ANTONIA M. APPS
REGIONAL DIRECTOR
Tejal Shah
Adam S. Grace
Travis Hill
Rhonda Jung
SECURITIES AND EXCHANGE COMMISSION
New York Regional Office
100 Pearl Street
Suite 20-100
New York, NY 10004-2616
212-336-9135 (Hill)
HillTr@sec.gov

Deborah A. Tarasevich
Elizabeth Doisy
Martin Zerwitz
SECURITIES AND EXCHANGE COMMISSION
100 F Street N.E. / Mail Stop 5631
Washington, D.C. 20549-5631

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

SECURITIES AND EXCHANGE COMMISSION, **Plaintiff,** **-against-** **CHIBUZO AUGUSTINE ONYEACHONAM, STANLEY CHIDUBEM ASIEGBU, and CHUKWUEBUKA MARTIN NWEKE-EZE,** **Defendants.**	**COMPLAINT** **24-CV-11026** **JURY TRIAL DEMANDED**

Plaintiff Securities and Exchange Commission ("Commission"), located at

100 Pearl Street, Suite 20-100, New York, New York 10004-2616, for its Complaint against Defendants Chibuzo Augustine Onyeachonam ("Onyeachonam"), whose last known address is No. 15 Sir Clement Ezeodili Street, Ifite Awka, Anambra State, Nigeria; Stanley Chidubem Asiegbu ("Asiegbu"), whose last known address is No. 15 Mission Road, Awka, Anambra State, Nigeria; and Chukwuebuka Martin Nweke-Eze ("Nweke-Eze"), whose last known address is No. 4 Ashawo Street, Akwai, Adamawa State, Nigeria, (together, "Defendants") alleges as follows:

SUMMARY

1. Defendants, none of whom is an actual securities industry professional, impersonated real-life United States securities broker and investment adviser representatives online and by telephone and fraudulently obtained at least $2.9 million from mostly U.S.-based investors, who never knew Defendants' true identities.

2. Since at least 2019 through the date of this Complaint's filing (the "Relevant Period"), Defendants—Nigerian nationals living in Nigeria—created websites impersonating at least 22 actual securities broker and investment adviser representatives (collectively, "Representatives") at prominent U.S. securities firms and touted the representatives' purported securities industry experience in a

fraudulent scheme to lure potential U.S. investors into investing funds with Defendants.

3. In addition to posing as representatives, Defendants made repeated misrepresentations—including promises of monthly investment returns of 15% to 25%—to potential investors to persuade them to invest.

4. Defendants, posing as Representatives, instructed investors to open accounts at broker-dealers and crypto-asset trading platforms and purchase crypto assets, which Defendants then misappropriated.

5. Defendants also directed investors to fake online investment platforms Defendants created, where Defendants showed investors fictitious high returns. These fake returns and Defendants' purportedly successful trading skills led many investors to invest additional funds that Defendants also misappropriated.

6. When investors ultimately sought to withdraw their funds, Defendants informed investors that they were required to pay additional fees before funds would be released to them—holding investors' funds ransom.

7. In all, Defendants—and/or others working with them—stole at least $2.9 million from at least 28 investors, most of whom reside in the U.S.

VIOLATIONS

8. By virtue of the foregoing conduct and as alleged further herein, Defendants violated Section 17(a) of the Securities Act of 1933 ("Securities Act")

[15 U.S.C. § 77q(a)], Section 10(b) of the Securities Exchange Act of 1934 ("Exchange Act") [15 U.S.C. § 78j(b)] and Rule 10b-5 thereunder [17 C.F.R. § 240.10b-5], and Sections 206(1) and (2) of the Investment Advisers Act of 1940 ("Advisers Act") [15 U.S.C. §§ 80b-6(1) and 80b-6(2)].

9. Unless Defendants are restrained and enjoined, they will engage in the acts, practices, transactions, and courses of business set forth in this Complaint or in acts, practices, transactions, and courses of business of similar type and object.

NATURE OF THE PROCEEDINGS AND RELIEF SOUGHT

10. The Commission brings this action pursuant to the authority conferred upon it by Securities Act Sections 20(b) and 20(d) [15 U.S.C. §§ 77t(b) and 77t(d)], Exchange Act Section 21(d) [15 U.S.C. § 78u(d)], and Advisers Act Sections 209(d) and 209(e) [15 U.S.C. §§ 80b-9(d) and 80b-9(e)].

11. The Commission seeks a final judgment: (a) permanently enjoining Defendants from violating the federal securities laws and rules this Complaint alleges they violated; (b) permanently enjoining Defendants from directly or indirectly, including, but not limited to, through any entity controlled by each Defendant: (i) participating in the issuance, purchase, offer, or sale of any security on behalf of someone else; or (ii) engaging in activities for purposes of inducing or attempting to induce the purchase or sale of any security, including holding themselves out as industry professionals; provided, however, that such injunction

shall not prevent each Defendant from purchasing or selling securities for his own personal account; (c) ordering Defendants to disgorge all ill-gotten gains they received as a result of the violations alleged here and to pay prejudgment interest thereon, pursuant to Exchange Act Sections 21(d)(3), 21(d)(5), and 21(d)(7) [15 U.S.C. §§ 78u(d)(3), 78u(d)(5), and 78u(d)(7)]; (d) ordering Defendants to pay civil money penalties pursuant to Securities Act Section 20(d) [15 U.S.C. § 77t(d)], Exchange Act Section 21(d)(3) [15 U.S.C. § 78u(d)(3)], and Advisers Act Section 209(e) [15 U.S.C. § 80b-9(e)]; and (e) ordering any other and further relief the Court may deem just and proper.

JURISDICTION AND VENUE

12. This Court has jurisdiction over this action pursuant to Securities Act Section 22(a) [15 U.S.C. § 77v(a)], Exchange Act Section 27 [15 U.S.C. § 78aa], and Advisers Act Section 214 [15 U.S.C. § 80b-14].

13. Defendants, directly and indirectly, have made use of the means or instrumentalities of interstate commerce or of the mails in connection with the transactions, acts, practices, and courses of business alleged herein.

14. Venue lies in this District under Securities Act Section 22(a) [15 U.S.C. § 77v(a)], Exchange Act Section 27 [15 U.S.C. § 78aa], and Advisers Act Section 214 [15 U.S.C. § 80b-14]. Certain of the acts, practices, transactions, and courses of business alleged in this Complaint occurred within this District. At least

one of Defendants' investor victims resides in New Jersey and communicated with Defendants from New Jersey.

DEFENDANTS

15. **Onyeachonam**, age 30, resides in Awka, Nigeria. He has never been associated with any entity registered with the Commission. According to social media, Onyeachonam purports to be a web developer with Nicrotech.com, a web design and development business that uses Onyeachonam's personal cell phone number and address.

16. **Asiegbu**, age 27, resides in Awka, Nigeria. He has never been associated with any entity registered with the Commission.

17. **Nweke-Eze**, age 29, resides in Akwai, Nigeria. He has never been associated with any entity registered with the Commission.

DEFENDANTS' FICTITIOUS ENTITIES

18. **Alpha Crypto Fund** is a fake investment fund at least Onyeachonam pitched by impersonating a financial professional. The associated website was visible to users in the U.S. and included an investor portal that was used to provide false information to investors regarding the performance of their investment. Onyeachonam set up, controlled, and operated The Alpha Crypto Fund domains (alphacryptofund.com and alphacryptofund.io). An email address attributable to

Onyeachonam registered the alphacryptofund.com domain in May 2023 and the alphacryptofund.io domain in July 2023.

19. **CopyTradeApp** is a fake internet platform visible to users in the U.S. and abroad that was used to make investors think that impersonated financial professionals were engaging in "copy trading," a portfolio management strategy by which the financial professional would trade the investor's assets in sync with other trading activity being conducted by the professional. Both CopyTradeApp domains (CopyTradeApp.io and CopyTradeApp.com) were set up by Onyeachonam. An email address attributable to Onyeachonam registered the Copytradeapp.io domain in August 2020 and the Copytradeapp.com domain in September 2022.

20. **InstaForex Service**, with a website visible to users in the U.S. and abroad, purported to hold investors' funds for the duration of their investment. When investors attempted to withdraw their funds, InstaForex Service purported to require various costs and fees before any funds would be released to investors. A credit card in Nweke-Eze's name was used to deposit funds into the domain registrar account through which instaforexservice.com was registered. Those funds were used to renew the hosting plan for instaforexservice.com.

21. **LumenTrades** is a fake investment account platform visible to users in the U.S. and abroad, where investors were shown their initial investment and

often substantial, fictitious trading returns. Onyeachonam set up, controlled, and operated LumenTrades. Email addresses attributable to Onyeachonam were used to register the LumenTrades.com domain in August 2018 and incorporate LumenTrades Financial Incorporated in Oregon in March 2019. Email addresses attributable to Onyeachonam also show that he paid to incorporate LumenTrades as a legal entity in the United Kingdom. An email address attributable to Asiegbu shows that he assisted with the operation and control of LumenTrades.com by: (1) emailing code for displaying stock and trading information to admin@lumentrades.com, an email address controlled by Onyeachonam; (2) creating a business profile for LumenTrades so that LumenTrades could be found on Google Search and Maps; and (3) testing the stock purchasing and live chat functions for LumenTrades.com.

22. **Nuvoak** is a fictitious investment adviser firm purported to be associated with an impersonated representative in Defendants' scheme. One of Nuvoak's web domains (MyNuvoakOnline.com), visible to users in the U.S. and abroad, contained an investor portal used to provide false information to investors regarding their investment performance. Onyeachonam set up, controlled, and operated MyNuvoakOnline.com. An email address attributable to Onyeachonam registered the MyNuvoakOnline.com domain in November 2023.

23. **Secawallet**, with a website visible to users in the U.S. and abroad, displayed blockchain addresses to which investors were instructed to send their crypto assets. The website was used to give investors the false impression that crypto assets were "stored" with Secawallet for investment on their behalf. In reality, the investors' crypto assets were stolen once they were sent to the addresses displayed by the Secawallet website. Onyeachonam set up, controlled, and operated Secawallet.com. An email address attributable to both Onyeachonam and Asiegbu registered the Secawallet.com domain in June 2022. An email address attributable to Onyeachonam took ownership of the domain in September 2023.

24. **Wealthwindow** is a fake investment account platform visible to users in the U.S. and abroad, where investors were shown their initial investment and fictitious trading returns, which were often substantial. An email address attributable to Onyeachonam was used to register the wealthwindow.io domain in April 2024.

FACTS

I. THE GENERAL STRUCTURE OF DEFENDANTS' FRAUDULENT CYBER INVESTMENT SCHEME

25. Defendants' scheme involved registering internet domain names with the real first and last names of actual U.S.-based securities brokerage or investment adviser representatives—for example, "johndoe.com"—whom Defendants planned

to impersonate.

26. Most of the Representatives were employed at prominent U.S. investment firms.

27. Defendants similarly formed limited liability companies ("LLCs") using the names of the professionals they were impersonating to make it look like the professionals had their own investment-related firms.

28. Defendants then created websites that copied the real Representatives' genuine employment history and credentials from the Financial Industry Regulatory Authority's ("FINRA") BrokerCheck or the Commission's Investment Adviser Public Disclosure websites.[1]

29. The websites Defendants created touted the Representatives' investment advisory, trading, and crypto expertise.

30. The websites also sometimes provided the names of the LLCs Defendants had created using the names of the professionals they were impersonating.

31. To lure potential investors to the websites, Defendants (and possibly others working with them) created profiles on YouTube and placed fictitious

[1] FINRA is a self-regulatory organization, and BrokerCheck is a publicly-available, online tool listing employment history, certifications, licenses, and any legal violations for brokerage firm representatives and investment advisers, available at https://brokercheck.finra.org.

comments from purported advisory clients and brokerage customers (collectively, "Fake Clients") underneath investment-themed YouTube videos.

32. The Fake Clients' purported comments praised the Representatives' investment services and trading success.

33. Defendants used fake LinkedIn personas and participated in investment group chats in encrypted messaging apps to reach out to potential victims and encourage them to research the Representative whose identity Defendants had stolen.

34. Defendants, who impersonated mostly female financial professionals in the U.S., also purchased voice-changing software.

35. When potential investors, thinking Defendants were the impersonated Representatives, contacted Defendants, Defendants sent emails claiming that the Representatives would trade on each investor's behalf across three markets—the U.S. stock market, the foreign exchange market, and the crypto asset market—and recommended an investment allocation strategy that Defendants claimed would generate profits of 15% to 25% monthly.

36. Defendants' emails to potential investors claimed that the Representatives used a "copy trading" program that linked each investor's and Representative's trading accounts to ensure that each investor could see all of the representative's trades on the investor's behalf.

37. The potential investor then completed a client investment form and contract agreement and returned them by email to Defendants.

38. Next, Defendants typically instructed each investor to download legitimate trading apps and open accounts at specific, genuine broker-dealers and crypto-asset trading platforms and then provide their login credentials to Defendants so that Defendants could sync the investor's real accounts to the impersonated Representative's purported copy trading program—Defendants' CopyTradeApp.

39. Defendants—still impersonating real financial professionals—then typically told each investor that, for the first three weeks, they would predominantly trade the investor's funds in the crypto market to take advantage of its bullish state.

40. Defendants typically instructed each investor to fund specific, genuine brokerage accounts and crypto accounts at approximately a "20:80 ratio" or "10:90 ratio"—meaning to put one quarter or one ninth the amount of funds in brokerage accounts as in crypto accounts.

41. Defendants typically further instructed each investor to purchase bitcoin with the funds in the crypto account and send the bitcoin to a specified address to "fund" the investment. In some cases, the receiving address was set up by investors at Defendants' instruction. In other cases, the address was provided

by Defendants who claimed that the address was held by third-party entities which stored the investors' bitcoin for the duration of their investment. In reality, the purported third-party entities—e.g., Secawallet and InstaForex Service—were controlled by Defendants.

42. When investors purchased and transferred the bitcoin, they incurred third-party fees associated with the purchase and transfer of crypto assets—payments that increased their ultimate losses from Defendants' scheme.

43. Once the bitcoin was in the address Defendants had specified, the bitcoin was moved through multiple addresses, often ultimately landing in addresses controlled by Defendants or their associates.

44. Defendants then stole each investor's bitcoin instead of investing it.

45. Investors' funds in their real brokerage accounts remained mostly untouched by Defendants.

46. However, some of the brokerage account funds were subsequently used to further "fund" the investors' crypto asset investments, which were accessible to Defendants.

47. Defendants informed investors that they could view their account balance on an investment platform website—one of Defendants' fake platforms such as LumenTrades, Wealthwindow, or MyNuvoakOnline.com—which showed investors' purported returns on their investments.

48. After investors saw their investment accounts grow substantially, as fictitiously depicted in Defendants' fake investment platforms, Defendants—still posing as the real Representatives—often offered new trading strategies that Defendants claimed required investors to put in additional funds to maximize their returns.

49. Many investors, believing their initial investments had been successful, invested additional funds.

50. When investors requested to withdraw their funds, Defendants typically demanded that the investors pay commissions, performance, or other purported fees to access their funds.

51. Some investors paid these purported fees.

52. Investors did not know that they were actually investing with Defendants and not the Representatives whose identities Defendants had stolen.

53. Onyeachonam participated in the scheme by setting up the impersonated Representatives' websites; incorporating entities in the names of at least six impersonated Representatives; promoting impersonated Representatives online; setting up and operating fake investment account platforms; purchasing products and services used in the scheme; and impersonating Representatives to communicate with victim investors.

54. According to Onyeachonam's public Goodreads profile, fifteen days

after Onyeachonam registered the Lumentrades.com domain in 2018, Onyeachonam read *The Confidence Game: Why We Fall for It . . . Every Time* (Penguin Books 2017), a book written by Maria Konnikova and described by The Washington Post as an "unnerving manual for conning and getting conned."

55. Asiegbu participated in the scheme by assisting in setting up websites used in the scheme; promoting the impersonated Representatives and fake investment account platforms to the investing public; and managing email addresses used to communicate with victim investors.

56. Nweke-Eze participated in the scheme by using social media to solicit potential investors; promoting impersonated Representatives and Defendants' fictitious trading platforms online; and managing an email address used to communicate with victim investors.

57. During their fraudulent scheme, Defendants impersonated at least 22 Representatives and stole at least $2.9 million from at least 28 investors, at least 23 of whom reside in the U.S.

58. The examples below detail Defendants' fraudulent scheme with respect to five of these U.S. investors.

II. ONYEACHONAM IMPERSONATED A REGISTERED REPRESENTATIVE FROM WISCONSIN AND DEFENDANTS STOLE MORE THAN $500,000 FROM A CALIFORNIA INVESTOR.

A. Onyeachonam Impersonated a Wisconsin Representative Online.

59. In November 2019, Onyeachonam set up a website impersonating a Wisconsin-based registered Representative and investment adviser Representative ("Representative A"), who was employed by a large, dually registered broker-dealer and investment adviser firm that is a household name.

60. In 2019, Representative A had 19 years of experience as a broker-dealer representative and/or investment adviser representative.

61. In 2019, an email address attributable to Onyeachonam registered a domain name with Representative A's actual first and last name.

62. Onyeachonam then created a website on that domain that advertised the Representative's financial services.

63. The website displayed the real credentials and employment history of Representative A and linked to Representative A's actual FINRA BrokerCheck website page.

64. Onyeachonam's phony website also listed an email address with Representative A's name as a contact method.

65. That email address, which Onyeachonam used to communicate with investors, had been set up using another email address attributable to

Onyeachonam.

66. In May 2020, Onyeachonam registered an LLC in the name of Representative A in the state of Colorado.

B. Defendants Promoted Representative A Online.

67. Onyeachonam, Asiegbu, and Nweke-Eze promoted Representative A using Google Ads, YouTube, and LinkedIn accounts, all of which directed potential investors to the Representative A website Onyeachonam had created.

68. On November 28, 2019, Onyeachonam opened a Google Ads account in the name of Representative A and listed his own name—"Chibuzo Onyeachonam"—as the contact person and his Nigerian address at the time as the postal address.

69. That day, email addresses attributable to Onyeachonam and Asiegbu began running ads on Google for Representative A stating, "[Representative A] is a Professional Investment Adviser, Expert Trader, Crypto Analyst, and a Financial Consultant."

70. The language in the Google ads was similar to the representations made on the phony Representative A website Onyeachonam had created.

71. The Google ads also linked to the phony Representative A website.

72. Email addresses attributable to Onyeachonam, Asiegbu, and Nweke-Eze also used fake identities to promote Representative A's trading and investment

services in comments to YouTube videos.

73. The comments took the form of a fictitious online conversation between strangers, one mentioning their investment success with Representative A and the other following up with questions about Representative A, concluding with an instruction from the purported Representative A client to look Representative A up on the Internet and call, email, or send a message.

74. The fictitious YouTube comments were scripted, and in emails between and among themselves (and others), Onyeachonam, Asiegbu, and Nweke-Eze emailed similar scripts used for another Representative Defendants impersonated.

75. An email address attributable to Onyeachonam also opened a LinkedIn account for Representative A that touted Representative A as a Financial Consultant at the firm for which Representative A genuinely worked.

C. A California Investor Found Representative A Online and Invested More Than $500,000.

76. An investor who at all relevant times has resided in California ("Investor A") learned about Representative A when someone in a Signal investor group chat circulated a link to YouTube comments touting Representative A's services.[2]

[2] Signal is an encrypted messaging app.

77. Investor A then found Representative A's fake website, reviewed Representative A's qualifications and licenses, and emailed the person Investor A thought was Representative A in August 2020 at the email address listed on the fake website that Onyeachonam had created.

78. On August 7, 2020, Onyeachonam sent an introductory email—purportedly from Representative A but actually from Onyeachonam—to Investor A asking where Investor A was located, what Investor A's experience was investing in financial markets, what his financial goals were, and how much Investor A had "set aside to achieve that financial goal."

79. In his email in response, Investor A said that he was a beginner in the financial market, he had only traded in foreign exchange, he had invested in other vehicles that provided a high annual yield, had about $40,000 to invest, and his goal was to obtain at least a 20% return on investment.

80. On August 14, 2020, Onyeachonam, again posing as Representative A, emailed Investor A and explained that Representative A traded across three major financial markets—the stock, foreign exchange, and digital currency markets—to maximize profit generation and that Representative A used a "copy trading" tool.

81. Onyeachonam's email further claimed that, after downloading and installing a list of trading apps, the client would create a trading account which the

trader would sync with a copy-trading tool to ensure that the client would be able to transparently view trading activity.

82. This email was identical to one that Onyeachonam sent to other potential investors who sought to invest through Representative A.

83. In August 2020, Onyeachonam, posing as Representative A, emailed Investor A a client investment form and a contract agreement.

84. The client investment form required Investor A to provide contact and background information, as well as information about his investing experience, financial assets, and investments.

85. The form claimed: "[Representative A] is a licensed Broker/Financial Adviser, regulated and accredited by the Financial Industry Regulatory Authority (FINRA) and Securities and Exchange Commission (SEC)[.] [Representative A] is therefore operating within the boundaries of [Representative A's] profession and the data you will provide below will be used for only investment purposes."

86. The contract agreement further represented that Investor A was required to pay a "10% commission fee" and a "one time payment of 5% insurance premium to protect your investment against any loss ascribable to market crash or fluctuation."

87. The contract agreement also promised that "the investment accounts would accrue a minimum of 15% profits monthly."

88. Investor A filled out the client investment form, signed the contract agreement, and returned both to Onyeachonam through the email address Onyeachonam had created and that purported to be Representative A's email address.

89. In August 2020, Onyeachonam, posing as Representative A, instructed Investor A to download and sign up for accounts at an SEC-registered broker-dealer, a platform for trading currency, and two crypto asset trading platforms and to set up a call so that Representative A could sync Investor A's accounts with Representative A's copy trading tool and discuss funding and investments.

90. On August 23, 2020, Onyeachonam, posing as Representative A, initiated a WhatsApp text conversation with Investor A.

91. Onyeachonam, posing as Representative A, and Investor A thereafter communicated primarily through WhatsApp messages.[3]

92. On August 26, 2020, Onyeachonam, posing as Representative A, messaged Investor A through WhatsApp and claimed that, to maximize profit realization, Investor A's capital would be split between the stock market and crypto asset market at a "11:89 ratio" for the first three weeks of trading due to the bullish state of the crypto asset market.

[3] WhatsApp is an encrypted messaging service.

93. On August 26, 2020, Onyeachonam, posing as Representative A, instructed Investor A to make an initial deposit of $1,200 in Investor A's newly-opened (genuine) brokerage account and $8,800 in Investor A's crypto asset account, to use the funds in the crypto asset account to purchase bitcoin, and to transfer the bitcoin to an address Investor A had set up at a crypto-asset trading platform pursuant to Onyeachonam's instructions.

94. In September 2020, following the instructions of Onyeachonam posing as Representative A, Investor A purchased bitcoin in his crypto asset account and transferred approximately $10,108.92 to an address Investor A had set up at a crypto-asset trading platform.

95. Investor A then told Onyeachonam, whom Investor A understood to be Representative A, that Investor A had sent the bitcoin to his address at a crypto-asset trading platform.

96. Onyeachonam, posing as Representative A, responded that she would start trading as soon as possible.

97. After transferring the initial investment, Investor A asked whether Representative A would be trading the funds in Investor A's (genuine) brokerage account, and Onyeachonam, posing as Representative A, replied affirmatively.

98. Onyeachonam, posing as Representative A, then emailed Investor A that his funds had been "uploaded to [Representative A's] copy trading system"—

the CopyTradeApp Onyeachonam had created, where Investor A could see his purported investment returns—and provided a link and login credentials to LumenTrades.com, the fake investment account platform Onyeachonam had also created.

99. The LumenTrades.com website displayed Investor A's investment and the purported trading returns, which appeared to be substantial.

100. After Onyeachonam secured Investor A's initial investment and Investor A saw the significant fictitious profits that Representative A was purportedly generating, Onyeachonam, posing as Representative A, succeeded in getting Investor A to transfer an additional $518,923.07, including funds gathered from friends and a loan from a financial institution, in purported investment funds over the next four months.

101. Onyeachonam, posing as Representative A, used various techniques to extract additional funds from Investor A in addition to the fake returns on LumenTrades: Onyeachonam (1) promoted new trading strategies that required additional funds to garner high returns; (2) repeatedly reminded Investor A that the crypto asset market was doing well; (3) touted Representative A's expertise, service, and trading success; and (4) encouraged Investor A to shift assets away from another investment adviser.

102. By the end of December 2020, the LumenTrades.com website showed

that Investor A's $518,299 net investment (after purported transaction fees) had purportedly earned $1,893,378 in net trading profits—a purported return of more than 250% in approximately four months.

103. Those earnings were fake, as Defendants had never actually invested Investor A's money as promised but had instead misappropriated it.

D. Onyeachonam Gave Investor A the Runaround When He Attempted to Withdraw Funds.

104. By late December 2020, Investor A's bitcoin had been moved from Investor A's crypto-asset trading platform address through several other addresses, and Defendants had thereby stolen the bitcoin.

105. On December 29, 2020, Investor A instructed Representative A (in reality, Onyeachonam) to withdraw his entire portfolio on January 1, 2021, and asked for withdrawal instructions, because he needed to pay back the individuals who had given Investor A money to invest.

106. The same day, Onyeachonam, posing as Representative A, responded, "Got it, [Investor A]."

107. Between December 29, 2020, and January 2, 2021, Investor A repeatedly messaged Representative A (in reality, Onyeachonam) on WhatsApp regarding Investor A's funds.

108. On January 2, 2021, Investor A stated, "[Representative A] I haven't heard back from you, I don't know where you are but please respond ASAP. I

need to move out the funds. I'm already late and they expected it Jan 1[.]"

109. On January 3, 2021, Onyeachonam, posing as Representative A, finally responded, "Hi [Investor A], Happy new year[.] I'm here."

110. On January 3, 2021, Investor A and Onyeachonam, posing as Representative A, messaged back and forth for approximately an hour. Investor A reiterated that he needed to withdraw his funds, and Onyeachonam, posing as Representative A, responded, "I will start processing it tomorrow."

111. When Investor A asked how many days it would take, Onyeachonam, posing as Representative A, responded, "3 business days."

112. Investor A and Onyeachonam, posing as Representative A, then turned their messages to the crypto market and the price of bitcoin.

113. Onyeachonam, posing as Representative A, reminded Investor A of Representative A's prediction that the price of bitcoin would "hit at least 25k before the last days of 2020," and Investor A responded, "You were right."

114. On January 6, 2021, Investor A asked Onyeachonam, posing as Representative A, whether the withdrawal had been processed.

115. On January 7, 2021, Onyeachonam, posing as Representative A, responded, "[Y]our funds are now available for withdrawal. Go to the investment page at Lumentrades and click withdraw."

116. Later the same day, Investor A asked how long it would take for the

funds to go from LumenTrades to Investor A's address once Investor A hit the withdraw button.

117. Onyeachonam, posing as Representative A, responded, "By the end of business day."

118. On January 8, 2021, Investor A messaged Representative A (in reality, Onyeachonam) stating that Investor A had not received his funds and that the LumenTrades website was down.

119. That day, Onyeachonam, posing as Representative A, responded, "You just placed a withdrawal yesterday, it will take 3 business days to complete," "I just saw that their site is down for maintenance," and "[t]hey will process your withdrawal."

120. Investor A reminded Representative A (in reality, Onyeachonam), "Oh you told me by the end of the business day."

121. Onyeachonam did not respond to that message.

122. On January 11, 2021, Onyeachonam, posing as Representative A, messaged Investor A that "Lumentrades is working on some features[;] that's why there is a little delay in withdrawal."

123. Investor A responded, "Ok thank you so much," and asked how long Representative A thought it would take.

124. Onyeachonam did not respond.

125. The same day, Investor A informed Representative A (in reality, Onyeachonam) that several people were upset with him, he was worried and anxious, his life would be destroyed, and his family and friends were close to killing him because he had not returned their money.

126. Onyeachonam, posing as Representative A, responded that Investor A would receive his funds soon and everything was going well.

127. Later the same day, Onyeachonam, posing as Representative A, told Investor A that his funds would be available two days later—by Wednesday, January 13, 2021.

128. On January 13, 2021, Investor A did not receive his funds.

129. Investor A messaged Representative A (in reality, Onyeachonam) regarding withdrawal.

130. On January 14, 2021, Onyeachonam, posing as Representative A, told Investor A that LumenTrades is on it, "[t]hey are updating their services," and that Investor A's funds would be available the next day.

131. On or around January 18, 2021, someone purporting to be from LumenTrades contacted Investor A and told him to pay additional money to receive a bonus.

132. On January 18, 2021, Investor A informed Representative A (in reality, Onyeachonam) about the LumenTrades call and said that he did not have

any more money and was "drained" and "basically bankrupt."

133. Onyeachonam, posing as Representative A, responded, "[P]lease follow the instruction on Lumentrades[.] . . . I did my best for you and you don't want to follow simple instruction[ ] to withdraw your funds[?]"

134. Investor A replied, "Lumentrades has no location, no real phone number, it's not a real exchange anywhere. They got my name spelled wrong in most of their emails . . . it's not legitimate."

135. On January 18, 2021, in Investor A's final WhatsApp message to Onyeachonam, Investor A stated, "Be honest with me. I figured it out by now that you are not who you pose to be on the website."

136. Investor A then posed one final question: "How do you sleep at night knowing you're destroying the lives of people who trust you[?]"

137. Investor A received no response to his message.

138. Nor did Investor A ever receive any funds or other assets back from Defendants.

139. Between August and December 2022, Defendants stole $529,031.99 from Investor A.

III. ONYEACHONAM AND ASIEGBU IMPERSONATED A FORMER REGISTERED REPRESENTATIVE FROM TEXAS, AND DEFENDANTS STOLE MORE THAN $55,000 FROM AN ARIZONA INVESTOR.

A. Onyeachonam and Asiegbu Impersonated a Former Texas Representative Online.

140. In April 2020, an unknown individual or individuals set up a website impersonating a former Texas-based broker-dealer and investment adviser Representative ("Representative B") previously employed by a large, dually registered broker-dealer and investment adviser firm that was a household name.

141. By 2020, Representative B had had 36 years of experience as a broker-dealer representative and/or investment adviser representative during his career.

142. In April 2020, an unknown individual or individuals registered a domain name with Representative B's actual first and last names.

143. An unknown individual or individuals also created a website on that domain that advertised Representative B's financial services.

144. The website displayed the real credentials and employment history of Representative B and linked to Representative B's actual FINRA BrokerCheck website page.

145. The phony website also listed an email address with Representative B's name as a contact method.

146. As early as May 2020, email account information indicates that Asiegbu and Onyeachonam controlled that email address, which was used to communicate with their investor victims.

147. Additionally, Asiegbu maintained a Google Search Console account, a tool that helps website owners and developers understand how their site appears in Google Search results, for the phony website.

148. In February 2021, Onyeachonam and/or Asiegbu purchased via an email address attributable to both of them a SSL certificate, a digital file that verifies a website's identity and encrypts communication between a web browser and a web server, for the phony website.

149. In June 2021, Onyeachonam registered an LLC in the name of Representative B in the state of Delaware.

B. Nweke-Eze Promoted Representative B Online.

150. Starting in at least July 2020, an email address attributable to Nweke-Eze used fake identities to promote Representative B's trading and investment services in comments to YouTube videos.

151. The comments took the form of a fictitious online conversation between strangers, one mentioning their investment success with Representative B and the other following up with questions about Representative B, concluding with an instruction from the purported Representative B client to look Representative B

up on the Internet and call, email, or send a message.

152. The fictitious YouTube comments were scripted, and in emails sent to himself and others potentially involved in the fraud, Nweke-Eze emailed similar scripts used for another representative Defendants impersonated.

C. An Arizona Investor Found Representative B Online and Invested More Than $55,000.

153. An investor who at all relevant times has resided in Arizona ("Investor B") learned about Representative B through comments made on YouTube touting Representative B's services.

154. Investor B then found Representative B's fake website, controlled by Asiegbu, and emailed Representative B in August 2020 using the email address listed on the fake website.

155. Investor B noted in his email that he had "heard good reviews about the services you provided to others."

156. On August 11, 2020, Onyeachonam and/or Asiegbu, posing as Representative B, sent an introductory email—purportedly from Representative B but actually from an email address attributable to Onyeachonam and Asiegbu—to Investor B asking where Investor B was located, what Investor B's experience was investing in financial markets, what his financial goals were, and how much Investor B had "set aside to achieve that financial goal."

157. In response, Investor B said that he was a beginner in the financial

market, he had made some trades and investments that had turned out poorly, he had about $130,000 in savings but did not want to invest all of it, and his goal was to earn enough to buy a property or invest in a business.

158. On August 13, 2020, Onyeachonam and/or Asiegbu, again posing as Representative B, emailed Investor B and claimed that Representative B traded across three major financial markets—the stock, foreign exchange, and digital currency markets—to maximize profit generation and that Representative B used a "copy-trading" tool.

159. The email from Onyeachonam and/or Asiegbu further claimed that, after downloading and installing a list of trading apps, the client would create a trading account which the trader would sync with a copy-trading tool to ensure that the client would be able to transparently view trading activity.

160. In August 2020, Onyeachonam and/or Asiegbu, posing as Representative B, emailed Investor B a client investment form and a contract agreement.

161. Both the client investment form and the contract agreement included seals for the SEC and FINRA BrokerCheck.

162. The client investment form required Investor B to provide contact and background information, as well as information about his investing experience, financial assets, and investments.

163. The form claimed: "[Representative B] is a licensed Broker/Financial Adviser, regulated and accredited by the Financial Industry Regulatory Authority (FINRA) and Securities and Exchange Commission (SEC)[.] [Representative B] is therefore operating within the boundaries of [Representative B's] profession and the data you will provide below will be used for only investment purposes."

164. The contract agreement further represented that Investor B was required to pay a "10% commission fee" and a "one time payment of insurance premium to protect your investment against any loss ascribable to market crash or fluctuation."

165. The contract agreement also promised that "the investment accounts would accrue a minimum of 15% profits monthly."

166. Investor B filled out the client investment form, signed the contract agreement, and returned both to Onyeachonam and/or Asiegbu through the email address they controlled that purported to be Representative B's address.

167. In August 2020, Onyeachonam and/or Asiegbu, again posing as Representative B, instructed Investor B via email to download and sign up for accounts at two SEC-registered broker-dealers, a platform for trading currency, and two crypto asset trading platforms, and to set up a call so that Representative B could sync Investor B's accounts with Representative B's copy trading tool and discuss funding and investments.

168. In September 2020, Onyeachonam and/or Asiegbu, posing as Representative B, emailed Investor B a strategy document regarding a "bitcoin pump opportunity."

169. An email address Onyeachonam and Asiegbu controlled contained a Google Drive file with a similar document, dated March 24, 2021, with identical letterhead and Representative B's fake contact information.

170. On September 1, 2020, Onyeachonam and/or Asiegbu, posing as Representative B, emailed Investor B and claimed that, to maximize profit realization, Investor B's capital would be split between the stock market and crypto asset market at a "19:81 ratio" for the first three weeks of trading due to the bullish state of the crypto asset market.

171. Representative B instructed Investor B to make an initial deposit of $5,700 in Investor B's newly-opened (genuine) brokerage account and $24,300 in Investor B's crypto asset account.

172. On September 14, 2020, Onyeachonam, posing as Representative B, initiated a WhatsApp text conversation with Investor B.

173. Onyeachonam, posing as Representative B, and Investor B thereafter communicated primarily through WhatsApp messages.

174. In September 2020, following the instructions from Onyeachonam, posing as Representative B, Investor B purchased bitcoin in his crypto asset

account and transferred approximately $20,382.97 in bitcoin to an address Investor B had set up at a crypto-asset trading platform.

175. Investor B was unable to set up the (genuine) brokerage account Onyeachonam, posing as Representative B, had instructed him to set up because Investor B needed additional documentation.

176. Onyeachonam and/or Asiegbu, posing as Representative B, then emailed Investor B that his funds had been "uploaded to [Representative B's] copy trading system"—the CopyTradeApp Onyeachonam had created, where Investor B could see his purported investment returns—and provided a link and login credentials to LumenTrades.com, the fake investment account platform Onyeachonam had also created.

177. The LumenTrades.com website displayed Investor B's investment and the purported trading returns from Representative B.

178. After Onyeachonam and/or Asiegbu secured Investor B's initial investment and Investor B saw the significant fictitious profits that Representative B was purportedly generating, Onyeachonam and/or Asiegbu, posing as Representative B, succeeded in getting Investor B to transfer an additional $37,811.92.

179. Onyeachonam and/or Asiegbu, posing as Representative B, used various techniques to extract additional funds from Investor B in addition to the

fake returns on LumenTrades: Onyeachonam and/or Asiegbu (1) promoted new trading strategies, which they informed Investor B required additional funds to garner high returns; (2) repeatedly reminded Investor B that the crypto asset market was doing well; (3) touted Representative B's expertise, service, and trading success; and (4) reminded Investor B of his financial goals (buying real property).

180. Defendants never invested Investor B's money as promised but instead misappropriated it.

D. Onyeachonam Gave Investor B the Runaround When He Attempted to Withdraw Funds.

181. By October 27, 2020, Investor B's bitcoin had been moved from Investor B's crypto-asset trading platform address through several addresses, and Defendants thereby stole it.

182. Starting on November 29, 2020, Investor B informed Representative B (in reality, Onyeachonam) via WhatsApp that he wanted to withdraw $30,000 and asked how to make a withdrawal.

183. Onyeachonam, posing as Representative B, messaged Investor B and asked when he planned to make the withdrawal.

184. Investor B responded, "In the next week or two, if possible. I got pretty sick and racked up some medical bills."

185. Representative B (in reality, Onyeachonam) replied, "Okay. Let me

know when you're ready."

186. On December 5, 2020, Investor B messaged the person he thought was Representative B: "I tried making a withdrawal from the lumentrades [website] and it wasn't working for me. What's the best route to go to get some [of] that profit out."

187. Onyeachonam, posing as Representative B, responded, "I will contact them and have it processed soon."

188. Between December 6, 2020, and December 21, 2020, Investor B repeatedly messaged Representative B (in reality, Onyeachonam) on WhatsApp regarding withdrawing Investor B's funds.

189. At various times in December 2020, Onyeachonam, posing as Representative B, told Investor B, "I'm trying to close some position[s] so I can process your withdrawal;" "You can withdraw it from Lumentrades but I still hold some positions that I need to liquidate. By Monday your funds will be available for withdrawal;" "You will be able [] to withdraw today. The funds are available;" and "go ahead and withdraw from your account at Lumentrades."

190. Investor B was never able to withdraw any of his funds from LumenTrades.

191. On January 2, 2021, Investor B messaged Representative B, "Whats the deal with withdrawals. Submitted it the 21st and its still pending."

192. Onyeachonam, posing as Representative B, replied, "I will contact them and get back to you."

193. On January 4, 2021, the purported "Lumentrades Billing Team" emailed Investor B from an email address created and controlled by Onyeachonam, "We sincerely apologise [sic] for the delay in withdrawal. We are updating our terms and functionalities. Your funds will be available tomorrow."

194. On January 15, 2021, the same email address emailed Investor B writing, "We have fully updated our terms and functionalities. You can now withdraw your investment and have it available in your account today."

195. Investor B never received any funds or other assets back from Defendants.

196. Between September and October 2020, Defendants stole $58,194,89 from Investor B.

IV. DEFENDANTS IMPERSONATED A REGISTERED REPRESENTATIVE FROM MINNESOTA AND STOLE MORE THAN $105,000 FROM A CALIFORNIA INVESTOR.

A. Asiegbu and Nweke-Eze Impersonated a Minnesota Representative Online.

197. In October 2020, an unknown individual or individuals set up a website impersonating a Minnesota-based broker-dealer and investment adviser Representative ("Representative C") employed by a large, dually registered broker-dealer and investment adviser firm that was a household name.

198. In 2020, Representative C had 13 years of experience as a broker-dealer representative and/or investment adviser representative.

199. In October 2020, an unknown individual or individuals registered a domain name with Representative C's actual first and last names.

200. An unknown individual or individuals created a website on that domain that advertised Representative C's financial services.

201. The website displayed the real credentials and employment history of Representative C and linked to Representative C's actual FINRA BrokerCheck website page.

202. The phony website also listed an email address with Representative C's name as a contact method.

203. That email address, used to communicate with Defendants' investor victims, was controlled by Asiegbu starting in at least November 2020 and by Nweke-Eze starting in at least June 2021.

204. Starting at least the day after the phony website's domain name was registered, Asiegbu controlled the website. For example, he set up and maintained through at least September 2021 a webhosting account for the domain—a service that stores and maintains a website's files and applications on a server so that it can be accessed on the internet. Webhosts are responsible for the technical aspects of a website's operation, including keeping the server running, implementing security

measures, and ensuring that files are transferred to visitors' browsers.

205. In June 2021, Onyeachonam registered an LLC in the name of Representative C in the state of Delaware.

B. Nweke-Eze Promoted Representative C Online.

206. Nweke-Eze promoted Representative C using YouTube, which directed potential investors to research Representative C.

207. Starting in at least November 2020, an email address attributable to Nweke-Eze used fake identities to promote Representative C's trading and investment services in comments to YouTube videos.

208. The comments took the form of a fictitious online conversation between strangers, one mentioning their investment success with Representative C and the other following up with questions about Representative C, concluding with an instruction from the purported Representative C client to look Representative C up on the Internet and call, email, or send a message.

209. The fictitious YouTube comments were scripted, and in emails sent to himself and others, Nweke-Eze emailed similar scripts used for another representative Defendants impersonated.

C. A California Investor Found Representative C Online and Invested More Than $105,000.

210. An investor who at all relevant times has resided in California ("Investor C") learned about Representative C through comments made on

YouTube touting Representative C's services.

211. Investor C then found Representative C's fake website, which Asiegbu controlled, and sent Representative C a message in June 2021 using the form on the website.

212. On June 23, 2021, Asiegbu and/or Nweke-Eze sent an introductory email—purportedly from Representative C but actually from an email address attributable to Asiegbu and Nweke-Eze—to Investor C asking where Investor C was located, what Investor C's experience was investing in financial markets, what her financial goals were, and how much Investor C had "set aside to achieve that financial goal." Asiegbu and/or Nweke-Eze used the email address they controlled that purported to be Representative C's address.

213. In response, Investor C said that she was a beginner in the financial market, she was interested in a balanced portfolio that provided monthly cashflow as well as long term growth, and she had $30,000 to invest and would like to increase the amount over time.

214. On June 28, 2021, Asiegbu and/or Nweke-Eze, again posing as Representative C, emailed Investor C and claimed that Representative C traded across three major financial markets—the stock, foreign exchange, and digital currency markets—to maximize profit generation and that Representative C used a "copy trading" tool.

215. The email further claimed that, after downloading and installing a list of trading apps, the client would create a trading account which the trader would sync with a copy-trading tool to ensure that the client would be able to transparently view trading activity.

216. Attached to the email was a document titled, "Portfolio Management Business Model."

217. The Portfolio Management Business Model included the seals for the SEC and FINRA BrokerCheck.

218. The Portfolio Management Business Model claimed, "[Representative C] is a licensed and regulated broker/portfolio manager with over 20 years of experience working with notable financial/investment firms in the United States."

219. The document also claimed that Representative C "guaranteed [a] monthly capital gain of 15-25%" and charged a 5-10% "performance fee or trade commission" and a 5% "insurance premium" to "insure investor's funds against losses."

220. In July 2021, Asiegbu and/or Nweke-Eze, posing as Representative C, emailed Investor C a client investment form and a contract agreement.

221. Both the client investment form and contract agreement included the seals for the SEC and FINRA BrokerCheck.

222. The client investment form was identical to one that an email address

associated with Onyeachonam and Asiegbu had emailed to support@lumentrades.com three months earlier, on March 24, 2021.

223. The client investment form required Investor C to provide contact and background information, as well as information about her investing experience, financial assets, and investments.

224. The form claimed: "[Representative C] is a licensed Broker/Financial Adviser, regulated and accredited by the Financial Industry Regulatory Authority (FINRA) and Securities and Exchange Commission (SEC)[.] [Representative C] is therefore operating within the boundaries of [Representative C's] profession and the data you will provide below will be used for only investment purposes."

225. The contract agreement further represented that Investor C was required to pay a "5% commission fee" and a "one-time payment of insurance premium to protect your investment against any loss ascribable to market crash or fluctuation."

226. The contract agreement also promised that "the investment accounts would accrue a minimum of 15% profits monthly."

227. Investor C filled out the client investment form, signed the contract agreement, and returned both to Asiegbu and/or Nweke-Eze through the email address that they controlled and that purported to be Representative C's email address.

228. In July 2021, Asiegbu and/or Nweke-Eze, posing as Representative C, instructed Investor C to download and sign up for accounts at two SEC-registered broker-dealers, a platform for trading currency, and two crypto asset trading platforms and to set up a call so that Representative C could sync Investor C's accounts with Representative C's copy trading tool and discuss funding and investments.

229. On July 8, 2021, Onyeachonam, posing as Representative C, initiated a WhatsApp text conversation with Investor C.

230. Representative C and Investor C thereafter communicated primarily through WhatsApp messages.

231. On July 19, 2021, Asiegbu and/or Nweke-Eze, posing as Representative C, emailed Investor C and claimed that, to maximize profit realization, Investor C's capital would be split between the stock market and crypto asset market at a "10:90 ratio" for the first three weeks of trading due to the bullish state of the crypto asset market.

232. Representative C (in reality, Asiegbu and/or Nweke-Eze) instructed Investor C to make an initial deposit of $2,000 in Investor C's newly-opened (genuine) brokerage account and $18,000 in Investor C's crypto asset account.

233. In July 2021, following these instructions, Investor C purchased bitcoin in her crypto asset account and transferred $19,005.17 in bitcoin to an

address Investor C had set up at a crypto-asset trading platform.

234. Investor C also deposited $2,000 into her (genuine) brokerage account.

235. On July 24, 2021, Onyeachonam, posing as Representative C, messaged Investor C claiming that Representative C would "start trading in your account today."

236. Asiegbu and/or Nweke-Eze, posing as Representative C, then emailed Investor C that her funds had been "uploaded to [Representative C's] copy trading system"—the CopyTradeApp Onyeachonam had created, where Investor C could see his purported investment returns—and provided a link and login credentials to LumenTrades.com, the fake investment account platform Onyeachonam had also created.

237. The LumenTrades.com website displayed Investor C's investment and the purported trading returns from Representative C, which appeared to be substantial.

238. Onyeachonam, posing as Representative C, and Investor C arranged a call via WhatsApp for August 19, 2021, at 9 a.m. Pacific Time to discuss a "new strategy" for investment.

239. Indeed, Onyeachonam's scheduling app listed a call on August 19, 2021, at 9 a.m. Pacific Time and described "Chibuzo [Onyeachonam]'s task" as to

"Call [Investor C's first name] • [Representative C's first name] Project."

240. After Defendants secured Investor C's initial investment and Investor C saw the significant fictitious profits that Representative C was purportedly generating, Defendants, posing as Representative C, succeeded in getting Investor C to transfer an additional $82,011.90 in purported investment funds over the next five months.

241. Defendants, posing as Representative C, used various techniques to extract additional funds from Investor C in addition to the fake returns on LumenTrades: Defendants (1) promoted new trading strategies that required additional funds to garner high returns; and (2) promised Investor C that, if she invested additional funds, she would be able to take monthly withdrawals without affecting the trading strategy.

242. Defendants never invested Investor C's money as promised but instead misappropriated it.

243. On December 2, 2021, Investor C asked Representative C for an "alternate contact" in case Investor C was unable to get a hold of Representative C.

244. Onyeachonam, posing as Representative C, responded that the firm would have its assistant "Susan" reach out.

245. On December 3, 2021, someone posing as "Susan Olsen," a fictitious individual with a LumenTrades.com email address, reached out to Investor C,

stating "You can reach out to me whenever you have any questions or difficulty with your account."

246. The same day, an email address attributable to Onyeachonam received identical draft correspondence from "Susan Olsen."

247. Investor C and Onyeachonam, posing as Representative C, discussed investing in the stock market.

248. On December 15, 2021, Onyeachonam, posing as Representative C, messaged Investor C, "I will start trading the funds [in Investor C's genuine brokerage account] as soon as possible."

249. Investor C responded, "awesome thanks for confirming."

250. Defendants never traded the funds in Investor C's genuine brokerage account.

D. Onyeachonam Gave Investor C the Runaround and Charged Additional Fees When She Attempted to Withdraw Funds.

251. By March 1, 2022, Investor C's bitcoin had been moved from Investor C's crypto-asset trading platform address through several addresses, and Defendants had stolen the bitcoin.

252. On March 1, 2022, Investor C messaged Representative C, "How do I withdraw my monthly gain?"

253. Representative C did not respond.

254. Investor C messaged Representative C several times throughout

March 2022, noted that her emails to Representative C were "getting bounced," and yet did not receive a response.

255. On June 29, 2022, Onyeachonam, posing as Representative C, messaged Investor C, claiming that Representative C had been sick the last few months and therefore had not responded to any of Investor C's messages.

256. Later in the conversation, Onyeachonam claimed that Investor C "needed to buy ethereum to pay the processing fee," and after doing so "[Investor C's] funds will be available to [withdraw]."

257. Investor C responded, "[A]re you sure they will release funds after I give processing fees?"

258. Representative C replied, "Yes, that's how it work[s]."

259. Following instructions from Onyeachonam, posing as Representative C, Investor C used funds in her crypto asset account to purchase ethereum and transferred $2,222.16 in ethereum to an address displayed for Investor C on Secawallet.com, which Onyeachonam set up, controlled, and operated.

260. Indeed, the address displayed for Investor C on Secawallet.com appeared several times in Onyeachonam's emails.

261. The next day, June 30, 2022, Investor C reported to Representative C that LumenTrades was now stating she needed to pay an advisory fee of approximately $8,000 to "unlock [her] funds."

262. Onyeachonam, posing as Representative C, told Investor C that "It's included in the contract."

263. Investor C responded, "in any case I don't have that kind of funds right now…."

264. On September 16, 2022, Investor C asked Representative C, "Is there any other fees after [the processing fees already paid] and your fees?"

265. Onyeachonam, posing as Representative C, responded, "Hi [Investor C], there is no other fees…. Once the pending payment is cleared, your funds will be automatically available."

266. On September 16, 2022, Investor C used funds in her crypto asset account to purchase ethereum and transferred $3,161.31 in ethereum to the same Secawallet.com address for Investor C previously described in paragraph 259 above.

267. On September 19, 2022, Onyeachonam, posing as Representative C, messaged Investor C, "[T]he payment has been confirmed. You can login to secawallet to withdraw your funds."

268. Investor C was still unable to withdraw her funds, and on September 26, 2022, Investor C messaged Representative C, "[Lumentrades] support is saying it's stuck because there is [not] enough processing fees. Did you know about it?"

269. The next day, Onyeachonam, posing as Representative C, responded,

"[P]lease follow the instruction from Lumentrades. I can't change anything at this point."

270. On September 29, 2022, Investor C received an email from support@secawallet.com informing Investor C that Secawallet had "started processing [Investor C's] stuck transaction."

271. On September 30, 2022, Investor C messaged Representative C, "I am worried and stressed."

272. Onyeachonam, posing as Representative C, responded, "I'm sorry about the stress. Everything should be settled today."

273. Investor C received no further communications from Representative C.

274. Investor C continued communicating with support@secawallet.com between September 2022 and February 2023.

275. During that period, Onyeachonam, posing as a support representative from Secawallet, instructed Investor C to provide certain documents to complete an "identity verification" process, citing "many unusual activities on your account."

276. Investor C complied by providing support@secawallet.com with scans of Investor C's driver's license, utility bill, and United States passport.

277. On October 14, 2022, Onyeachonam, posing as a support

representative with Secawallet, emailed Investor C, "For security reasons, we won't be able to release the funds to the provided [crypto] address."

278. The purported support representative with Secawallet (in reality, Onyeachonam) directed Investor C to purchase a hardware wallet, a physical device that stores crypto assets offline, from shop.secawallet.com and told Investor C that this hardware wallet would be mailed to her physical address.

279. Two days later, Investor C responded, "Kindly please release the funds, this looks more like a scam to me now."

280. On November 7, 2022, Onyeachonam, posing as a support representative with Secawallet, emailed Investor C a formal invoice for the hardware wallet that listed its price as $899.99.

281. Investor C continued exchanging emails regarding the hardware wallet with Onyeachonam, while he was posing as a support representative with Secawallet, until February 22, 2023.

282. On that date, Onyeachonam, still posing as the Secawallet support representative, sent Investor C an email stating, "Once we receive your payment, your hardware wallet will be shipped to your location."

283. Investor C received no further communications from support@secawallet.com.

284. Nor did Investor C ever receive any funds or other assets back from

Defendants.

285. Between July 2021 and September 2022, Defendants stole $106,400 from Investor C.

V. ONYEACHONAM AND ASIEGBU IMPERSONATED A REGISTERED REPRESENTATIVE FROM CALIFORNIA AND STOLE MORE THAN $45,000 FROM A NEW JERSEY INVESTOR.

A. Onyeachonam and Asiegbu Impersonated a California Representative Online.

286. In October 2020, an unknown individual or individuals set up a website impersonating a California-based broker-dealer and investment adviser representative ("Representative D") employed by a large, dually registered broker-dealer and investment adviser firm that was a household name.

287. In 2020, Representative D had 22 years of experience as a broker-dealer representative and/or investment adviser representative.

288. In October 2020, an unknown individual or individuals registered a domain name with Representative D's actual first and last names.

289. An unknown individual or individuals then created a website on that domain that advertised Representative D's financial services.

290. Asiegbu controlled the phony website starting in at least October 2020, and Onyeachonam controlled it starting in at least August 2021. For example, Asiegbu maintained hosting accounts for the phony website, and Onyeachonam maintained an account at an email delivery service that allowed

email messages to be generated from the phony website.

291. The phony website displayed the real credentials and employment history of Representative D and linked to Representative D's actual FINRA BrokerCheck website page.

292. The phony website also listed an email address with Representative D's name as a contact method.

293. That email address, used to communicate with investor victims, was controlled by Asiegbu since at least March 2021 and by Onyeachonam since at least April 2022.

294. In June 2021, Onyeachonam registered an LLC in the name of Representative D in the state of Delaware.

B. Onyeachonam and Asiegbu Promoted Representative D Online.

295. As of March 2022, an email address attributable to Onyeachonam and Asiegbu used fake identities to promote Representative D's trading and investment services in comments to YouTube videos.

296. The comments took the form of a fictitious online conversation between strangers, one mentioning their investment success with Representative D and the other following up with questions about Representative D, concluding with an instruction from the purported Representative D client to look Representative D up on the Internet and call, email, or send a message.

297. The fictitious YouTube comments were scripted, and in emails between and among themselves and others, Onyeachonam and Asiegbu emailed similar scripts used for another representative Defendants impersonated.

C. A New Jersey Investor Found Representative D Online and Invested More Than $45,000.

298. An investor who at all relevant times has resided in New Jersey ("Investor D") learned about Representative D through comments made on YouTube touting Representative D's services.

299. Investor D then found Representative D's fake website (in reality, controlled by Asiegbu and Onyeachonam) and sent Representative D a message in February 2022 using the form on the website.

300. On February 9, 2022, Asiegbu and/or Onyeachonam sent an introductory email—purportedly from Representative D but actually from Asiegbu and/or Onyeachonam—to Investor D asking where Investor D was located, what Investor D's experience was investing in financial markets, what his financial goals were, and how much Investor D had "set aside to achieve that financial goal."

301. To send the email, Asiegbu and/or Onyeachonam used the email address they controlled that purported to be Representative D's address, and Representative D's purported email signature block included the seals for both the SEC and FINRA BrokerCheck.

302. In response, Investor D said that he had been investing for the last five years, had $25,000 to invest, and that his goal was to have steady monthly side income.

303. On February 10, 2022, Asiegbu and/or Onyeachonam, again posing as Representative D, emailed Investor D and claimed that Representative D traded across three major financial markets—the stock, foreign exchange, and digital currency markets—to maximize profit generation and that Representative D used a "copy trading" tool.

304. The email further claimed that, after downloading and installing a list of trading apps, the client would create a trading account which the trader would sync with a copy-trading tool to ensure that the client would be able to transparently view trading activity.

305. This email was identical to one that Asiegbu and/or Onyeachonam sent to other potential investors who sought to invest through Representative D.

306. In February 2022, Asiegbu and/or Onyeachonam, posing as Representative D, emailed Investor D a client investment form and a contract agreement.

307. The client investment form required Investor D to provide contact and background information, as well as information about his investing experience, financial assets, and investments.

308. The form claimed: "[Representative D] is a licensed Broker/Financial Adviser, regulated and accredited by the Financial Industry Regulatory Authority (FINRA) and Securities and Exchange Commission (SEC)[.] [Representative D] is therefore operating within the boundaries of [Representative D's] profession and the data you will provide below will be used for only investment purposes."

309. Investor D filled out the client investment form, signed the contract agreement, and returned both to the email address that purported to be Representative D's email address.

310. In February 2022, Asiegbu and/or Onyeachonam, posing as Representative D, instructed Investor D to download and sign up for accounts at two SEC-registered broker-dealers, a platform for trading currency, two crypto asset trading platforms, and LumenTrades.com and to set up a call so that Representative D could sync Investor D's accounts with Representative D's copy trading tool and discuss funding and investments.

311. On February 19, 2022, Onyeachonam, posing as Representative D, initiated a WhatsApp text conversation with Investor D.

312. Onyeachonam, posing as Representative D, and Investor D thereafter communicated primarily through WhatsApp messages.

313. On February 24, 2022, Asiegbu and/or Onyeachonam, posing as Representative D, emailed Investor D; claimed that, to maximize profit realization,

Investor D's capital would be split between the stock market and crypto asset market at a "9:91 ratio" for the first three weeks of trading due to the bullish state of the crypto asset market; and instructed Investor D to make an initial deposit of $2,250 in Investor D's newly-opened (genuine) brokerage account and $22,750 in Investor D's crypto asset account.

314. In February and March 2022, following these instructions, Investor D purchased bitcoin in his crypto asset account and transferred $21,539.25 in bitcoin to an address Investor D had set up at a crypto-asset trading platform pursuant to instructions from Onyeachonam, posing as Representative D.

315. Investor D also deposited $2,500 into his (genuine) brokerage account.

316. On March 2, 2022, Investor D messaged Representative D (in reality, Onyeachonam) and asked, "[W]hat about [the genuine brokerage account]? I have $2,500 [in] it."

317. Onyeachonam, posing as Representative D, responded, "Yes, I will start trading the accounts at once."

318. Onyeachonam and Asiegbu never placed any trades in Investor D's genuine brokerage account.

319. On March 10, 2022, Onyeachonam, posing as Representative D, messaged Investor D, "I'm executing my first trade on your [crypto asset] account

today."

320. Investor D responded, "Awesome."

321. The LumenTrades.com website displayed Investor D's investment and the purported trading returns from Representative D.

322. On March 19, 2022, Investor D messaged Representative D, "I just logged [] into Lumentrades and saw you did trading yesterday and was able to make 17% profit in one day! That is awesome!"

323. After Onyeachonam secured Investor D's initial investment and Investor D saw the significant fictitious profits that Representative D was purportedly generating, Onyeachonam, posing as Representative D, succeeded in getting Investor D to transfer an additional $24,954.60 in purported investment funds in March 2022.

324. Onyeachonam and Asiegbu never invested Investor D's money as promised but instead misappropriated it.

325. On March 28, 2022, Investor D asked Representative D (in reality, Onyeachonam) if LumenTrades.com was "legit," because Investor D had sent an email to support@lumentrades.com and the email bounced back.

326. Onyeachonam, posing as Representative D, messaged Investor D, "They are doing scheduled maintenance. That's the reason for the delay…. Don't be worried, I got you as your investment advisor. You have to trust me as

investment advisor. I have your best interest at heart."

D. Onyeachonam and Asiegbu Gave Investor D the Runaround When He Attempted to Withdraw Funds.

327. By the end of March 2022, Investor D's bitcoin had been moved through several addresses, and Onyeachonam and Asiegbu had stolen it.

328. On March 28, 2022, Investor D asked Representative D (in reality, Onyeachonam) how to withdraw funds.

329. Onyeachonam, posing as Representative D, responded, "Let me know when [] you're ready to make a withdrawal. I have to close all the open positions in your account. And the funds will be available for withdrawal."

330. On March 30, 2022, Investor D messaged Representative D (in reality, Onyeachonam), "I would like to withdraw the profit at the end of the day tomorrow, Mar 31st."

331. Onyeachonam, posing as Representative D, did not respond.

332. Investor D sent Representative D (in reality, Onyeachonam) many messages over the next few days and did not receive a response.

333. On April 2, 2022, Investor D emailed Representative D (in reality, Onyeachonam), "I have tried to reach out on all possible ways. I don't understand why you don't reply to my messages? I'm again getting worried about the investment. I have also bought new home in Dallas and will need some profit we make for down payment."

334. Neither Onyeachonam nor Asiegbu, posing as Representative D, responded.

335. On April 6, 2022, Investor D messaged Representative D (in reality Onyeachonam), "[P]lease reply to me so that I don't doubt this to be a Fraud."

336. The next day, Onyeachonam, posing as Representative D, responded, "Please calm down. I'm working currently. I'm not 100% available to chat all the time but I will always make out time to communicate with my clients."

337. Investor D responded, "I understand you may have lots of clients. I just want you to understand my situation as it changed after we spoke. I bought a house in Dallas and counting on some profit I can take out for down payment."

338. Onyeachonam, posing as Representative D responded, "I will make the funds available for withdrawal. How much do you want to withdraw?"

339. Investor D responded, "[C]urrently it is showing me profit of $6,398. I just want to withdraw profit."

340. Onyeachonam, posing as Representative D, replied, "If you withdraw that amount it will halt my trading strategy but I can proceed to process the withdrawal if that's what you want."

341. Investor D asked follow up questions but received no response from Representative D.

342. Investor D messaged Representative D (in reality, Onyeachonam)

many times over the next two weeks asking about withdrawing his funds but received no response.

343. On April 21, 2022, Investor D messaged Representative D (in reality, Onyeachonam), "[D]on't make me believe it's a Fraud. I also called [Representative D's genuine employer]. I spoke to [another employee] and she told me you were just a Sales Associate."

344. Onyeachonam, posing as Representative D, replied, "I don't know why you're being insecure. I don't know why you called [Representative D's employer]. You're working with me independently…."

345. Investor D responded, "Because you are not replying to me. I want to take out profit as per our agreement. If I can't, then I want to just withdraw all my investment."

346. Onyeachonam, posing as Representative D, messaged back, "Alright, the funds will be available tomorrow."

347. The next day Investor D was unable to withdraw any money from his LumenTrades account, and his messages to Representative D that day and over the next six days went unanswered.

348. On April 29, 2022, Onyeachonam, posing as Representative D, messaged Investor D, "I'm trading. Relax, allow me to do my job."

349. Onyeachonam, posing as Representative D, then failed to respond to

any of Investor D's messages between April 29, 2022, and June 28, 2022, when Onyeachonam, posing as Representative D, messaged Investor D in part, "Your funds are ready," and instructed Investor D to create an account with Secawallet.com, which Onyeachonam set up, controlled, and operated.

350. After Investor D set up a Secawallet account, he messaged Representative D (in reality, Onyeachonam), "[I]t is asking me to send 2 [ethereum] to someone. Is that you?"

351. Onyeachonam, posing as Representative D, responded, "No, [it's] Lumentrades withdrawal processing fee."

352. Investor D did not pay the "processing fee."

353. On September 7, 2022, Investor D wrote to Representative D, "I don't want to pay anymore fees, you help me with the withdrawal. Let me know how I can withdraw."

354. Onyeachonam, posing as Representative D, responded (in his final WhatsApp message to Investor D), "[Y]ou need to pay the processing fee."

355. Investor D wrote back, "I will pay the fees when [investor D's money was withdrawn to a particular crypto asset platform]. I don't want to pay fees on any other sites. Please move the funds into [a particular crypto asset platform] and let me know when it's available."

356. Investor D received no response to his message.

`

357. Nor did Investor D ever receive any funds or other assets back from Onyeachonam and Asiegbu.

358. Onyeachonam and Asiegbu stole $46,493.95 from Investor D.

VI. ONYEACHONAM IMPERSONATED A REGISTERED REPRESENTATIVE FROM GEORGIA, AND ONYEACHONAM AND NWEKE-EZE STOLE MORE THAN $500,000 FROM A CALIFORNIA INVESTOR.

A. Onyeachonam Impersonated a Georgia Representative Online.

359. In November 2021, an unknown individual or individuals set up a website impersonating a broker-dealer and investment adviser Representative based in the State of Georgia ("Representative E") who was employed by a large, dually registered broker-dealer and investment adviser firm that is a household name.

360. In 2021, Representative E had 37 years of experience as a registered representative and/or investment adviser representative.

361. In November 2021, an unknown individual or individuals registered a domain name with Representative E's actual first and last names.

362. An unknown individual or individuals also created a website on that domain that advertised Representative E's financial services.

363. The phony website displayed the real credentials and employment history of Representative E and linked to Representative E's actual FINRA BrokerCheck website page.

`

364. The phony website listed an email address with Representative E's name as a contact method.

365. Onyeachonam controlled this email address, used to communicate with Defendants' investor victims, by at least February 2022.

366. The phony website also touted the legal registration of an LLC in the name of Representative E, claiming that Representative E offered financial planning services through that LLC.

367. In June 2021, Onyeachonam registered the LLC listed on the phony website in the name of Representative E in the state of Delaware.

368. Onyeachonam controlled the phony website starting in at least January 2022, as alleged in the paragraphs below.

369. Among other things, Onyeachonam received a test communication from the phony website's cpanel, a web-based interface that allows website owners to manage their websites and hosting accounts, in January 2022.

370. From September to December 2023, Onyeachonam accessed the cpanel page for the phony website six times.

371. Starting by at least September 2023, Onyeachonam maintained an account for the phony website with a web analytics tool that helps website owners analyze visitor behavior, track traffic, and optimize their websites.

B. Onyeachonam and Nweke-Eze Promoted Representative E Online.

372. Starting in at least June 2022, an email address attributable to Nweke-Eze used fake identities to promote Representative E's trading and investment services in comments to YouTube videos.

373. The comments took the form of a fictitious online conversation between strangers, one mentioning their investment success with Representative E and the other following up with questions about Representative E, concluding with an instruction from the purported Representative E client to look Representative E up on the Internet and call, email, or send a message.

374. The fictitious YouTube comments were scripted, and in emails sent to himself and others potentially involved in the fraud, Nweke-Eze emailed similar scripts used for another representative Defendants impersonated.

375. An email address attributable to Onyeachonam opened a LinkedIn account for Representative E that touted Representative E as a financial advisor at the LLC Onyeachonam had registered in Representative E's name with the state of Delaware.

C. A California Investor Found Representative E Online and Invested More Than $500,000.

376. An investor who at all relevant times has resided in California ("Investor E") found Representative E's fake website and sent Representative E (in

reality, Onyeachonam) a message in December 2022 using the form on the website.

377. On December 5, 2022, Onyeachonam sent an introductory email—purportedly from Representative E but actually from Onyeachonam—to Investor E asking where Investor E was located, what Investor E's experience was investing in financial markets, what his financial goals were, and how much Investor E had "set aside to achieve that financial goal."

378. Onyeachonam sent the email using the email address that purported to be Representative E's address, and Representative E's purported email signature block included the seals for both the SEC and FINRA BrokerCheck.

379. In response, Investor E said that he had average knowledge of the financial markets, his goal was to increase his net worth to $7-8 million in five years, and that he had properties and stocks worth $5.5 million.

380. On December 7, 2022, Onyeachonam, again posing as Representative E, emailed Investor E and claimed that Representative E traded across three major financial markets—the stock, foreign exchange, and digital currency markets—to maximize profit generation.

381. In December 2022 and January 2023, Onyeachonam, posing as Representative E, emailed Investor E a client investment form and a contract agreement.

382. The client investment form included the seals for both the SEC and FINRA Brokercheck.

383. The client investment form required Investor E to provide contact and background information, as well as information about his investing experience, financial assets, and investments.

384. The form claimed: "[Representative E] is a licensed Broker/Financial Adviser, regulated and accredited by the Financial Industry Regulatory Authority (FINRA) and Securities and Exchange Commission (SEC)[.] [Representative E] is therefore operating within the boundaries of [Representative E's] profession and the data you will provide below will be used for only investment purposes."

385. The contract agreement claimed that Investor E was required to pay "10% of the profit accrued by the portfolio under the management."

386. The contract agreement also promised that "the investment accounts of [Investor E] under the management of [Representative E] would accrue a minimum of 5% profits monthly."

387. Investor E filled out the client investment form, signed the contract agreement, and returned both to Onyeachonam through the email address he controlled, which purported to be Representative E's address.

388. On December 23, 2022, Onyeachonam, posing as Representative E, sent an email to Investor E instructing him to download and sign up for accounts at

two SEC-registered broker-dealers, a platform for trading currency, one crypto asset trading platform, and Secawallet and to set up a call so that Representative E could sync Investor E's accounts with Representative E's copy trading tool and discuss funding and investments.

389. On January 13, 2023, Onyeachonam, posing as Representative E, initiated a WhatsApp text conversation with Investor E.

390. Onyeachonam, posing as Representative E, and Investor E thereafter communicated primarily through WhatsApp messages.

391. On January 13, 2023, Onyeachonam, posing as Representative E, instructed Investor E through a WhatsApp message to sign up for Representative E's copy trading system and provided a link to a purported copy-trading tool to purportedly ensure that the client would be able to transparently view trading activity.

392. On January 16, 2023, Onyeachonam, posing as Representative E, emailed Investor E and claimed that, to maximize profit realization, Investor E's capital would be split between the stock market and crypto asset market at a "40:60 ratio" for the first three weeks of trading due to the bullish state of the crypto asset market.

393. In the same email, Onyeachonam instructed Investor E to make an initial deposit of $20,000 in Investor E's (genuine) brokerage account and $30,000

in Investor E's crypto asset account.

394. In January and February 2023, following these instructions, Investor E purchased bitcoin in his crypto asset accounts and transferred $33,997.54 in bitcoin to addresses displayed by the Secawallet website.

395. Investor E also deposited $20,000 in his (genuine) brokerage account.

396. On January 31, 2023, Onyeachonam, posing as Representative E, told Investor E that she had started trading Investor E's crypto asset account and provided a link and login credentials to LumenTrades.com, the fake investment account platform Onyeachonam had created.

397. The LumenTrades.com website displayed Investor E's investment and the purported trading returns from Representative E, which appeared to be substantial.

398. After Onyeachonam secured Investor E's initial investment and Investor E saw the significant fictitious profits that Representative E was purportedly generating, Onyeachonam, posing as Representative E, succeeded in getting Investor E to transfer an additional $209,879.04 in purported investment funds over the next three months.

399. Onyeachonam, posing as Representative E, used various techniques to extract additional funds from Investor E in addition to the fake returns on LumenTrades: Onyeachonam (1) promoted new trading strategies that required

additional funds to garner high returns; (2) repeatedly reminded Investor E that the crypto asset market was doing well; (3) touted Representative E's expertise, service, and trading success; and (4) promised Investor E that, if his account reached $200,000, he would be able to "withdraw $3,000 monthly without affecting the investment" using Representative E's "passive income strategy."

400. On June 1, 2023, Onyeachonam, posing as Representative E, emailed Investor E about an "exceptional investment opportunity" called the Alpha Crypto Private Fund and attached a Prospectus for the Fund.

401. The Prospectus touted Alpha Crypto Private Fund as having "consistently achieved a 6% monthly ROI [return on investment]" and having a "current valuation of $29 million."

402. The Prospectus also claimed that "we only charge a nominal fee of 10% on the profit generated," and that the "minimum investment amount" was $600,000.

403. On June 9, 2023, Onyeachonam, posing as Representative E, emailed Investor E, attaching a document titled "Tax-Loss Harvesting," and, in his cover email, wrote, "I strongly urge you to consider the new investment recommendation, as it flawlessly aligns with your financial goal. Thank you for your trust, [Investor E]. As your financial advisor, I have your best interests at heart."

404. The "Tax-Loss Harvesting" document purported to explain various tax aspects of investments and recommended the Alpha Crypto Private Fund because it "balances regular withdrawals and long-term capital growth potential" and "implements an advanced Tax-loss harvesting strategy, which adds an extra layer of benefit."

405. The "Tax-Loss Harvesting" document also claimed that, if Investor E rolled over his LumenTrades account and invested approximately $82,000 in additional funds, he would "achieve a harmonious balance between regular withdrawal of $3,000 and the potential for longer-term capital growth."

406. On June 14, 2023, Onyeachonam, posing as Representative E, emailed Investor E an investment application form and subscription agreement for the Alpha Crypto Private Fund.

407. The Alpha Crypto Private Fund investment application form required Investor E to provide contact and background information, as well as information about his investing experience, financial assets, and investments.

408. The Alpha Crypto Private Fund subscription agreement claimed that the Alpha Crypto Private Fund "shall generate a monthly profit of 6%," and "shall charge a performance fee of 10% of the Profit earned by the Subscriber."

409. Investor E filled out the client investment form, signed the subscription agreement, and returned both to Representative E (in reality,

Onyeachonam).

410. On June 16, 2023, Investor E purchased bitcoin in his crypto asset account and transferred $35,185.11 in bitcoin to an address displayed by the Secawallet website.

411. Four days later, Onyeachonam, posing as Representative E, messaged Investor E via WhatsApp that it would be "advantageous" to increase his current portfolio of $358,965.78 to $400,000 to "ensure seamless integration with our fund's investment and tax strategy."

412. Investor E responded, "So 42k more…. Ok I will arrange that."

413. Onyeachonam, posing as Representative E, replied, "Ok, once your portfolio reaches $400,000, it will transitioned [sic] to the fund."

414. On June 21, 2023, Investor E purchased bitcoin in his crypto asset account and transferred $39,258.74 in bitcoin to an address displayed by the Secawallet website.

415. On July 12, 2023, Onyeachonam, posing as Representative E, provided a link and log-in credentials to portal.alphacryptofund.com, the fake investment account platform Onyeachonam had created and controlled.

416. On July 26, 2023, Onyeachonam, posing as Representative E, provided a link and log-in credentials to portal.alphacryptofund.io, which he called "the backup domain" and which Onyeachonam also created and controlled.

417. Both the portal.alphacryptofund.com and portal.alphacryptofund.io websites displayed Investor E's investment and the purported trading returns from Representative E's work with the purported Alpha Crypto Private Fund, and the trading returns appeared to be substantial.

418. Between August 7 and August 23, 2023, Investor E and Onyeachonam, posing as Representative E, discussed via WhatsApp messages Investor E beginning monthly withdrawals of $3,000 at the end of the month.

419. On August 23, 2023, Onyeachonam, posing as Representative E, purported to explain to Investor E via WhatsApp how to make a withdrawal from the Alpha Crypto Fund investor portal.

420. Investor E then wrote to Representative E (in reality, Onyeachonam), "So for my investment, we will solely focus on crypto."

421. Onyeachonam, posing as Representative E, replied, "Yes for now. We will transition to other markets when I see opportunity for high returns."

422. Investor E responded, "sounds good thx."

423. Later that day, Investor E submitted a request to withdraw funds from his Alpha Crypto Fund account.

424. On August 25, 2023, Investor E confirmed via WhatsApp messages with Representative E (in reality, Onyeachonam) that he had received the $3,000 withdrawal in his crypto asset account and was able to transfer the money to his

bank account.

425. On September 12, 2023, email addresses attributable to Onyeachonam exchanged with others a draft of an email to a purported investor regarding a purported capital call, and the draft email had two attachments.

426. On September 13, 2023, Onyeachonam, posing as Representative E, sent Investor E an email attaching two documents regarding a purported capital call by the Alpha Crypto Private Fund—the same email and attachments Onyeachonam had emailed in draft form the day before.

427. The first attachment, the capital call notice, purported to require Investor E to make a capital contribution of $197,220.57 to the Alpha Crypto Private Fund to reach a total commitment of $600,000 "as per the Subscription Agreement dated 06/14/2023."

428. The capital call notice warned that, if Investor E failed to make the payments by September 29, 2023, he would be "subject to late fees," and would be charged interest on the unpaid amount and/or suffer a reduction in his percentage interest in the Fund.

429. The second attachment, titled "ALPHA CRYPTO PRIVAGE FUND: New Investment Strategy," claimed that the capital call was necessary to take significant positions, to invest in blockchain infrastructure projects and diversity investments, and to create a tax-loss harvesting solution.

430. On September 13, 2023, Investor E messaged Representative E (in reality, Onyeachonam), "I think I committed to 400k on my initial sign up, 600k would be high investment for me."

431. In response, Onyeachonam, posing as Representative E, messaged Investor E that investing in the Alpha Crypto Private Fund aligned with his goals of a passive income stream, continued wealth accumulation, and an optimized tax strategy.

432. Representative E (in reality, Onyeachonam) also offered Investor E an "upgrade to Tier 2, designed for investors who hold a full stake in the fund and receive the exact percentage the fund earns each month."

433. On September 15, 2023, Investor E messaged Representative E, "I will send 100k first and remaining later."

434. Onyeachonam, posing as Representative E, responded, "Ok."

435. On September 29, 2023, Investor E purchased bitcoin in his crypto asset account and transferred an additional $99,089.28 to an address displayed by Secwallet.com.

436. As Investor E was working on transferring the funds, Onyeachonam, posing as Representative E, messaged him, "[Investor E], just a friendly reminder: please ensure that you move the funds to your secawallet account by 11:59 pm today to avoid incurring late fees."

437. Investor E responded, "yes working on it."

438. On October 9, 2023, Onyeachonam, posing as Representative E, sent Investor E an email attaching the Alpha Crypto Private Fund's purported September 2023 performance report.

439. The purported performance report claimed "total assets under management" of $35.5 million, a September opening balance of $29.2 million, "September Performance" of 6.42% and "YTD Performance" of 58.7%.

440. The report included a purported "Fund Manager's Commentary" from Representative E.

441. On October 13, 2023, Investor E asked Representative E (in reality, Onyeachonam) via WhatsApp why Investor E's account on the Alpha Crypto Fund investor portal showed a return of 4.08%, while the September newsletter stated a return of 6.42%.

442. Onyeachonam, posing as Representative E, responded that if Investor E invested an additional $96,000, he would "receive the actual percentage that the fund earns," and that Investor E would begin "to receive a stable cash flow of $3,000 every month."

443. Investor E responded that he would work on selling a rental property to cover the additional funds.

444. On November 3, 3023, Onyeachonam posing as Representative E,

sent Investor E an email attaching the Alpha Crypto Private Fund's purported October 2023 performance update.

445. The purported performance update listed monthly returns of 6.72%, year-to date returns of 59.5%, and year-to-date asset growth of 23.5%.

446. The purported performance update appeared to be signed by Representative E as the Fund Manager of the Alpha Crypto Private Fund.

447. On November 3, 2023, Onyeachonam, posing as Representative E, messaged Investor E that he needed to invest additional funds to utilize a tax saving strategy that "could potentially lessen [Investor E's] tax liabilities by up to 45%," noting that "timing is crucial," and that the additional funds needed to be invested soon for the strategy to be available.

448. On November 10, 2023, Investor E purchased bitcoin in his crypto asset account, transferred an additional $59,127.54 in bitcoin to an address displayed by the Secawallet website, and told Representative E (in reality, Onyeachonam) via WhatsApp that this investment "should fulfill the 600k requirement principle + profit rollover."

449. On November 10, 2023, Onyeachonam, posing as Representative E, messaged Investor E that he was approximately $35,000 short of the "required principal target" because rolling over profits to meet funding requirements was not "feasible" to "avoid a potentially complex tax situation."

450. On November 27, 2023, Investor E purchased bitcoin in his crypto asset account, transferred an additional $36,601.13 in bitcoin to an address displayed on the Secawallet website, and messaged Representative E (in reality, Onyeachonam), "I just deposited the final funding to the Secawallet."

451. Investor E also asked, "That should fulfill the capital requirement for the fund right?"

452. Onyeachonam, posing as Representative E, responded, "Yes."

453. In reality, Onyeachonam and Nweke-Eze never invested Investor E's money as promised but instead misappropriated it.

D. Onyeachonam Gave Investor E the Runaround When He Attempted to Withdraw Additional Funds.

454. By late November 2023, Investor E's bitcoin had been moved through several addresses, and Onyeachonam and Nweke-Eze had stolen it.

455. On November 28, 2023, Investor E wrote to Representative E (in reality, Onyeachonam), "I will start my monthly withdrawal in Jan [2024]."

456. Onyeachonam, posing as Representative E, responded, "I got it, January 2024."

457. On January 11, 2024, Investor E emailed Representative E (in reality, Onyeachonam), "I am trying to contact you, can you either reply back to this email or send me message on whatsapp. thx."

458. Onyeachonam, posing as Representative E, responded, "I will get

back to you on WhatsApp as soon as possible."

459. Onyeachonam did not respond on WhatsApp.

460. Investor E emailed Representative E (in reality, Onyeachonam) multiple times in January 2024 about being unable to make withdrawals from the Alpha Crypto Fund portal or the Secawallet website and about his emails to the support address for these websites being returned, having failed to deliver.

461. On January 26, 2024, Investor E emailed the support email address for Secawallet and received a notice that the email was unable to be delivered.

462. Onyeachonam, posing as Representative E, and Investor E spoke on the phone on February 2, 2024.

463. After the phone call, Investor E emailed Representative E (in reality, Onyeachonam) three times in February 2024 without a response.

464. On February 20, 2024, Onyeachonam, posing as Representative E, sent a final email to Investor E, noting that Investor E's portfolio had accrued more than $220,000 in profit and suggesting that Investor E either move the invested funds to "a more conservative stock portfolio" or invest additional bitcoin into the current portfolio to ensure Investor E could meet his goal of withdrawing $3,000 monthly.

465. Investor E did not respond to this email.

466. Investor E did not receive any additional funds or other assets back

from Onyeachonam or Nweke-Eze other than the single $3,000 payment described above.

467. Between January and November 2023, Onyeachonam and Nweke-Eze stole $510,138.38 from Investor E.

FIRST CLAIM FOR RELIEF
Violations of Securities Act Sections 17(a)(1) and (3)
(All Defendants)

468. The Commission re-alleges and incorporates by reference here the allegations in paragraphs 1 through 467.

469. Defendants, directly or indirectly, singly or in concert, in the offer or sale of securities and by the use of the means or instruments of transportation or communication in interstate commerce or the mails, (i) knowingly or recklessly have employed one or more devices, schemes or artifices to defraud, and/or (ii) knowingly, recklessly, or negligently have engaged in one or more transactions, practices, or courses of business which operated or would operate as a fraud or deceit upon the purchaser.

470. By reason of the foregoing, Defendants, directly or indirectly, singly or in concert, have violated and, unless enjoined, will again violate Securities Act Sections 17(a)(1) and (3) [15 U.S.C. §§ 77q(a)(1) and 77q(a)(3)].

SECOND CLAIM FOR RELIEF
Violations of Securities Act Section 17(a)(2)
(Onyeachonam)

471. The Commission re-alleges and incorporates by reference here the allegations in paragraphs 1 through 54, 57 through 149, 153 through 196, 205, 210 through 371, and 375 through 467.

472. Onyeachonam, directly or indirectly, singly or in concert, in the offer or sale of securities and by the use of the means or instruments of transportation or communication in interstate commerce or the mails, knowingly, recklessly, or negligently has obtained money or property by means of one or more untrue statements of a material fact or omissions of a material fact necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading.

473. By reason of the foregoing, Onyeachonam, directly or indirectly, singly or in concert, has violated and, unless enjoined, will again violate Securities Act Section 17(a)(2) [15 U.S.C. § 77q(a)(2)].

THIRD CLAIM FOR RELIEF
Violations of Exchange Act Section 10(b) and Rules 10b-5(a) and (c) Thereunder
(All Defendants)

474. The Commission re-alleges and incorporates by reference here the allegations in paragraphs 1 through 467.

475. Defendants, directly or indirectly, singly or in concert, in connection

with the purchase or sale of securities and by the use of means or instrumentalities of interstate commerce, or the mails, or the facilities of a national securities exchange, knowingly or recklessly have (i) employed one or more devices, schemes, or artifices to defraud, and/or (ii) engaged in one or more acts, practices, or courses of business which operated or would operate as a fraud or deceit upon other persons.

476. By reason of the foregoing, Defendants, directly or indirectly, singly or in concert, have violated and, unless enjoined, will again violate Exchange Act Section 10(b) [15 U.S.C. § 78j(b)] and Rules 10b-5(a) and (c) thereunder [17 C.F.R. §§ 240.10b-5(a) and 240.10b-5(c)].

FOURTH CLAIM FOR RELIEF
Violations of Exchange Act Section 10(b) and Rule 10b-5(b)
(Onyeachonam)

477. The Commission re-alleges and incorporates by reference here the allegations in paragraphs 1 through 54, 57 through 149, 153 through 196, 205, 210 through 371, and 375 through 467.

478. Onyeachonam, directly or indirectly, singly or in concert, in connection with the purchase or sale of securities and by the use of means or instrumentalities of interstate commerce, or the mails, or the facilities of a national securities exchange, knowingly or recklessly has made one or more untrue statements of a material fact or omitted to state one or more material facts

necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading.

479. By reason of the foregoing, Onyeachonam, directly or indirectly, singly or in concert, has violated and, unless enjoined, will again violate Exchange Act Section 10(b) [15 U.S.C. § 78j(b)] and Rule 10b-5(b) thereunder [17 C.F.R. § 240.10b-5(b)].

FIFTH CLAIM FOR RELIEF
Violations of Advisers Act Sections 206(1) and (2)
(Onyeachonam and Asiegbu)

480. The Commission re-alleges and incorporates by reference here the allegations in paragraphs 1 through 55, 57 through 149, 153 through 205, 210 through 371, and 375 through 467.

481. At all relevant times, Onyeachonam and Asiegbu were investment advisers, under Advisers Act Section 202(11) [15 U.S.C. § 80b-2(11)].

482. Onyeachonam and Asiegbu, by use of the mails or any means or instrumentality of interstate commerce, directly or indirectly have (i) knowingly or recklessly employed one or more devices, schemes, or artifices to defraud any client or prospective client, and/or (ii) knowingly, recklessly, or negligently engaged in one or more transactions, practices, and courses of business which operated or would operate as a fraud or deceit upon any client or prospective client.

483. By reason of the foregoing, Onyeachonam and Asiegbu, directly or

indirectly, singly or in concert, have violated and, unless enjoined, will again violate Advisers Act Sections 206(1) and (2) [15 U.S.C. §§ 80b-6(1) and 80b-6(2)].

PRAYER FOR RELIEF

WHEREFORE, the Commission respectfully requests that the Court enter a Final Judgment:

I.

Permanently enjoining Defendants and their agents, servants, employees and attorneys and all persons in active concert or participation with any of them from violating, directly or indirectly, Section 17(a) of the Securities Act [15 U.S.C. § 77q(a)], Section 10(b) of the Exchange Act [15 U.S.C. § 78j(b)] and Rule 10b-5 thereunder [17 C.F.R. § 240.10b-5], and Sections 206(1) and (2) of the Advisers Act [15 U.S.C. §§ 80b-6(1) and 80b-6(2)];

II.

Permanently enjoining Defendants from directly or indirectly, including, but not limited to, through any entity controlled by each Defendant: (i) participating in the issuance, purchase, offer, or sale of any security on behalf of someone else; or (ii) engaging in activities for purposes of inducing or attempting to induce the purchase or sale of any security, including holding themselves out as industry professionals; provided, however, that such injunction shall not prevent each Defendant from purchasing or selling securities for his own personal account;

III.

Ordering Defendants to disgorge all ill-gotten gains they received directly or indirectly, with pre-judgment interest thereon, as a result of the alleged violations, pursuant to Exchange Act Sections 21(d)(3), 21(d)(5), and 21(d)(7) [15 U.S.C. §§ 78u(d)(3), 78u(d)(5), and 78u(d)(7)];

IV.

Ordering Defendants to pay civil monetary penalties under Securities Act Section 20(d) [15 U.S.C. § 77t(d)], Exchange Act Section 21(d)(3) [15 U.S.C. § 78u(d)(3)], and Advisers Act Section 209(e) [15 U.S.C. § 80b-9(e)]; and

V.

Granting any other and further relief this Court may deem just and proper.

JURY DEMAND

The Commission demands a trial by jury.

Dated: New York, New York
December 11, 2024

/s/ Antonia M. Apps

ANTONIA M. APPS
REGIONAL DIRECTOR
Tejal Shah
Adam S. Grace
Travis Hill
Rhonda Jung
Attorneys for Plaintiff
SECURITIES AND EXCHANGE COMMISSION
New York Regional Office
100 Pearl Street
Suite 20-100
New York, NY 10004-2616
212-336-9135 (Hill)
HillTr@sec.gov

Deborah A. Tarasevich
Elizabeth Doisy
Martin Zerwitz
Securities and Exchange Commission
100 F Street N.E. / Mail Stop 5631
Washington, D.C. 20549-5631

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

SECURITIES AND EXCHANGE COMMISSION, **Plaintiff,** **-against-** **CHIBUZO AUGUSTINE ONYEACHONAM, STANLEY CHIDUBEM ASIEGBU, and CHUKWUEBUKA MARTIN NWEKE-EZE,** **Defendants.**	**24-CV-11026** **DESIGNATION OF AGENT FOR SERVICE**

Pursuant to Local Rule 101.1(f), because the Securities and Exchange Commission (the "Commission") does not have an office in this district, the United States Attorney for the District of New Jersey is hereby designated as eligible as an alternative to the Commission to receive service of all notices or papers in the captioned action.

Therefore, service upon the United States or its authorized designee, David Dauenheimer, Deputy Chief, Health Care Fraud Unit, United States Attorney's Office for the District of New Jersey, 970 Broad Street, Suite 700, Newark, NY 07102, shall constitute service upon the Commission for purposes of this action.

Respectfully submitted,

/s/ Antonia M. Apps

ANTONIA M. APPS
REGIONAL DIRECTOR
Tejal Shah
Adam S. Grace
Travis Hill
Rhonda Jung
Attorneys for Plaintiff
SECURITIES AND EXCHANGE COMMISSION
New York Regional Office
100 Pearl Street
Suite 20-100
New York, NY 10004-2616
212-336-9135 (Hill)
HillTr@sec.gov

Deborah A. Tarasevich
Elizabeth Doisy
Martin Zerwitz
Securities and Exchange Commission
100 F Street N.E. / Mail Stop 5631
Washington, D.C. 20549-5631

Attorneys for Plaintiff
Securities and Exchange Commission