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

IN THE MATTER OF:	)	
FIDELITY BROKERAGE SERVICES LLC,	)	Docket No. E-2024-0373
RESPONDENT.	)	

CONSENT ORDER

I. PRELIMINARY STATEMENT

This Consent Order (the "Order") is entered into by the Securities Division of the Office of the Secretary of the Commonwealth of Massachusetts (the "Division") and Fidelity Brokerage Services LLC ("FBS," "Fidelity," or "Respondent"), with respect to an investigation by the Enforcement Section of the Securities Division (the "Enforcement Section") into whether Respondent's acts and practices constituted violations of the Massachusetts Uniform Securities Act, M.G.L. c. 110A (the "Act"), and the regulations promulgated thereunder at 950 CMR 10.00-14.413 (the "Regulations"). The Division concluded that Fidelity failed to enforce certain cybersecurity controls necessary to restrict unauthorized access by customers to images of documents associated with other customer accounts within an internal database and that as a result, an unidentified and unauthorized third party (the "Threat Actor") accessed and obtained images of documents bearing sensitive information, including personally identifiable information[1] ("PII") of approximately 77,000

[1] PII refers to "a resident's first name and last name or first initial and last name in combination with any 1 or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's

customers and individuals, including at least 2,768 Massachusetts customers and individuals, through a data breach occurring between August 17 and 19, 2024 (the "Data Breach").

On April 22, 2026, Respondent submitted an Offer of Settlement (the "Offer") to the Division. Respondent neither admits nor denies the Statement of Facts set forth in Section VI below, neither admits nor denies the Violations of Law set forth in Section VII below, and consents to the entry of this Order by the Division, consistent with the language and terms of the Offer, settling the investigation, INV-2024-0373, with prejudice. Pursuant to M.G.L. c. 110A, § 412(b), this Order "is necessary or appropriate in the public interest or for the protection of investors and consistent with the purposes fairly intended by the policy and provisions of [the Act]."

II. JURISDICTION AND AUTHORITY

1. The Division has jurisdiction over matters relating to securities pursuant to the Act and Regulations.

2. The Offer was made in accordance with the Act and Section 10.10 of the Regulations.

III. RELEVANT TIME PERIOD

3. Except as otherwise expressly stated, the acts and practices described herein occurred during the approximate time period of January 1, 2022 to August 31, 2024.

IV. RESPONDENT

4. Fidelity Brokerage Services LLC ("FBS," "Fidelity," or "Respondent") is a limited

license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that [PII] shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public." M.G.L. c. 93H, § 1. Statutory definitions of personally identifiable information in other jurisdictions vary.

liability company organized under the laws of Delaware with a principal office located at 245 Summer Street, Boston, MA 02210. Massachusetts approved FBS's registration as a broker-dealer on July 31, 1981. FBS maintains a Central Registration Depository ("CRD") number of 7784.

V. RELATED PERSON

5. National Financial Services LLC ("NFS") is a limited liability company organized under the laws of Delaware with a principal office located at 245 Summer Street, Boston, MA 02110. Massachusetts approved NFS's registration as a broker-dealer on February 1, 1983. NFS maintains a CRD number of 13041. NFS served as custodian for certain customers also impacted by the Data Breach.

VI. STATEMENT OF FACTS

A. Fidelity Did Not Protect Against Unauthorized Access to Certain Customer Account Records.

6. Fidelity developed a system intended to allow customers to obtain images of certain documents associated with the customer using Fidelity's website.

7. The Threat Actor ultimately used this system to obtain images of documents containing PII or other sensitive customer information from an internal database (the "Document Image Repository").

8. The Threat Actor obtained images of documents that included one or more of the following: (1) Social Security numbers; (2) financial account numbers; (3) passport numbers; (4) driver's license numbers; (5) state-issued identification card numbers; (6) insurance information; (7) medical information; (8) dates of birth; (9) scanned images of active credit cards; (10) scanned images of passports; and (11) scanned images of licenses.

9. At the time of the Data Breach, Fidelity did not implement certain security controls

necessary to restrict customers from accessing certain images associated with other customer accounts in the Document Image Repository.

10. Between August 17 and 19, 2024, the Threat Actor accessed and obtained certain images of documents related to Fidelity customers and other individuals by manipulating technical information used to communicate with Fidelity's website.

11. In some cases, the Threat Actor accessed PII for Massachusetts residents who were not themselves customers of Fidelity, including relatives of Fidelity customers, named and contingent beneficiaries, and other persons associated with Fidelity customer transactions, some of whom were minors.

12. On or about October 9, 2024, Fidelity undertook to provide notice of the Data Breach to Massachusetts residents but failed to provide notice of the Data Breach to certain Massachusetts residents.

B. The Threat Actor Exploited Cybersecurity Vulnerabilities and Fidelity's Cybersecurity Controls Related to the Document Image Repository.

13. To accomplish the Data Breach, the Threat Actor exploited a vulnerability related to Fidelity's access controls.

14. Access controls ensure that an IT system properly authenticates its users (*e.g.*, that the user is who they say they are) and authorize actions (*e.g.*, ensure a user is permitted to access a specific document or perform a function).

15. Part of the system Fidelity developed used application programming interfaces ("APIs"), which facilitate connections between software applications.

16. An API enables various software applications to easily exchange data.

17. APIs work in the background, beyond the view of users, to send requests and information.

18. During the Data Breach, the Threat Actor exploited two Fidelity APIs.

19. The first API exchanged information between Fidelity's website and an internal server (the "Front-End API").

20. The second API exchanged information between the internal server and the Document Image Repository.

21. Certain images stored in the Document Image Repository were identified by a unique ten digit identifier (the "Image ID").

22. While on Fidelity's website, an authenticated Fidelity customer could retrieve images associated with their account by clicking on a link displayed to that customer.

23. In the background, a request, or "call," would be placed for the Image ID corresponding to the requested image. The Document Image Repository would then be searched for a document corresponding to the Image ID. If a corresponding document existed, the image would have been retrieved and displayed to the user.

i. The Threat Actor Exposed Vulnerabilities in the Design and Security of the Document Image Retrieval System.

24. In connection with the Data Breach, the Threat Actor used two brokerage accounts that it opened in July 2024 using the identities of two individuals in a type of identity theft known as "true name fraud."

25. True name fraud involves the use of another person's real identity to open fraudulent accounts.

26. The Threat Actor was able to access Fidelity's website as an authenticated user by using the Fidelity credentials that the Threat Actor established when setting up the brokerage accounts. Once logged in, the Threat Actor was able to access the document image retrieval function available through Fidelity's website.

27. On August 17, 2024, in an apparent trial run, the Threat Actor logged in to Fidelity's systems and manipulated certain technical information used to communicate with Fidelity's website to generate and submit approximately 1,000 API calls, presumably fishing for images of documents associated with other customer accounts from the Document Image Repository using variations of the Image IDs.

28. The Threat Actor again logged in to Fidelity's website as an authenticated user on August 18, 2024 and August 19, 2024.

29. During this time, the Threat Actor made approximately 23.7 million calls for images by generating random ten digit Image IDs, likely using an automated script.

30. While the vast majority of the Threat Actor's calls failed, the Threat Actor accessed approximately 373,000 unique images of documents associated with the accounts of other Fidelity customers.

31. These images of documents contained PII and/or medical information for at least 2,768 Massachusetts residents, at least 2,650 of which were customers of FBS or associated with FBS customer accounts (for example, because of their status as a beneficiary or power of attorney).

32. The Threat Actor's activity was initially detected by a system intended to detect denial of service ("DDoS") attacks—attempts to disrupt a system by overwhelming it with network traffic.

33. On August 19, 2024, at 8:06 AM, Fidelity was alerted to what was perceived to be a "small scale DDoS attack."

34. Subsequent analysis by Fidelity revealed the Threat Actor was not orchestrating a DDoS attack, but instead was accessing images of documents stored within the Document

Image Repository.

ii. Fidelity Did Not Implement Reasonable Security Controls Specific to the APIs Exploited in the Data Breach and Used in Connection With its Brokerage Business.

35. Fidelity Investments is the parent company of Fidelity. Fidelity Investments established enterprise-wide cybersecurity policies, applicable to Fidelity.

36. Fidelity's cybersecurity was managed at an enterprise-wide level by an internal group composed of approximately 1,200 employees called Enterprise Cyber Security ("ECS").

37. Fidelity relies upon ECS for day-to-day cybersecurity operations and to establish strategies, policies, and standards for security and operations.

38. One of Fidelity's policies relating to cybersecurity states "[p]rotecting Fidelity['s] critical information assets and data from cyberattacks, loss[,] and misuse is a top corporate priority."

39. Fidelity's cybersecurity policy required certain access controls to be implemented to protect customer data.

40. With respect to certain APIs, responsibility for implementing security controls rested with the teams responsible for those APIs.

41. Fidelity did not ensure the team responsible for the Document Image Repository properly implemented certain necessary authorization controls.

42. At the time of the Data Breach, Fidelity did not reasonably enforce its technical security policies designed to restrict users—including the Threat Actor—to accessing only the images in the Document Image Repository that are associated with that user's account.

43. In connection with the Document Image Repository, Fidelity Investments

maintained a service guide detailing its operations, including security functions (the "Service Guide").

44. The Service Guide directed the use of authorization controls as early as May 2019 and continuing through the date of the Data Breach.

45. When deploying a new API that connected to the Document Image Repository in 2022, Fidelity did not enforce these technical security policies to prevent the Threat Actor from accessing images of documents not associated with the Threat Actor's account.

46. Only after the Data Breach did Fidelity enforce its technical security policies for the API connected to the Document Image Repository, including those identified by the Service Guide.

47. In addition, Fidelity's systems did not hide the parameters of the Image ID from authenticated users of Fidelity's website. Any authenticated user, after logging into their Fidelity.com account and attempting to retrieve an image associated with their account, could take certain actions to ultimately see that the Image ID was composed of a ten digit string of numbers.

48. In fact, the Image ID was viewable through use of an internet browser by displaying developer tools.

49. Because the Image IDs were potentially visible to any authenticated user when retrieving images associated with their account and viewing the code in the browser, the Threat Actor was able to identify the parameters of the Image ID. The Threat Actor used this information to manipulate certain technical information used to communicate with Fidelity's website, and ultimately generated and submitted its API requests to Fidelity.

iii. Fidelity Did Not Design a Reasonable Test Environment to Identify Vulnerabilities in the APIs Exploited by the Threat Actor.

50. Prior to the Data Breach, Fidelity conducted penetration tests on APIs relevant to the Threat Actor's exploitation.

51. The objective of a penetration test is to identify vulnerabilities in the IT applications or systems being tested.

52. The penetration tests were conducted using a test environment—a simulated version of a system designed to be attacked by ethical hackers.

53. The test environment prepared by Fidelity did not properly expose testers to the view image functionality, because the test accounts used did not contain images for the testers to attempt to access.

54. Had the test accounts used for Fidelity's penetration tests included images, the vulnerabilities exploited by the Threat Actor may have been identified.

iv. Fidelity Engaged External Consultants That Made Recommendations for Areas of Improvement Prior to the Data Breach.

55. Fidelity annually reviewed its security and privacy risks against the standard guidelines set by the National Institute of Standards and Technology (the "NIST Assessments") and employed two consulting firms prior to the Data Breach to conduct these assessments. The assessments reviewed Fidelity practices and made recommendations for general areas of improvement, including with respect to APIs, although none identified the particular vulnerabilities that gave rise to the Data Breach.

56. Notwithstanding Fidelity's engagement of these consultants and the performance of the NIST Assessments, the vulnerabilities at issue in the Data Breach persisted until 2024.

57. Months prior to the Data Breach, Fidelity began the process of evaluating a vendor (the "API Support Provider"), which already provided Fidelity with other cybersecurity services including DDoS protection, as well as the comparable services of another provider.

58. On November 1, 2024, Fidelity retained the services of the API Support Provider.

C. Fidelity Failed to Enforce Certain Necessary Security Policies Informed by Regulatory Standards and Industry Guidance.

i. The Threat Actor Exploited a Known Cybersecurity Vulnerability.

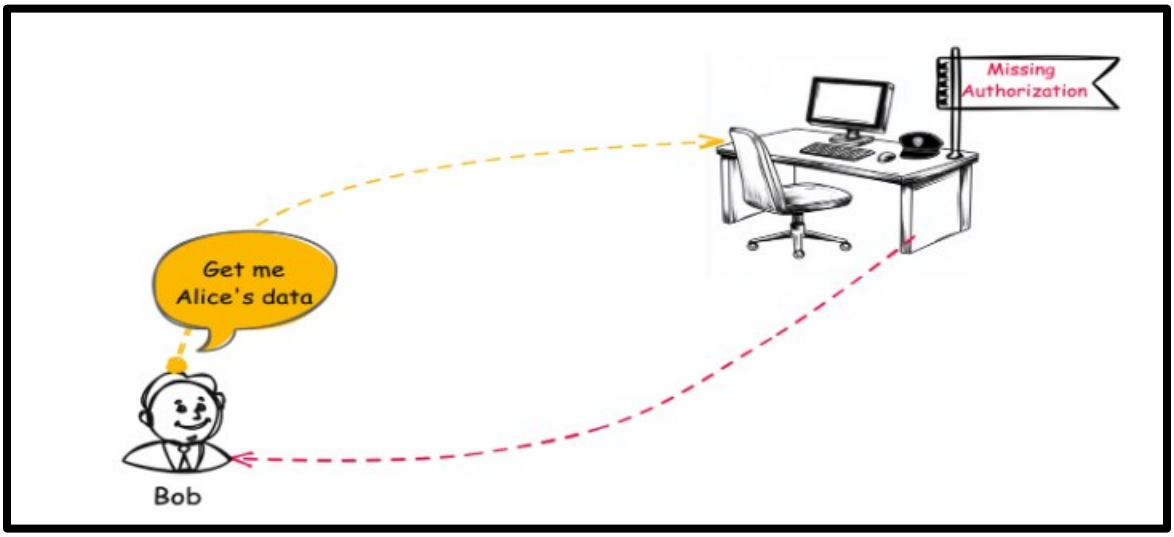
59. Fidelity knew or should have known about the cybersecurity vulnerabilities exploited by the Threat Actor.

60. As the Open Worldwide Application Security Project ("OWASP"), a non-profit organization that serves as an industry resource, explains, authorization involves the "process of verifying that a requested action . . . is approved . . . ."[2]

61. OWASP further explains that "[a] user who has been authenticated (perhaps by providing a username and password) is often not authorized to access every resource and perform every action that is technically possible through a system."[3]

[2] OWASP Cheat Sheet Series, https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.html (last visited March 9, 2026) (citing NIST).
[3] OWASP Cheat Sheet Series, https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.html (last visited March 9, 2026).

62. A missing authorization control can be understood through the following diagram:



https://cwe.mitre.org/data/images/CWE-862-Diagram.png

63. As depicted above, the missing authorization control allows "Bob" to retrieve "Alice's" data because the system fails to recognize that "Bob" is placing a request for data other than his own.

64. According to OWASP, missing and improper authorization controls present a high likelihood of exploitation.[4]

65. OWASP further cautions against a subset of authorization control issues, known as broken object-level authorization—an access control mechanism used to validate that a user can only access the objects they have permissions to access.[5]

66. As OWASP explains, "[a]ttackers can exploit API endpoints that are vulnerable to broken object-level authorization by manipulating the ID of an object that is sent within

[4] OWASP Cheat Sheet Series, https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.html (last visited March 9, 2026).
[5] OWASP API Security Top 10, https://owasp.org/API-Security/editions/2023/en/0xa1-broken-object-level-authorization/ (last visited March 9, 2026).

the request. Object IDs can be anything from sequential integers, UUIDs,[6] or generic strings." OWASP also notes that broken object-level authorization issues are easy to exploit and "extremely common."[7]

67. Access control issues were among OWASP's Top 10 risks to be involved in exploits and security incidents.[8]

68. As described by OWASP, access controls can be exploited as a result of an "Insecure Direct Object Reference" through which attackers "access or modify objects by manipulating identifiers used in a web application's URLs or parameters."[9]

69. For example, a web application may use a string of numbers in connection with a particular object, such as an image of check. By manipulating this string of a numbers, an attacker may gain access to materials associated with another user's account.

ii. State and Federal Laws and Regulations Mandate the Implementation of Reasonable Cybersecurity Policies and Procedures.

70. State and federal laws and regulations require broker-dealers to implement controls to establish reasonable cybersecurity programs.

71. Federal regulators adopted the Privacy of Consumer Financial Information rule, known as Regulation S-P, which became effective in 2000.

72. Regulation S-P requires registered financial firms, including broker-dealers, to "adopt written policies and procedures that address administrative, technical, and physical

[6] UUIDs are unique identifiers sometimes use as a quick way to generate random strings of integers. *See e.g.*, https://cheatsheetseries.owasp.org/cheatsheets/Cryptographic_Storage_Cheat_Sheet.html.
[7] OWASP API Security Top 10, https://owasp.org/API-Security/editions/2023/en/0xa1-broken-object-level-authorization/ (last visited March 9, 2026).
[8] *See* OWASP Top 10 API Security Risks – 2023, https://owasp.org/API-Security/editions/2023/en/0x11-t10/ (last visited March 9, 2026).
[9] OWASP Cheat Sheet Series, https://cheatsheetseries.owasp.org/cheatsheets/Insecure_Direct_Object_Reference_Prevention_Cheat_Sheet.html (last visited March 9, 2026).

safeguards for the protection of customer records and information."

73. Massachusetts registered broker-dealers, including Fidelity, are required to comply with Regulation S-P as well as Massachusetts laws and regulations governing cybersecurity and data privacy.

74. FINRA, since at least 2015, has identified "access management" issues in its guidance to registered broker-dealers.

75. Although Fidelity had technical security policies designed to limit access to the Document Image Repository to authorized users, Fidelity did not reasonably enforce those policies and thereby prevent the Threat Actor from accessing document images without authorization.

VII. VIOLATIONS OF LAW

Count I - Violations of M.G.L. c. 110A, § 204(a)(2)(J)

76. Section 204 of the Act provides:

> (a) The secretary may by order impose an administrative fine or censure or deny, suspend, or revoke any registration or take any other appropriate action if he finds (1) that the order is in the public interest and (2) that the applicant or registrant or, in the case of a broker-dealer or investment adviser, any partner, officer, or director, any person occupying a similar status or performing similar functions, or any person directly or indirectly controlling the broker-dealer or investment adviser:
>
> . . .
>
> (J) has failed reasonably to supervise agents, investment adviser representatives or other employees to assure compliance with this chapter[.]

M.G.L. c. 110A, § 204(a)(2)(J).

77. Respondent's acts and practices, as described above, constitute violations of

M.G.L. c. 110A, § 204(a)(2)(J).

VIII. STATUTORY BASIS FOR RELIEF

Section 407A of the Act provides, in pertinent part:

> (a) If the secretary determines, after notice and opportunity for hearing, that any person has engaged in or is about to engage in any act or practice constituting a violation of any provision of this chapter or any rule or order issued thereunder, he may order such person to cease and desist from such unlawful act or practice and may take such affirmative action, including the imposition of an administrative fine, the issuance of an order for an accounting, disgorgement or rescission or any other such relief as in his judgment may be necessary to carry out the purposes of [the Act].

M.G.L. c. 110A, § 407A.

IX. ORDER

IT IS HEREBY ORDERED:

A. Respondent shall permanently cease and desist from further acts and practices in violation of the Act and Regulations;

B. Respondent is censured by the Division;

C. Respondent shall, within five (5) business days of the entry of this Order, pay an administrative fine in the amount of one million two hundred and fifty thousand dollars ($1,250,000 (USD)) to the Commonwealth of Massachusetts. Payment shall be: (1) made by wire transfer, certified check, bank cashier's check, United States postal money order, or bank money order; (2) made payable to the Commonwealth of Massachusetts; (3) either hand-delivered or mailed to One Ashburton Place, Room 1701, Boston, Massachusetts 02108, or wired per Division instructions; and (4) submitted under cover letter or other documentation that identifies the payor making the payment and the docket number of the proceedings. Additionally,

Respondent shall provide the Enforcement Section with written notice of the form of payment and timing of payment at least seventy-two (72) hours prior to the payment;

D. Pursuant to this Order, Respondent certified that it conducted a review not unacceptable to the Division to identify Massachusetts residents whose PII was exposed in the Data Breach who were due notice under Massachusetts law and who were not previously notified by Respondent ("Impacted Residents").

   i. Respondent has submitted to the Division a list of all Impacted Residents, including name, address, e-mail address, and breached elements;

   ii. Respondent shall, within thirty (30) days of the entry of this Order, mail a written notice ("Notice Letter") compliant with applicable law, and not unacceptable to the Division, to all Impacted Residents;

   iii. Respondent shall provide the Division with a list of all Impacted Residents for whom Respondent receives a Notice Letter as returned to sender and otherwise is unable to identify a mailing address ("Undeliverable Residents"); and

   iv. To the extent the Division provides mailing address information for Undeliverable Residents, Respondent shall mail a Notice Letter to the address provided by the Division within fifteen (15) days of the Division providing such different address;

E. Respondent shall, within ninety (90) days of the entry this Order, submit a written certification by a person authorized by Respondent who is not unacceptable to the Division, certifying that cybersecurity controls related to customer data stored in

the Document Image Repository have been changed and enhanced to remediate the vulnerabilities that gave rise to the Data Breach. At a minimum, Respondent shall certify that:

i. Reasonable controls have been implemented to prevent users from accessing without authorization images associated with other customer accounts through the API call process to the Document Image Repository at issue in the Data Breach;

ii. Reasonable controls have been implemented to prevent exposure of Document Image Repository Image IDs to users by the Front-End API at issue in the Data Breach; and

iii. Respondent has changed or enhanced its policies and procedures with respect to its APIs that access customer account data to reasonably prevent the unauthorized access to customer account data, including PII;

F. Respondent shall, within ninety (90) days of the entry of this Order, submit to the Division a report by an independent cybersecurity consultant, not unacceptable to the Division, concerning the implementation and efficacy of the controls specified in Section IX(E)(i) and (ii) related to customer data stored in the Document Image Repository at issue in the Data Breach. The report shall be delivered to the Division within ten (10) days of its completion.

i. Respondent agrees to retain copies of any and all report(s) as set forth in paragraph (F) above in an easily accessible place for a period of five (5) years from the date of the reports;

G. For purposes of this Order, the last day of the time period so computed is to be

included unless it is a Saturday, Sunday, or legal holiday or any other day on which the Division is not open for regular business, in which event the period shall run until the end of the next following business day;

H. 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;

I. 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;

J. If Respondent is the subject of a voluntary or involuntary bankruptcy petition within one (1) year of the entry of this Order, Respondent shall provide written notice to the Division within five (5) days of the date of the petition;

K. Any fine, penalty, and/or money that Respondent shall pay in accordance with this Order is intended by Respondent and the Division to be a contemporaneous exchange for new value given to Respondent pursuant to 11 U.S.C. § 547(c)(1)(A) and is, in fact, a substantially contemporaneous exchange pursuant to 11 U.S.C. § 547(c)(1)(B);

L. Respondent has agreed that if it fails to comply with any of the terms set forth in this Order, the Division may institute an action to have this agreement declared null and void. Additionally, Respondent has agreed that, after notice and an opportunity for hearing, and the issuance of an order finding that Respondent has not complied with this Order, the Division may move to have this Order declared null and void,

in whole or in part, and re-institute the associated proceeding that had been brought against Respondent;

M. Respondent has agreed and understands that its failure to fully comply with any of the terms set forth in this Order is a violation of the Act and Regulations, and the Division may take action seeking compliance of any such terms or any such relief as may be necessary to carry out the purposes of the Act and Regulations; and

N. For good cause shown, the Division may agree to extend any of the procedural dates set forth above. Respondent shall to make any requests for extensions of the dates set forth above in writing to the Division.

X. WAIVER

Respondent waives any right to contest this Order, including whether the Order is fair, reasonable, and in the public interest, any right to a hearing, to written findings of fact, conclusions of law, or to any other process provided by the Act and Regulations, and waives any right to judicial review of this Order pursuant to M.G.L. c. 110A, § 411 and M.G.L. c. 30A, § 14(7).

XI. PUBLIC INTEREST

Consistent with the purposes fairly intended by the policy and provisions of M.G.L. c. 110A, this Order is necessary, appropriate, in the public interest, and for the protection of investors.

XII. NO DISQUALIFICATION

This Order waives any disqualification in the laws of Massachusetts, or rules or regulations thereunder, including any disqualification from relying upon the registration exemptions or safe harbor provisions to which Respondent may be subject. This Order is

not intended to be a final order based upon violations of the Act that prohibit fraudulent, manipulative, or deceptive conduct. This Order is not intended to form the basis of any disqualifications under Section 3(a)(39) of the Securities Exchange Act of 1934; or Rules 504(b)(3) and 506(d)(1) of Regulation D, Rule 262(a) of Regulation A and Rule 503(a) of Regulation CF under the Securities Act of 1933. This Order is not intended to form the basis of disqualification under the FINRA rules prohibiting continuance in membership absent the filing of a MC-400A application or disqualification under SRO rules prohibiting continuance in membership. This Order is not intended to form a basis of a disqualification under 204(a)(2) of the Uniform Securities Act of 1956 or Section 412(d) of the Uniform Securities Act of 2002. Except in an action by the Division to enforce the obligations of this Order, any acts performed or documents executed in furtherance of this Order: (a) may not be deemed or used as an admission of, or evidence of, the validity of any alleged wrongdoing, liability, or lack of any wrongdoing or liability; or (b) may not be deemed or used as an admission of; or evidence of, any such alleged fault or omission of Respondent in any civil, criminal, arbitration, or administrative proceeding in any court, administrative agency, or tribunal.

WILLIAM FRANCIS GALVIN
SECRETARY OF THE COMMONWEALTH

Diane Young-Spitzer

Diane Young-Spitzer, Esq.
Director & General Counsel
Securities Division
Office of the Secretary of the Commonwealth
John W. McCormack Building, 17th Floor
One Ashburton Place
Boston, MA 02108

Dated: April 27, 2026