COMMONWEALTH OF MASSACHUSETTS
OFFICE OF THE SECRETARY OF THE COMMONWEALTH
SECURITIES DIVISION
ONE ASHBURTON PLACE, ROOM 1701
BOSTON, MASSACHUSETTS 02108

IN THE MATTER OF:)
)
SUMMIT EQUITIES, INC.) Docket No. R-2018-0083
)
RESPONDENT.)
)

CONSENT ORDER

This Consent Order (the "Order") is entered into by the Massachusetts Securities Division of the Office of the Secretary of the Commonwealth (the "Division") and Summit Equities, Inc. ("Summit" or "Respondent") arising out of an ongoing investigation by the Registration, Inspections, Compliance and Examinations Section (the "RICE Section") of the Division into whether Summit's Agents' use and potential sharing of Summit customers' personal identifiable information ("PII"), Summit's supervision of its Agents' use and potential sharing of customers' PII, and the steps taken by Summit to protect its customers' PII from being shared with or accessed by unaffiliated third parties, violated MASS. GEN. LAWS ch. 110A, the Massachusetts Uniform Securities Act (the "Act") and the corresponding regulations promulgated thereunder at 950 MASS. CODE REGS. 10.00, *et seq*. (the "Regulations").

On December 21, 2018, Summit submitted an Offer of Settlement (the "Offer") to the Division. Solely for the purpose of this matter's resolution, Respondent admits the Statement of Facts set forth in Section IV, admits the Violation of Law set forth in Section V, and consents to the entry of this Order by the Division, consistent with the language and terms of the Offer, settling the claims brought hereby with prejudice.

I. JURISDICTION AND AUTHORITY

1. As provided for by the Act, the Division has jurisdiction over matters relating to securities pursuant to Chapter 110A of the Massachusetts General Laws.

2. The RICE Section brings this action pursuant to the authority conferred upon the Division by Sections 204 and 407A of the Act, wherein the Division has the authority to conduct an adjudicatory proceeding to enforce the provisions of the Act and the Regulations.

3. This Offer is made in accordance with MASS. GEN. LAWS ch. 110A. Specifically, Respondent has been registered as a broker-dealer in Massachusetts since August 15, 1984.

II. RELEVANT TIME PERIOD

4. Except as otherwise expressly stated, the conduct described herein occurred during the approximate time period of January 1, 2013 to February 1, 2018 (the "Relevant Time Period").

III. RESPONDENT

5. Summit Equities, Inc., ("Summit") is a broker-dealer with headquarters in New Jersey. Summit has a FINRA Central Registration Depository ("CRD") number of 11039. Summit has been registered in Massachusetts since August 15, 1984.

IV. STATEMENT OF FACTS

6. Individual 1 is a former Agent of Summit with a residential address in New Jersey and a FINRA CRD number of 4636157. Individual 1 was registered with Summit from February 14, 2003, and registered in Massachusetts as an Agent of Summit from January 24, 2017, until his discharge on January 12, 2018.

7. Individual 2 is a former Agent of Summit with a residential address in New Jersey and a FINRA CRD number of 2143630. Individual 2 was registered with Summit from April 14, 2003, and registered in Massachusetts as an Agent of Summit from January 24, 2017 until January 16, 2018.

8. Individual 3 is a former Agent of Summit with a residential address in New York and a FINRA CRD number of 2249803. Individual 3 was registered with Summit from July 5, 2005 until January 24, 2018. Individual 3 was registered in Massachusetts as an Agent of Summit from July 5, 2005 to December 31, 2005, and from January 2, 2015 until February 21, 2018.

9. Individual 4 is a former Agent of Summit with a residential address in New York and a FINRA CRD number of 4977264. Individual 4 was registered with Summit from June 9, 2005, and registered in Massachusetts as an Agent of Summit from February 29, 2008 until February 8, 2018.

10. Individual 5 worked as a non-registered sales assistant to Individual 1 and Individual 2 from December 13, 2017 until January 16, 2018. Her FINRA CRD number is 6889318.

A. **Summit Implemented Policies And Procedures Designed To Protect The Security Of And Prevent Unauthorized Access To Customers' PII.**

11. Summit's Written Information Security Policy titled Privacy, Data Security, Identity Theft Protection and Associated Policies, as it was in effect prior to February 2018

(the "Privacy & Security Policy"), detailed how customers' confidential personal identifying information ("PII") should be handled, accessed, stored, disclosed, and destroyed.

12. The Privacy & Security Policy was designed, in part, to aid Summit in developing programs to protect customer information and guard against its misuse.

13. The Privacy & Security Policy stated that "Summit uses the term 'Personal Information' to refer specifically to information that is protected under the relevant state data security statute.... As used in Summit's procedures, PII includes Personal Information, but Personal Information does not necessarily include all PII."

14. Under Massachusetts law, Personal Information is defined as a Massachusetts resident's first name and last name or first initial and last name in combination with an additional data element, including the resident's social security number, driver's license number, financial account number, or credit or debit card number.[1]

15. The Privacy & Security Policy stated, among other things, that "[t]he Firm will strive to: (a) ensure the security and confidentiality of the information; (b) protect against anticipated threats and hazards to the security and integrity of the information; and (c) protect against unauthorized access to, or improper use of, the information."

16. The Privacy & Security Policy prohibited all Summit independent contractors and employees from disclosing customers' PII to third parties without the customer's consent, except under circumstances where it is necessary to effect or administer a transaction authorized by the customer; disclosed to certain parties in furtherance of managing the customer's assets and with the customer's express permission; disclosed to certain Summit service providers that keep customer PII confidential; or required by law.

[1] *See* 201 MASS. CODE REGS. 17.02.

17. Pursuant to Summit's obligations under the SEC's Regulation S-P to take measures to safeguard Summit customers' PII from being accessed or misused by unauthorized third parties, the Privacy & Security Policy required all Summit independent contractors and employees departing the firm for any reason to return and not retain copies of all records and files in their possession containing Summit customers' PII. Specifically, the Privacy & Security Policy stated as follows at Section I(C)(a)(iii)(7):

> All Employees are required, upon request by [any officer of Summit], and upon termination or resignation for any reason, to return and not retain any copies of any and all records and files containing information classified as PII, in any form that may at the time of such termination be in their possession or control, including all such information stored on laptops, handheld computers (*e.g.*, Windows Mobile, iOS or Android-based devices), blackberries, smart phones, tablets and other portable devices (such devices, "Portable Devices") or other media, or in files, records, notes, or papers.

18. Summit required its independent contractors and employees to complete various forms of training including annual compliance meeting, online courses, and annual attestation acknowledging the independent contractor's or employee's understanding of Summit's policies and procedures.

B. Summit Did Not Reasonably Supervise Its Agents' Use And Potential Sharing Of Summit Customers' PII.

i. Summit Permitted Its Agents To Use Third-Party CRM Systems Over Which Summit Did Not Have Access Or Control.

19. During the Relevant Time Period, Summit permitted its Agents to maintain, under the Agents' exclusive possession and control, electronic systems for the management of customer or client data, commonly referred to as Contact- or Customer Relationship Management Systems ("CRM").

20. Summit Agents inputted and stored private customer information, including PII, in the Agents' own third-party CRM system, over which Summit had no access or control.

21. Summit's Agents were able to input data points about Summit's customers to their third-party CRM systems such as a customer's name, address, phone numbers, date of birth, social security number, relationships, account and insurance details, notes about the customer and relationship, tasks, and activity history.

ii. <u>Summit Was Or Became Aware That Its Agents Were Using And Inputting Summit Customers' PII Into A Third-Party CRM System.</u>

22. During the Relevant Time Period, Summit was aware or became aware that at least some of its Agents used a third-party CRM system offered by Redtail Technology Inc. ("Redtail"), called Tailwag.

23. Tailwag is a web-based CRM system designed for financial professionals, which allows users to log in and access stored information from any computer, tablet, or device with internet access.

24. During their association with Summit, Individual 1 and Individual 2 shared a Tailwag system under the control of Individual 1, and Individual 3 and Individual 4 each used their own Tailwag system.

25. Individual 1, Individual 2, Individual 3, and Individual 4 input Summit customer information into their Tailwag systems including, but not limited to, customer names, addresses, contact information, dates of birth, social security numbers, account details, insurance details, e-mail exchanges with customers, and customer relationship notes.

iii. Summit Did Not Have Access To Individual 1's, Individual 2's, Individual 3's, Or Individual 4's Respective Third-Party CRM Systems.

26. The Privacy & Security Policy did not provide for Summit to gain access to Agents' third-party CRM systems.

27. The Privacy & Security Policy did not provide for Summit to review what customer information was put into Agents' third-party CRM systems.

28. The Privacy & Security Policy did not provide for Summit to monitor the storage or use of the customer information put into Agents' third-party CRM systems.

29. Neither Summit nor Individual 1's direct supervisor was an authorized user on Individual 1's Tailwag system

30. Neither Summit nor Individual 2's direct supervisor was an authorized user on Individual 1's Tailwag system.

31. Neither Summit nor Individual 3's direct supervisor was an authorized user on Individual 3's Tailwag system.

32. Neither Summit nor Individual 4's direct supervisor was an authorized user on Individual 4's Tailwag system.

33. Summit did not have access to or gain control over Individual 1's, Individual 2's, Individual 3's, and Individual 4's Tailwag systems in any manner.

iv. As A Result Of Not Having Access To Individual 1's, Individual 2's, Individual 3's, Or Individual 4's Tailwag Systems, Summit Was Not Able to Monitor Or Control The Users Of Each Tailwag System In Order To Prevent Access By Or Sharing With Unauthorized Persons.

34. Summit's inability to access its Agents' third-party CRM systems prevented Summit from being able to monitor any other users who had access to the third-party CRM systems.

35. Summit did not monitor or control the list of authorized users on Individual 1's, Individual 2's, Individual 3's, and Individual 4's respective Tailwag systems.

36. On December 9, 2017, Individual 1 created a user account on his Tailwag system for Individual 5.

37. Individual 5's user account logged into Individual 1's Tailwag system approximately twelve (12) times on December 9, 2017.

38. As of December 9, 2017, Individual 5 was not an employee or independent contractor of Summit.

39. As a result of not having access to Individual 1's Tailwag system, Summit could not monitor or control Individual 5's access to Summit customers' PII.

v. As A Result Of Not Having Access To Individual 1's, Individual 2's, Individual 3's, Or Individual 4's Tailwag Systems, Summit Was Not Able to Monitor Or Control The Information that Agents Input Into The Tailwag Systems To Prevent Unauthorized Sharing Of Summit Customers' PII.

40. Summit's inability to access its Agents' third-party CRM systems prevented Summit from being able to monitor the types of customer information that Agents input into the third-party CRM system and the potential unauthorized sharing of that information.

41. In the week prior to Individual 1's departure from Summit, Individual 5 viewed or hid customer social security numbers on Individual 1's Tailwag system one hundred and thirteen (113) times between January 8, 2018 and January 12, 2018.

42. During the month of January 2018, Individual 5 and Individual 1 downloaded files, exported certain contacts, and printed calendars from Individual 1's Tailwag system.

43. During the month of January 2018, Individual 3 and his assistant exported information that had been input into Individual 3's Tailwag system.

44. Between January 2, 2018 and January 12, 2018, Individual 4 viewed or hid customer social security numbers on his Tailwag system one hundred and sixteen (116) times.

45. Summit's inability to access Individual 1's, Individual 2's, Individual 3's, and Individual 4's Tailwag systems prevented Summit from being able to monitor the type of customer information that Agents input into the Agents' respective Tailwag systems, as well as unauthorized sharing and potential dissemination of that information.

C. Summit Did Not Take Reasonable Steps To Ensure That Individual 1, Individual 2, Individual 3, and Individual 4 Complied With The Privacy & Security Policy Upon Their Respective Departures From Summit.

46. In effect, the Privacy & Security Policy prohibited Summit Agents from taking Summit customers' PII with them upon departing from Summit.

47. Summit could remotely wipe or disable the Agent's mobile devices, system access, and building access, and restore their computers to factory settings prior to returning them to the Agent, as needed.

48. Because Summit did not obtain access to its Agents' third-party CRM systems, Summit was unable to remotely wipe or otherwise remove its customers' PII within those CRM systems as needed.

49. Upon Individual 1's, Individual 2's, Individual 3's, and Individual 4's respective departures, Summit did not have the ability to ensure that its customers' PII was returned, destroyed, and not shared with or accessed by unauthorized persons by removing or wiping the information stored on their respective Tailwag systems.

50. When an Agent leaves Summit, it is Summit's practice for Summit or its attorneys to send letters ("Compliance Letters") to the former Agent and the Chief Compliance Officer ("CCO") of the former Agent's new firm demanding that the former Agent either

immediately return Summit customers' PII or certify that the Agent did not take Summit customers' PII.

51. On January 12, 2018, Summit terminated Individual 1's registration.

52. Upon termination, a remote wipe was sent to Individual 1's mobile devices, and his computers were returned to factory settings and given back to him. Summit immediately terminated Individual 1's registrations.

53. Upon termination, Summit could not and did not remotely wipe Individual 1's Tailwag system.

54. On January 22, 2018, Summit's attorney sent a Compliance Letter to Individual 1's new broker-dealer copying Individual 1, to "serve as notice that neither [the new broker-dealer], nor [Individual 1], may retain *or use* any nonpublic information protected under Regulation S-P."

55. On January 24, 2018, Individual 3 voluntarily terminated his registration from Summit.

56. Upon termination, a remote wipe was sent to Individual 3's mobile devices, and his computers were returned to factory settings and given back to him.

57. Upon termination, Summit could not and did not remotely wipe Individual 3's Tailwag system.

58. On February 4, 2018, Summit's attorney sent Compliance Letters to the CCO of Individual 3's new broker-dealer and Individual 3 requiring that Individual 3 "[...] return all PII you have in your possession and certify that you have deleted all electronic copies of such information [...] [and] you certify that you have not disclosed or used any such PII."

59. Summit did not receive responses to the Compliance Letters it sent to Individual 1 and Individual 3.

60. On January 16, 2018, and February 8, 2018, respectively, Individual 2 and Individual 4 terminated their registrations from Summit.

61. Upon termination, a remote wipe was sent to Individual 2's and Individual 4's mobile devices, and Individual 2's computers were returned to factory settings and given back to him.

62. Upon termination, Summit could not and did not remotely wipe Individual 4's Tailwag system.

63. Summit did not send Compliance Letters to Individual 2 or Individual 4 to determine whether either former Agent took Summit customers' PII.

64. Prior to or during the period when Individual 1, Individual 2, Individual 3, and Individual 4 departed from Summit, Summit did not ensure that all of its customers' PII was maintained within Summit, returned to Summit, or destroyed.

65. Summit did not take reasonable steps to ensure the security and confidentiality of its customers' PII.

66. When Individual 1, Individual 2, Individual 3, and Individual 4 departed from Summit, they took their Tailwag systems with them including Summit customer names, addresses, contact information, dates of birth, and financial account numbers.

67. As a result of Summit's noncompliance with its own Privacy & Security Policy, Summit customers' PII was removed from Summit and shared with or accessed by at least one unauthorized third party without the customers' prior consent.

V. VIOLATION OF LAW

A. Violation of MASS. GEN. LAWS ch. 110A, § 204(a)(2)(J)

68. MASS. GEN. LAWS ch. 110A, § 204(a)(2)(J) provides, in pertinent part:

> The secretary may by order deny, suspend, or revoke any registration if he finds (1) that the order is in the public interest and (2) that the applicant or registrant[:]
>
> (J) has failed reasonably to supervise agents, [...] or other employees to assure compliance with this chapter[.]

69. The RICE Section realleges and incorporates the allegations of paragraphs 1 through 67 above.

70. The conduct of Respondent, as described above, constitutes a violation of MASS. GEN. LAWS ch. 110A, § 204(a)(2)(J).

VI. ORDER

Summit consents to the entry of this Order,

IT IS HEREBY ORDERED THAT:

Summit, in full settlement of these matters, admits the Statement of Facts set forth in Section IV, admits the Violation of Law set forth in Section V, makes the following representations, and agrees to the undertaking herein as part of this Order:

A. Respondent shall permanently cease and desist from violations of the Act and Regulations in the Commonwealth.

B. Respondent shall certify the steps it took to prevent the Agents who left after the Relevant Time Period from retaining Summit customers' PII upon departure.

C. Respondent shall notify all of its Massachusetts customers potentially impacted by the wrongdoing described above that their PII may have been shared with or accessed by unaffiliated parties without their prior consent. For the purpose of this provision, a customer is "potentially impacted" if (1) any of the customer's accounts was serviced by an Agent who left Summit between January 1, 2013 to present, (2) the Agent serviced the account(s) at the time the Agent left Summit, and (3) as of the time the Agent left the firm, the Agent used any third-party CRM system.

D. Within ten (10) business days of the date of this Order, Respondent shall provide the Division a written report identifying all Agents who have left Summit between January 1, 2018 and the date of entry of this Order. The report shall include each Agent's (1) full name, (2) CRD number, (3) the date on which the Agent left Summit, (4) whether the Agent used a third-party CRM system as of the date the Agent left Summit, and (5) a detailed description of all measures taken by Summit to ensure that the Agent returned and did not retain any records or materials, or copies thereof, containing Summit PII, pursuant to Summit's Privacy & Security Policy.

E. Within five (5) business days of the date of this Order, Respondent shall pay an administrative fine in the amount of one hundred thousand dollars ($100,000) to the Commonwealth of Massachusetts. Payment shall be: (1) made by United States postal money order, certified check, bank cashier's check, bank money order or wire transfer; (2) made payable to the Commonwealth of Massachusetts; and (3) either hand-delivered or mailed to One Ashburton Place, Room 1701, Boston, Massachusetts 02108 or wired per the Division's instructions; and (4) submitted under cover letter or other documentation that identifies Respondent making the payment and the docket number of the proceedings. Respondent shall also provide the Division with notice no later than twenty-four hours prior to the payment.

F. Respondent shall not claim, assert, or apply for a tax deduction or tax credit with regard to any state, federal, or local tax for any amounts that Respondent shall pay pursuant to this Order.

G. Respondent shall not seek or accept, directly or indirectly, reimbursement or indemnification, including, but not limited to, any payments made pursuant to any insurance policy, with regard to any amount that Respondent shall pay pursuant to this Order.

BY ORDER OF:
WILLIAM FRANCIS GALVIN
SECRETARY OF THE COMMONWEALTH

By: Diane Young-Spitzer
Diane Young-Spitzer
Acting Director & General Counsel
Massachusetts Securities Division
One Ashburton Place, Room 1701
Boston, MA 02108

Date: December 26, 2018