response

26. On April 13, 14, and 18, 2016, one or more persons impersonating VFA contractor representatives subjected VFA to an intrusion that proceeded in several phases. In the course of this attack, the intruders exploited the weaknesses in VFA's cybersecurity policies and Identity

---

[6] *See, e.g.*, *Identity Theft Red Flags Rules*, Release No. 34-69359 (Apr. 10, 2013) ("Advancements in technology also have led to increasing threats to the integrity and privacy of personal information.") (footnote omitted).

[7] Although certain training sessions conducted by VFA touched on the topic of identity theft, primarily in the insurance business context, those training sessions did not focus on the Identity Theft Prevention Program. In addition, those training sessions were sparsely attended, with only 3 VFA employees attending the 2015 training and only 5 VFA employees attending the 2016 training. Similarly, VFA's contractor representatives received annual compliance training that touched on a specific 2014 hacking incident, but did not cover the Identity Theft Prevention Program, and was not attended by all VFA representatives and compliance and IT security staff. For example, two of the representatives whose passwords were fraudulently reset during the intrusion did not complete the 2016 compliance training.

Theft Prevention Program outlined above. Prior to the intrusion, between January and March 2016, VFA had been subject to other fraudulent activity in which unknown persons impersonated VFA representatives, including one of the representatives targeted in April 2016, sometimes using the same phone numbers and techniques as those used in the April 2016 intrusion.

27. Each of the three days began with a phone call to the FAST team, which was responsible for supporting VPro and SmartWorks. Two of the calls came from a phone number suspected of having been used in prior fraudulent activity at Voya. On each day, a caller impersonated a different VFA contractor representative, provided two forms of the representative's PII, and requested a reset of that contractor representative's VPro password. One of the representatives had been targeted during the prior fraudulent activity. On each occasion, FAST staff reset the password and provided a temporary password to the caller by phone. In two instances, FAST staff also provided the VFA contractor representative's VPro username to the caller. On each of the three days, the intruders used the contractor representative's VPro login credentials to access SmartWorks remotely. The intruders' sessions were not terminated when the authorized users initiated new sessions, and their sessions were not timed out after several periods of inactivity of 15 minutes or longer.

28. Upon accessing SmartWorks, the intruders had access to PII of approximately 5,600 VFA customers, including address, date of birth, last four digits of the Social Security number, and email address. For at least 2,000 of these customers, the intruders viewed a full Social Security number and/or another government-issued identification number. The intruders also edited and ran reports containing customer information in SmartWorks. For all affected customers who held annuity contracts, the intruders had the ability to copy the unique contract numbers, which Voya customer service used as an identity authenticating factor during customer service calls. Through VPro, the intruders also had the ability to, but apparently did not, access a platform that VFA representatives and employees used to manage customer accounts, including to initiate distribution requests and execute trades.

29. Upon receipt of an email notification of password change, the first contractor representative notified FAST in the late morning of April 13, 2016 that he had not requested the change. The FAST member then reset that representative's VPro password and escalated the incident to a FAST manager, who reported it to Voya's security incident response team. The FAST manager emailed the entire FAST team the following morning, formally notifying the team of the incident and directing staffers not to provide usernames and temporary passwords by phone. However, in the intervening period, the intruders had obtained the second contractor representative's username, reset his password and gained access to SmartWorks. Moreover, the FAST manager's directive that no passwords be provided by phone and that the phone number monitoring list should be reviewed was not heeded on April 18, 2016, when a FAST team member provided a password to an intruder impersonating a third representative.

30. On the second day of the intrusion, Voya's security staff, which was charged with responding to the breach, identified certain IP addresses as likely involved in the intrusion. However, they failed to block these IP addresses or freeze the compromised representatives' SmartWorks sessions while the malicious sessions were in progress in part based on their mistaken belief that resetting the compromised VPro passwords would terminate these sessions. The

intruders continued to have access to the PII of VFA customers for most of the day on the first two days of the intrusion and for more than two hours on the last day, until the intruders exited VFA's systems.

31. After the first contractor representative notified VFA of the fraudulent reset of his password, Voya's annuity customer service call center received five telephone calls from unknown callers impersonating one of that representative's customers and three calls from unknown callers impersonating the representative himself. These calls came in from four different phone numbers, which in six instances had area codes outside of the customer's and the representative's state of residence. Several of the calls came in from a number on the "monitoring list."[8] The callers obtained account-level information from technical support, changed the customer's email address of record to a "@yopmail.com" email address, and caused VFA to send certain of the customer's account documents to that address.[9]

32. The intruders made other attempts to obtain customer-specific account information during the intrusion, and were successful in obtaining account documents for two additional VFA customers by establishing online Voya.com profiles, which provided them access to, among other things, account balances, account documents, tax documents, and other account information. Using these Voya.com profiles, the intruders changed the customers' email addresses of record to disposable email addresses (such as @yopmail.com and @sharklasers.com), changed phone numbers of record, and changed the delivery method for statements and account confirmations to online and email, rather than by mail.

33. During the intrusion, Voya conducted testing of other contractor representatives' password resets in an effort to identify the scope of the intrusion and mitigate its impact in case other representatives were affected. This testing involved contacting the relevant representatives and inquiring whether they initiated the password resets. However, this testing was done only on the passwords reset between April 1 and 14, 2016, which included only the first half of the intrusion. There was no testing of passwords that were reset during the back half of the intrusion (April 15 through 18, 2016). In addition, 41% of the resets tested resulted in an "unable to reach" finding, and six of these resets occurred during the intrusion. There was no follow-up to these failures to reach the representatives whose passwords were reset during the intrusion.

34. After the intruders voluntarily left VFA's networks, VFA blocked two malicious IP addresses using its IPS/IDS systems. The intruders thereafter continued attempting to obtain distributions and information from the compromised accounts by contacting Voya's customer

---

[8] Despite a variety of indications of potential fraud during these eight calls, only one customer support representative escalated a call for suspicion of fraud. After he described the circumstances he found to be suspicious (garbled connection, suspicious voice, and questions about what was the last document VFA received, how to change the beneficiary, and wire transfers), he was nonetheless given approval to service the caller's request to send a copy of the customer's contract to the caller.

[9] Yopmail.com is a disposable email service that allows users to create an email address, review incoming emails, and destroy all content thereafter.

support call centers, as well other financial institutions, although no unauthorized transfers of funds or securities from VFA customer accounts are known to have occurred as a result of the attack.

Violations

35. As a result of the conduct described above, VFA willfully[10] violated Rule 30(a) of Regulation S-P (17 C.F.R. § 248.30(a)), 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.

36. As a result of the conduct described above, VFA willfully violated Rule 201 of Regulation S-ID (17 C.F.R. § 248.201), which requires registered broker-dealers and investment advisers that offer or maintain covered accounts to develop and implement a written Identity Theft Prevention Program that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account.

VFA's Remedial Efforts

37. After the intrusion, VFA promptly undertook certain remedial acts, including: (a) blocking the malicious IP addresses; (b) revising its user authentication policy to prohibit provision of a temporary password by phone; (c) issuing breach notices to the affected customers, describing the intrusion and offering one year of free credit monitoring; and (d) implementing effective MFA for VPro.

38. Furthermore, on August 28, 2017, VFA named a new Chief Information Security Officer, who is responsible for creating and maintaining cybersecurity policies and procedures and an incident response plan tailored to VFA's business.

39. In determining to accept the Offer, the Commission considered the remedial acts undertaken by VFA.

Undertakings

40. Respondent has undertaken the following:

a. Retention of Compliance Consultant. Respondent shall retain, at its expense, an independent compliance consultant (the "Consultant") to conduct a comprehensive review of Respondent's policies and procedures for compliance with Regulation S-P and Regulation S-ID.

[10] A willful violation of the securities laws means merely "'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.'" *Id.* (quoting *Gearhart & Otis, Inc. v. SEC*, 348 F.2d 798, 803 (D.C. Cir. 1965)).

b. Respondent shall require the Consultant to enter into an agreement that provides that for the period of engagement and for a period of two years from completion of the engagement, the Consultant shall not enter into any employment, consultant, attorney-client, auditing or other professional relationship with Respondent, or any of its present or former affiliates, directors, officers, employees, or agents acting in their capacity. The agreement will also provide that the Consultant will require that any firm with which he/she is affiliated or of which he/she is a member, and any person engaged to assist the Consultant in performance of his/her duties under this Order shall not, without prior written consent of the Commission staff, enter into any employment, consultant, attorney-client, auditing or other professional relationship with Respondent, or any of its present or former affiliates, directors, officers, employees, or agents acting in their capacity as such for the period of the engagement and for a period of two years after the engagement.

c. Respondent shall cooperate fully with the Consultant.

d. Within three months after the date of the issuance of this Order, Respondent shall require the Consultant to submit a written Initial Report to Respondent and to the Commission staff. The Initial Report shall describe the review performed, the conclusions reached, and shall include any recommendations deemed necessary to make the policies and procedures and their implementation comply with applicable requirements.

e. Respondent shall adopt all recommendations contained in the Initial Report within 90 days of the date of its issuance, provided, however, that within 30 days of the issuance of the Initial Report, Respondent shall advise, in writing, the Consultant and the Commission staff of any recommendations that Respondent considers to be unduly burdensome, impractical or inappropriate. With respect to any such recommendation, Respondent need not adopt that recommendation at that time but shall propose in writing an alternative policy, procedures or system designed to achieve the same objective or purpose. As to any recommendation on which Respondent and the Consultant do not agree, Respondent and the Consultant shall attempt in good faith to reach an agreement within 60 days after the issuance of the Initial Report. Within 15 days after the conclusion of the discussion and evaluation by Respondent and the Consultant, Respondent shall require that the Consultant inform Respondent and the Commission staff in writing of the Consultant's final determination concerning any recommendation that Respondent considers to be unduly burdensome, impractical, or inappropriate. Within 10 days of this written communication from Consultant, Respondent may seek approval from the Commission staff to not adopt recommendations that Respondent can demonstrate to be unduly burdensome, impractical, or

inappropriate. Should the Commission staff agree that any proposed recommendations are unduly burdensome, impractical, or inappropriate, Respondent may adopt its proposed alternative policy, procedures or systems designed to achieve the same objective or purpose.

f. Within nine months after the date of issuance of this Order, Respondent shall require the Consultant to complete its review and issue a written Final Report to Respondent and the Commission staff. The Final Report shall describe the review performed, the conclusions reached, the recommendations made by the Consultant, any recommendations not adopted by Respondent pursuant to Paragraph 40(e), any proposals made by Respondent, any alternative policies, procedures or systems adopted by Respondent pursuant to Paragraph 40(e), and how Respondent is implementing the Consultant's final recommendations.

g. Respondent shall take all necessary and appropriate steps to implement all recommendations and alternative policies, procedures or systems adopted by Respondent pursuant to Paragraph 40(e) above, to the extent it has not already done so.

h. For good cause shown and upon timely application by the Consultant or Respondent, the Commission's staff may extend any of the deadlines set forth in these undertakings.

41. Respondent shall certify, in writing, compliance with the undertaking(s) set forth above. The certification shall identify the undertaking(s), provide written evidence of compliance in the form of a narrative, and be supported by exhibits sufficient to demonstrate compliance. The Commission staff may make reasonable requests for further evidence of compliance, and Respondent agrees to provide such evidence. The certification and supporting material shall be submitted to Paul Montoya, with a copy to the Office of Chief Counsel of the Enforcement Division, no later than sixty days from the date of the completion of the undertakings.

IV.

In view of the foregoing, the Commission deems it appropriate and in the public interest to impose the sanctions agreed to in VFA's 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. VFA 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)) and of Rule 201 of Regulation S-ID (17 C.F.R. § 248.201);

B. VFA is censured; and

C. VFA shall pay, within 10 (ten) business days of the entry of this Order, a civil money penalty in the amount of $1,000,000 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) VFA may transmit payment electronically to the Commission, which will provide detailed ACH transfer/Fedwire instructions upon request;

(2) VFA 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) VFA 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 VFA 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: Paul Montoya, Assistant Regional Director, Division of Enforcement, Chicago Regional Office, Securities and Exchange Commission, 175 W. Jackson Blvd., Suite 1450, Chicago, Illinois, 60604.

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.

E. Respondent shall comply with its undertakings as enumerated in Paragraphs 40 and 41 above.

By the Commission.

Brent J. Fields
Secretary