NEW YORK STATE
DEPARTMENT OF FINANCIAL SERVICES
ONE STATE STREET
NEW YORK, NEW YORK 10004

----------x

In the Matter of :

GENESIS GLOBAL TRADING, INC. :

----------x

CONSENT ORDER

The New York State Department of Financial Services (the "Department" or "DFS") and Genesis Global Trading, Inc. ("GGT" or the "Company") are willing to resolve the matters described herein without further proceedings.

WHEREAS, GGT is licensed by the Department, pursuant to 23 NYCRR Part 200 (the "Virtual Currency Regulation"), to engage in virtual currency business activity in New York State and is a "licensee" pursuant to 23 NYCRR § 200.2(f);

WHEREAS, among other obligations, the Virtual Currency Regulation requires that licensees adhere to federal and New York laws and regulations that require businesses to maintain effective controls to guard against money laundering and certain other illicit activities, maintain a robust cybersecurity program, and ensure that consumers are fully informed with respect to all aspects of the transactions they enter into;

WHEREAS, New York's first-in-the-nation cybersecurity regulation, 23 NYCRR Part 500 (the "Cybersecurity Regulation"), was promulgated to strengthen cybersecurity and data protection for the financial services industry and thus sets out clear standards and guidelines for industry compliance, robust consumer protection, and vital cybersecurity controls;

WHEREAS, by virtue of its license granted pursuant to the Virtual Currency Regulation, GGT is a "Covered Entity" pursuant to 23 NYCRR § 500.1(c);

WHEREAS, the Department conducted an initial full-scope examination of GGT covering the period of May 17, 2018, through March 31, 2019 (the "First Exam") and found deficiencies in GGT's overall compliance function, including, among other things, its anti-money laundering ("AML") and cybersecurity compliance programs;

WHEREAS, the Department conducted a second full-scope examination of GGT covering the period of April 1, 2019, through March 31, 2022 (the "Second Exam"), and determined that, while GGT's business had grown significantly during this period, little effort or resources had been directed to addressing the deficiencies identified in the First Exam. In fact, the Second Exam identified further compliance failures with respect to the Virtual Currency Regulation and the Cybersecurity Regulation;

WHEREAS, following the Second Exam, the Department initiated an enforcement investigation into GGT's compliance with the Virtual Currency Regulation and the Cybersecurity Regulation; and

WHEREAS, following the enforcement investigation, the Department concluded that GGT violated certain sections of the Virtual Currency Regulation and the Cybersecurity Regulation.

NOW THEREFORE, in connection with an agreement to resolve this matter without further proceedings, the Department finds as follows:

THE DEPARTMENT'S FINDINGS

Introduction

1. The Department is the primary financial services regulator in the State of New York, and the Superintendent of Financial Services (the "Superintendent") is responsible for ensuring the safety, soundness, and prudent control of the various financial services businesses that the Department oversees through the enforcement of the various laws and regulations applicable to financial services licensees, including the New York Financial Services Law and the regulations promulgated thereunder.

2. The Superintendent has the authority to conduct investigations, bring enforcement proceedings, levy monetary penalties, and order injunctive relief against parties who have violated laws and regulations.

The Virtual Currency Regulation

3. The Department developed and oversees a first-of-its-kind regulatory framework pertaining to virtual currency businesses. Companies that conduct virtual currency business activity[1] in the State of New York must be licensed to do so by the Department, through what is known as a BitLicense, or chartered through the Department's Limited Purpose Trust Charter

[1] Virtual currency business activity means the conduct of any one of the following types of activities involving New York or a New York resident: (1) receiving virtual currency for transmission or transmitting virtual currency, except where the transaction is undertaken for non-financial purposes and does not involve the transfer of more than a nominal amount of virtual currency; (2) storing, holding, or maintaining custody or control of virtual currency on behalf of others; (3) buying and selling virtual currency as a customer business; (4) performing exchange services as a customer business; or (5) controlling, administering, or issuing a virtual currency.

process. In either event, virtual currency business activity in New York is subject to the Department's ongoing supervision.

4. The specific obligations of virtual currency companies are set forth in the Virtual Currency Regulation. Among the licensing and compliance requirements contained in the Virtual Currency Regulation, each licensee must comply with financial reporting requirements, *see* 23 NYCRR § 200.14; develop and implement various compliance policies and programs, including a robust AML program, *see* 23 NYCRR § 200.15, a cybersecurity program, *see* 23 NYCRR § 200.16, and a business continuity and disaster recovery ("BCDR") policy, *see* 23 NYCRR § 200.17; and ensure that consumers are fully informed as to all aspects of the transactions they enter into, *see* 23 NYCRR § 200.19.

5. The Superintendent is empowered to impose civil monetary penalties for violations of the Virtual Currency Regulation pursuant to Section 408 of the New York State Financial Services Law.

The Cybersecurity Regulation

6. Among the Superintendent's many roles is a consumer protection function, which includes the protection of individuals' private and personally sensitive data from careless, negligent, or willful exposure by Covered Entities.

7. To support this critical role, the Cybersecurity Regulation, as defined above, places on all Covered Entities an obligation to establish and maintain a cybersecurity program designed to protect the confidentiality, integrity, and availability of its Information Systems, as well as any Nonpublic Information ("NPI") belonging to consumers contained therein. 23 NYCRR §§ 500.1(e), 500.1(g), 500.2(a).

8. The basis of such cybersecurity program, as well as the policies and procedures that make up the program, is the cybersecurity risk assessment. *See* 23 NYCRR §§ 500.02, 500.9. Based on the risks identified in the risk assessment and the development of cybersecurity policies and procedures, *see* 23 NYCRR § 500.3, Covered Entities must ensure the integrity of their Information Systems and NPI by, among other things, conducting annual penetration testing, 23 NYCRR § 500.5, maintaining audit trails, 23 NYCRR § 500.6, limiting user access privileges, 23 NYCRR § 500.7, implementing data retention policies and encryption, 23 NYCRR §§ 500.13, 500.15, and establishing a robust incident response plan, 23 NYCRR § 500.16.[2]

9. The Superintendent is empowered to impose civil monetary penalties for violations of the Cybersecurity Regulation pursuant to Section 408 of the New York State Financial Services Law.

Events at Issue

Background

10. GGT's primary business was non-custodial, over-the-counter trading of digital currencies. GGT acted as the principal in all trades, buying and selling digital currencies from its own digital currency inventory. GGT earned a spread when it buys or sells digital currencies out of its inventory. The counterparties with which GGT worked were primarily institutional entities and high-net-worth individuals who generally fit the definition of accredited investors. GGT also served as an authorized participant in several private open-ended trusts that are invested exclusively in various digital currencies.

11. The Department, through reviews conducted during both the First Exam and the Second Exam, as well as during the enforcement investigation, determined that GGT failed to

[2] Section 200.16 of the Virtual Currency regulation echoes and expands on many of the requirements contained in the Cybersecurity Regulation.

maintain effective compliance with the Virtual Currency Regulation and the Cybersecurity Regulation.

12. Policies, procedures, and processes at GGT did not keep pace with the Company's significant growth during the relevant period.

Deficiencies in GGT's Anti-Money Laundering Program

13. Section 200.15 of the Virtual Currency Regulation requires virtual currency licensees to establish and maintain an AML program based on a risk assessment that considers legal, compliance, financial, and reputational risks associated with the licensee's activities, services, customers, counterparties, and geographic location. 23 NYCRR § 200.15(b).

14. GGT did not complete a risk assessment that met the Virtual Currency Regulation's requirements until mid-2022 (the "2022 Enterprise-Wide Risk Assessment"). GGT's failure, until that time, to conduct a firm-wide risk assessment of its products, services, customers, and lines of business meant that GGT did not have proper controls in place to mitigate the high inherent risks certain products and services posed to GGT and its customers. Indeed, the mitigating controls that supposedly were in place to address or offset these risks were classified by the 2022 Enterprise-Wide Risk Assessment as weak and marginal.

15. GGT's failure to conduct a thorough and up-to-date firm-wide risk assessment prior to 2022 caused the Department to have significant concerns about GGT's business model as a whole, especially its ability to ensure a strong, risk-based AML program compliant with Section 200.15.

16. A compliant AML program must, at a minimum, (1) provide for a system of internal controls, policies, and procedures designed to ensure ongoing compliance with all applicable anti-money laundering laws, rules, and regulations; (2) provide for independent

testing for compliance conducted by qualified internal personnel of the licensee or a qualified external party; (3) designate a qualified individual or individuals responsible for coordinating and monitoring day-to-day compliance; and (4) provide ongoing training for appropriate personnel. 23 NYCRR § 200.15(c). The AML program must be memorialized in a written policy that is reviewed and approved by the licensee's board of directors or equivalent governing body, 23 NYCRR § 200.15(d), and the individual responsible for coordinating and monitoring day-to-day AML compliance must fulfill each of the responsibilities enumerated in 23 NYCRR § 200.15(k).

17. GGT's AML program failed to meet these standards in several areas. For example, the First Exam found that the ongoing transaction monitoring process to identify unusual and suspicious transactions was not documented in GGT's BSA/AML policies and procedures. Furthermore, the procedures did not detail the enhanced due diligence reviews that were being conducted for high-risk customers and accounts.

18. Although some improvements were made to GGT's AML program between the First and Second Exams, the AML policies and procedures that were in place at GGT during both exams were generic and contained significant gaps. This finding was supported by the fact that the 2022 Enterprise-Wide Risk Assessment assigned marginal and weak ratings to GGT's AML policies and procedures. Further, not only were certain GGT's Board members and new employees not being trained in a timely manner, but certain internal AML policies and procedures were not incorporated in the training modules that were offered.

19. Although GGT did designate a BSA/AML officer, as required by Section 200.15(c)(3), such appointment was done informally (via email), and prior to 2022 there is no

evidence that the appointed individual had sufficient authority or resources to administer an effective AML compliance program based on GGT's risk profile.

20. Section 200.15(e)(3) further requires that licensees monitor for transactions that might signify money laundering, tax evasion, or other illegal or criminal activity and file Suspicious Activity Reports ("SARs") in accordance with applicable federal laws, rules, and regulations.

21. After identifying several deficiencies in GGT's transaction monitoring and SAR filing policies and procedures during the First Exam, the Department's review of these same policies and procedures during the Second Exam found additional deficiencies. For example, the rules-based automated transaction monitoring system that GGT used to identify unusual and suspicious transactions was never subjected to a validation review to provide assurance that the system was tailored to the licensee's activities and was operating as intended. In fact, a significant number of alerts were routinely classified as low risk and not reviewed. In addition, there were no rules management policies or procedures in place for the ongoing maintenance of the automated transaction monitoring system.

22. During the Second Exam, the Department found that the number of SARs filed by GGT was not commensurate with the level of transactions being processed, resulting in concerns as to whether adequate suspicious activity detective measures were in place. Moreover, during the same timeframe, GGT did not file any continuing SARs as required by federal regulation. In addition, no reports of SAR filings were relayed to the Board of Directors until the summer of 2022.

Deficiencies in GGT's Sanctions Screening Program

23. Section 200.15(i) further requires that each licensee must "demonstrate that it has risk-based policies, procedures, and practices to ensure, to the maximum extent practicable, compliance with regulations issued by the [Office of Foreign Assets Control ("OFAC")]." 23 NYCRR § 200.15(i). OFAC is the office in the United States Department of Treasury responsible for administering and enforcing economic and trade sanctions.

24. Although the Second Exam determined that GGT had implemented a process whereby its entire consumer database was being subjected to ongoing screening against updated sanctions listings — thus remediating an issue identified during the First Exam — the Second Exam found that Genesis still was not conducting enhanced screening of employees and third-party service providers and, therefore, still was not fully compliant with OFAC guidelines.

Deficiencies in Consumer Protection Disclosure Requirements

25. The Virtual Currency Regulation also contains robust disclosure requirements designed to ensure that consumers are fully informed about material risks, terms, and conditions of each transaction into which they enter. *See* 23 NYCRR § 200.19. The Second Exam found that GGT was deficient in ensuring that consumers were so informed.

26. Specifically, for a time during the Second Exam, GGT could not demonstrate it was providing the required transaction disclosures to consumers, such as the amount of the transaction; the type and nature of the virtual currency transaction; the warning that an executed transaction cannot be undone; and other customary disclosures. *See* 23 NYCRR § 200.19(c).

27. Further, GGT did not have a process in place to ensure that all required disclosures were acknowledged as received by its customers, *see* 23 NYCRR § 200.19(d), and

did not ensure that all information required to be on transactions receipts was indeed contained in said receipts, *see* 23 NYCRR § 200.19(e).

Deficiencies in GGT's Cybersecurity Program

28. To support the Superintendent's critical obligation to protect private and sensitive data, the Department requires, through the Cybersecurity Regulation, that every Covered Entity such as GGT conduct a periodic risk assessment of its Information Systems sufficient to inform the design of the cybersecurity program and update such risk assessment(s) as necessary to address changes to the Covered Entity's Information Systems, NPI, or business operations. *See* 23 NYCRR §§ 500.1(e), 500.1(g), 500.9(a), 200.16.

29. The cybersecurity risk assessment is the foundation of a Covered Entity's cybersecurity program. Each Covered Entity is required to establish and maintain a cybersecurity program based on a risk assessment and designed to protect the confidentiality, integrity, and availability of the Covered Entity's Information Systems and NPI. *See* 23 NYCRR §§ 500.2, 200.16(a).

30. The cybersecurity risk assessment also serves to inform the design of the cybersecurity policies required by the Cybersecurity Regulation and the Virtual Currency Regulation. *See* 23 NYCRR §§ 500.3, 200.16(b). These policies must be approved by the Covered Entity's board of directors and designed to protect the Covered Entity's Information Systems and NPI. 23 NYCRR § 500.3.

31. The cybersecurity risk assessment completed by GGT in December 2022, itself years late, was not sufficiently comprehensive and did not include identification of areas, systems, or processes that required material improvement, updating, or redesign, or plans for

enhancing GGT's cybersecurity program to achieve full compliance with the requirements of the Cybersecurity Regulation. 23 NYCRR § 500.9.

32. Furthermore, the December 2022 risk assessment failed to allow for revision of controls to respond to technological developments and evolving threats and did not adequately consider the cybersecurity risks to GGT's business operations, including NPI collected or stored on Information Systems and the inadequate controls in place to protect Information Systems. 23 NYCRR § 500.9.

33. The First Exam reviewed GGT's cybersecurity policies and procedures and determined that several were deficient, including policies on asset inventory and device management, BCDR planning, systems and network monitoring, systems and application development and quality assurance, vendor and third-party service provider management, risk assessment, and incident response. 23 NYCRR § 500.3(c), (e), (g), (h), (l), (m), (n). Moreover, the Department found no evidence that the Board of Directors annually reviewed and approved the policies that were in place. *See* 23 NYCRR §§ 500.3, 200.16(b).

34. While improvements were made between the First Exam and the Second Exam, certain policies still lacked sufficient detail to adequately protect GGT's Information Systems and NPI stored therein.

35. For example, the policies implemented between the First Exam and Second Exam failed to address asset inventory and device management at GGT, as required by Section 500.3(c). Until September 2022, GGT's incident response policy also failed to include the requirement that a Covered Entity must report any Cybersecurity Events to the Department within 72 hours. 23 NYCRR §§ 200.16(b)(6), 500.17(a). This particular shortcoming was identified in the First Exam and remained outstanding at the time of the Second Exam.

36. Further, the BCDR policy, which the First Exam found deficient due to GGT's failure to conduct a comprehensive business impact analysis to assess and prioritize all business functions and processes, consider legal and regulatory requirements, and establish key recovery metrics as required by Section 200.17 of the Virtual Currency Regulation, still lacked sufficient BCDR procedures to address certain cybersecurity program aspects. *See* 23 NYCRR §§ 200.17, 500.3(e). Moreover, the Second Exam found that GGT employees were not being sufficiently trained on their roles and responsibilities under the BCDR policy and no annual testing of the policy was being conducted. 23 NYCRR § 200.17.

37. The Department also concluded that GGT's data classification policies and procedures, which are required under 23 NYCRR § 500.3(b), were incomplete, thus resulting in significant concerns regarding GGT's ability to adequately assess its compliance with the Cybersecurity Regulation's access privilege, 23 NYCRR § 500.7, data disposal, 23 NYCRR § 500.13, and encryption, 23 NYCRR § 500.15, requirements. These issues, in turn, prevented GGT from effectively limiting access to sensitive information.

38. GGT was well aware of the deficiencies in its ability to protect NPI. An internal audit report from September 2021 found that while some access management activities were being performed, there were a number of deficiencies that left the Company's Information Systems particularly vulnerable. The September 2021 internal audit ultimately concluded that that privileged access was inappropriately provided to unauthorized individuals causing unauthorized activity due to the fact that there is a lack of a formal program to periodically recertify user access to GGT infrastructure. *See* 23 NYCRR § 500.7.

39. Of further concern with respect to the protection of NPI, the Second Exam also found that policies and procedures for the secure disposal, on a periodic basis, of NPI had never

been established. In fact, data in critical applications was stored indefinitely and there was no process in place for categorizing and purging data that is no longer necessary to store, despite the clear requirements outlined in Section 500.13 of the Cybersecurity Regulation.

40. Additionally, due to the lack of a data classification policy, there were no means to ensure that all sensitive data and NPI were identified and encrypted as required by Section 500.15 of the Cybersecurity Regulation.

41. Overall, both the First Exam and the Second Exam found GGT's cybersecurity program to be significantly lacking. Specifically, a lack of compliant risk assessment, together with GGT's failure to have a comprehensive understanding of the NPI stored on its Information Systems, resulted in a program that did not, and could not, protect the confidentiality, integrity, and availability of the Covered Entity's Information Systems. 23 NYCRR §§ 500.2, 200.16(a).

GGT's Reporting Failures

42. Both the Virtual Currency Regulation and the Cybersecurity Regulation contain a number of provisions wherein the BitLicensee or Covered Entity is required to report certain information, or certify that certain information is correct, to the company's board of directors and the Department. GGT failed to meet these requirements.

43. Section 200.14 of the Virtual Currency Regulation lists the reports and financial disclosure requirements that licensees are required to submit to the Department regularly, such as audited financial statements that are supported by an opinion and an independent certified public accountant's attestation as to "the effectiveness of the licensee's internal control structure." 23 NYCRR § 200.14(b).

44. GGT failed to obtain the opinion and attestation by an independent certified public accountant as to the effectiveness of GGT's internal control structure until 2023 (for the 2022 calendar year).

45. To facilitate ongoing compliance with the Cybersecurity Regulation and maintain the security of a Covered Entity's Information Systems and NPI, Covered Entities must designate a qualified chief information security officer ("CISO"). The CISO is responsible for overseeing and implementing the Covered Entity's cybersecurity program and enforcing its cybersecurity policy. In so doing, the CISO must report in writing, at least annually, to the Covered Entity's board of directors about the status of the cybersecurity program, as well as any material cybersecurity risks facing the Covered Entity. *See* 23 NYCRR § 500.4.

46. The Virtual Currency Regulation takes the CISO's reporting responsibility a step farther by requiring the CISO to submit its report on the cybersecurity program to the Department. *See* 23 NYCRR § 200.16(d).

47. However, none of GGT's Board of Directors meeting minutes contain reference to annual reporting by the CISO on the status of GGT's cybersecurity program. In fact, GGT admitted to the Department that, until it hired a new CISO in November 2022, no annual cybersecurity reports were developed, let alone presented to the Board of Directors or the Department.

48. Additionally, pursuant to Section 500.17(b) of the Cybersecurity Regulation, Covered Entities are required to annually certify their compliance with the Cybersecurity Regulation.

49. Notwithstanding the fact that GGT was on notice of its non-compliance with the Cybersecurity Regulation as a result of the findings in the First Exam, which GGT received as

early as October 19, 2019, GGT certified compliance with the Cybersecurity Regulation for the calendar year 2019 on February 14, 2020, and for the calendar year 2020 on April 8, 2021.

50. In light of the foregoing findings, GGT was not in compliance with the Cybersecurity Regulation at the time of the certifications. As a result, GGT's certifications for the calendar years 2019 and 2020 were improper.

Violations of Law and Regulations

51. GGT failed to maintain a compliant anti-money laundering program, in violation of 23 NYCRR § 200.15.

52. GGT failed to ensure all consumer protection disclosures were made and acknowledged by consumers, in violation of 23 NYCRR § 200.19(c), (d), (e).

53. GGT failed to maintain a cybersecurity program based on a risk assessment, and designed to protect the confidentiality, integrity, and availability of its Information Systems, in violation of 23 NYCRR §§ 500.2, 500.9, 200.16(a).

54. GGT failed to maintain and implement compliant cybersecurity policies, in violation of 23 NYCRR §§ 500.3, 200.16(b), 200.17, 500.16(b)(6).

55. GGT failed to limit user access privileges, in violation of 23 NYCRR § 500.7.

56. GGT failed to implement policies and procedures for the secure disposal on a periodic basis of NPI, in violation of 23 NYCRR § 500.13.

57. GGT failed to encrypt NPI in transit and at rest, in violation of 23 NYCRR § 500.15.

58. GGT failed to submit an opinion and attestation by an independent certified public accountant, in violation of 23 NYCRR § 200.14(b).

59. GGT failed to ensure that its CISO submitted annual written reports to its Board of Directors and the Department, in violation of 23 NYCRR §§ 500.4, 200.16(d).

60. GGT improperly certified compliance with the Cybersecurity Regulation for the calendar years 2019 and 2020, in violation of 23 NYCRR § 500.17(b).

NOW THEREFORE, to resolve this matter without further proceedings, the Department and the Company stipulate and agree to the following terms and conditions:

SETTLEMENT PROVISIONS

Monetary Penalty

61. No later than ten (10) days after the Effective Date (as defined below) of this Consent Order, the Company shall pay a total civil monetary penalty pursuant to Financial Services Law § 408 to the Department in the amount of eight million U.S. dollars and 00/100 Cents ($8,000,000.00). The payment shall be in the form of a wire transfer in accordance with instructions provided by the Department.

62. The Company shall not claim, assert, or apply for a tax deduction or tax credit with regard to any U.S. federal, state, or local tax, directly or indirectly, for any portion of the civil monetary penalty paid pursuant to this Consent Order.

63. The Company shall neither seek nor accept, directly or indirectly, reimbursement or indemnification with respect to payment of the penalty amount, including, but not limited to, payment made pursuant to any insurance policy.

64. The Department acknowledges GGT's cooperation throughout this investigation. The Department also recognizes and credits GGT's ongoing efforts to remediate the shortcomings identified in this Consent Order. Among other things, GGT has demonstrated its commitment to remediation by devoting significant financial and other resources to updating

both its BSA/AML and cybersecurity programs over the past eighteen (18) months to ensure compliance with the Virtual Currency and Cybersecurity Regulations.

Surrender of License

65. GGT has notified the Department of its intention to cease operations, including all operations in New York State, and to surrender its license to conduct virtual currency business activity.

66. With the execution of this Consent Order, GGT hereby surrenders any and all licenses issued to it by the Department and consents to the denial of any and all pending applications for licenses, such surrender and denial having the same force and effect as of said licenses had been revoked or denied after a hearing.

67. The Department agrees and hereby accepts the surrender of any and all licenses issued by it to GGT and hereby denies any and all pending applications for licenses, such surrender and denial having the same force and effect as if said licenses had been revoked or denied after a hearing.

68. Surrender of the license shall not relieve the Company of its obligation to complete the lookback previously agreed upon in communications between the Department and the Company.

Full and Complete Cooperation

69. The Company commits and agrees that it will fully cooperate with the Department regarding all terms of this Consent Order.

Further Action by the Department

70. No further action will be taken by the Department against the Company or its successors for the conduct set forth in this Consent Order, or in connection with the remediation

set forth in this Consent Order, provided that the Company fully complies with the terms of the Consent Order. Furthermore, no further action will be taken by the Department against the Company for conduct in connection with the Department's investigation.

71. Notwithstanding any other provision in this Consent Order, however, the Department may undertake additional action against the Company for transactions or conduct that were not disclosed in the written materials submitted to the Department in connection with this matter.

Waiver of Rights

72. The Company submits to the authority of the Superintendent to effectuate this Consent Order.

73. The parties understand and agree that no provision of this Consent Order is subject to review in any court, tribunal, or agency outside of the Department.

Parties Bound by the Consent Order

74. This Consent Order is binding on the Department and the Company, as well as any successors and assigns. This Consent Order does not bind any federal or other state agency or any law enforcement authority.

Breach of Consent Order

75. In the event that the Department believes the Company to be in material breach of the Consent Order, the Department will provide written notice to the Company, and the Company must, within ten (10) days of receiving such notice, or on a later date if so determined in the Department's sole discretion, appear before the Department to demonstrate that no material breach has occurred or, to the extent pertinent, that the breach is not material or has been cured.

76. The Company understands and agrees that its failure to make the required showing within the designated time period shall be presumptive evidence of the Company's breach. Upon a finding that a breach of this Consent Order has occurred, the Department has all the remedies available to it under the New York Financial Services Law, and any other applicable laws, and may use any evidence available to the Department in any ensuing hearings, notices, or orders.

Notices

77. All notices or communications regarding this Consent Order shall be sent to:

For the Department:

Ndidi C. Obicheta
Senior Assistant Deputy Superintendent
Consumer Protection and Financial Enforcement
New York State Department of Financial Services
One State Street
New York, New York 10004

Madeline W. Murphy
Assistant Deputy Superintendent
Consumer Protection and Financial Enforcement
New York State Department of Financial Services
One Commerce Plaza
Albany, New York 12257

Justin D. Parnes
Assistant Deputy Superintendent
Consumer Protection and Financial Enforcement
New York State Department of Financial Services
One State Street
New York, New York 10004

For Genesis Global Trading, Inc.:

Legal Department
c/o Genesis Global Holdco, LLC
175 Greenwich St, FL 38
New York, NY 10007
legal@genesistrading.com

Miscellaneous

78. This Consent Order and any dispute thereunder shall be governed by the laws of the State of New York without regard to any conflicts of laws principles.

79. This Consent Order may not be altered, modified, or changed unless in writing and signed by the parties hereto.

80. This Consent Order constitutes the entire agreement between the Department and the Company and supersedes any prior communication, understanding, or agreement, whether written or oral, concerning the subject matter of this Consent Order.

81. Each provision of this Consent Order shall remain effective and enforceable against the Company, its successors, and assigns, until stayed, modified, suspended, or terminated by the Department.

82. In the event that one or more provisions contained in this Consent Order shall for any reason be held to be invalid, illegal, or unenforceable in any respect, such invalidity, illegality, or unenforceability shall not affect any other provision of this Consent Order.

83. No promise, assurance, representation, or understanding other than those contained in this Consent Order has been made to induce any party to agree to the provisions of this Consent Order.

84. Nothing in this Consent Order shall be construed to prevent any consumer or any other third party from pursuing any right or remedy at law.

85. This Consent Order may be executed in one or more counterparts and shall become effective when such counterparts have been signed by each of the parties hereto (the "Effective Date").

[*remainder of this page intentionally left blank*]

IN WITNESS WHEREOF, the parties have caused this Consent Order to be signed on the dates set forth below.

NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES

By: /s/ John A. Nicosia
JOHN A. NICOSIA
Senior Assistant Deputy Superintendent
Consumer Protection and Financial Enforcement

January 10, 2024

By: /s/ Alison L. Passer
ALISON L. PASSER
Deputy Director of Enforcement
Consumer Protection and Financial Enforcement

January 10, 2024

By: /s/ Kevin R. Puvalowski
KEVIN R. PUVALOWSKI
Acting Executive Deputy Superintendent for
Consumer Protection and Financial Enforcement

January 10, 2024

GENESIS GLOBAL TRADING, INC.

By: /s/ Arianna Pretto-Sakmann
ARIANNA PRETTO-SAKMANN
Chief Legal Officer

January 3, 2024

THE FOREGOING IS HEREBY APPROVED. IT IS SO ORDERED.

/s/ Adrienne A. Harris
ADRIENNE A. HARRIS
Superintendent of Financial Services

January 11, 2024