UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES SECURITIES AND EXCHANGE COMMISSION,	
Plaintiff,	
vs.	**Civil No.**
DENIS GEORGIYEVICH SOTNIKOV, ADAPTIVE TECHNOLOGY LLC, AGQ BUSINESS GROUP LLC, ATL BUSINESS GROUP LLC, BO&SA CORPORATION, DN INDUSTRIAL LLC, and EXPERT DIGITAL LLC,	**COMPLAINT**
Defendants,	
and	
NATALIA ALEKSANDROVNA MAZITOVA, GREAT IMPERIAL LLC, HRC CLEARING HOUSE LLC, INTEKO CARGO LLC,	**JURY TRIAL DEMANDED**
Relief Defendants.	

COMPLAINT

Plaintiff United States Securities and Exchange Commission (the "SEC" or the "Commission") alleges as follows against the following Defendants, whose names and last known addresses are set forth below:

a) Denis Georgiyevich Sotnikov ("Sotnikov"), 706 Diplomat Parkway, Hallandale Beach, Florida 33009;

b) Adaptive Technology LLC ("Adaptive Technology"), 801 Three Island Boulevard, Apt. 520, Hallandale Beach, Florida 33009;

c) AGQ Business Group LLC ("AGQ Business Group"), 1201 S Ocean Drive, Apt. 800, Hollywood, Florida 33019;

d) ATL Business Group LLC ("ATL Business Group"), 801 Three Island Boulevard, Apt. 520, Hallandale Beach, Florida 33009;

e) BO&SA Corporation ("BO&SA"), 1201 S. Ocean Drive, #2107S, Hollywood, Florida 33019;

f) DN Industrial LLC ("DN Industrial"), 3180 S Ocean Drive, #230, Hallandale Beach, Florida 33009; and

g) Expert Digital LLC ("Expert Digital"), 1201 S. Ocean Drive, #2107S, Hollywood, Florida 33019;

and as to the following Relief Defendants, whose names and last known addresses are set forth below:

a) Natalia Aleksandrovna Mazitova ("Mazitova"), 706 Diplomat Parkway, Hallandale Beach, Florida 33009;

b) Great Imperial LLC ("Great Imperial"), 18401 Collins Ave., Apt. 1173, Sunny Isles Beach, Florida 33160;

c) HRC Clearing House LLC ("HRC Clearing"), 801 Three Island Boulevard, Apt. 520, Hallandale Beach, Florida 33009; and

d) Inteko Cargo LLC ("Inteko Cargo"), 706 Diplomat Parkway, Hallandale Beach, Florida 33009.

SUMMARY

1. This matter concerns an ongoing fraudulent scheme in which U.S investors – many of whom are older and using their retirement savings – are lured to websites offering fictitious Certificates of Deposit ("CDs") at above-market rates.[1] Some of the websites "spoof" actual U.S.-based financial firms,[2] while others offer CDs from fake financial firms.

[1] Like bonds, CDs are debt-based, fixed-income securities that an investor holds until a fixed maturity date. The CDs offered as part of the scheme described here are fictitious instruments not issued by a legitimate U.S. bank, and are therefore not subject to protections offered by the federal banking laws. These fictitious CDs did, however, mimic real CDs by purporting to have a fixed maturity and promising a specific and above-market-rate of return, and they were offered to the general public and marketed as legitimate securities.

[2] "Spoofing" is the act of disguising a communication from an unknown source as being from a known, trusted source. *See, e.g., https://www.investopedia.com/terms/s/spoofing.asp*.

2. The spoofed websites use domain names similar to the domain names of actual financial institutions or that sound like real financial firms. The spoofed websites falsely claim that the firms offering CDs to investors are FDIC, FINRA, SIPC, or New York Stock Exchange members, and that the deposits are FDIC-insured.

3. The spoofed websites are advertised in search results provided by the two leading internet search and advertising companies. As a result, unsuspecting investors see advertisements for the spoofed websites at the top of their search results when conducting internet searches for CDs with attractive rates. Potential investors who visit a spoofed website are directed to call a telephone number on the website. Believing that they are dealing with a legitimate U.S.-based financial firm offering legitimate CDs, potential investors who call the number on a spoofed website speak with an individual purporting to be an "account executive" of the firm identified on the website. Potential investors provide an email address, after which they are contacted via email by the fake account executive, who often impersonates a real broker or sales representative of a spoofed financial firm.

4. Investors are instructed by the fake account executives to wire funds to bank accounts opened on behalf of purported "clearing firms" identified in the emails. Once the funds are received by the purported "clearing firm," they are quickly transferred to different bank accounts, both domestic and foreign, making it difficult or impossible for investors to regain their funds.

5. Since November 2014, the perpetrators of this scheme have created websites spoofing at least 24 actual financial firms and 8 fictitious financial firms, resulting in over $26 million in known investor losses. As described in this Complaint, Sotnikov and the entity defendants – Adaptive Technology, AGQ Business Group, ATL Business Group, BO&SA, DN

Industrial, and Expert Digital (collectively, the "Defendant LLCs") – are directly linked to 7 of the spoofed websites, through which investors have lost over $1.8 million.[3]

6. Sotnikov's participation is essential to the fraudulent scheme. He organized and/or controls the Defendant LLCs, each of which has been represented to investors as "clearing" or "offering" the CDs of a spoofed or fictitious financial firm and received investor funds. In fact, the Defendant LLCs are not clearing firms, and they do not offer or sell legitimate CDs or other securities. Instead, the Defendant LLCs were created by Sotnikov to serve as conduits to receive wire transfers from duped investors in furtherance of the fraudulent scheme alleged in this Complaint.

7. After investor funds are wired into a bank account nominally owned by one of the Defendant LLCs, but in fact controlled by Sotnikov, he either transfers the funds to other LLC-owned bank accounts that he or his wife, Relief Defendant Mazitova, control, including accounts nominally owned by the Relief Defendant LLCs, transfers the funds to other foreign bank accounts, transfers the funds to one of his personal bank accounts, or directly pays for his and/or his wife's personal expenses out of the accounts.

NATURE OF PROCEEDING AND RELIEF SOUGHT

8. The SEC brings this action against Sotnikov, the Defendant LLCs, Mazitova and the Relief Defendant LLCs pursuant to Section 21A [15 U.S.C. § 78u-l] of the Exchange Act and Section 20(b) of the Securities Act [15 U.S.C. § 77t(b)] seeking a judgment from the Court: (a) enjoining Sotnikov and the Defendant LLCs from engaging in future violations of the federal securities laws; (b) ordering the Defendants and the Relief Defendants to disgorge an amount

[3] In addition to $1.8 million in investor losses identified thus far, over $4 million of investor funds have been frozen by the banks at which the Defendant LLCs and Relief Defendant LLCs held or hold accounts.

equal to the profits gained and losses avoided as a result of the actions described herein, with prejudgment interest; and (c) ordering Sotnikov and the Defendant LLCs to pay civil monetary penalties.

JURISDICTION AND VENUE

9. This Court has jurisdiction over this action pursuant to Sections 21(d), 21(e), 21A and 27(a) of the Exchange Act [15 U.S.C. §§ 78u(d), 78u(e), 78u-l, and 78aa(a)] and Sections 20(b) and 22(a) of the Securities Act [15 U.S.C. §§ 77t(b) and 77v(a)].

10. Sotnikov and the Defendant LLCs, directly or indirectly, used the means of interstate commerce and/or the facilities of a national securities exchange, in connection with the transactions, acts, practices, and courses of business alleged in this Complaint.

11. Venue in this district is proper pursuant to Section 27 of the Exchange Act [15 U.S.C. § 78aa] because certain of the offers and sales of securities and certain of the acts, practices, transactions, and courses of business constituting the violations alleged in this Complaint occurred within this District. Specifically, the spoofed websites described herein were available to investors throughout this District, at least one investor residing in this District wired funds to one of the Sotnikov-controlled Defendant LLCs as a result of the fraudulent scheme,[4] and many of the investor wire transfers for fake CDs alleged in this Complaint were cleared through bank facilities in Mount Laurel, New Jersey.

DEFENDANTS

12. **Denis Georgiyevich Sotnikov**, age 36, is a Russian national who resides in Hallandale Beach, Florida. Sotnikov organized and/or controls or controlled each of the Defendant LLCs and Relief Defendant LLCs HRC Clearing and Inteko Cargo, and opened and

[4] Upon information and belief, that investor is a resident of Voorhees, New Jersey.

controls or controlled bank accounts nominally owned by the Defendant LLCs and Relief Defendant LLCs HRC Clearing and Inteko Cargo.

13. **Adaptive Technology LLC** is a Wyoming limited liability corporation ("LLC"), with a Hallandale Beach, Florida address listed in its incorporation papers. Sotnikov organized Adaptive Technology and he is listed in its incorporation papers as its "manager." Adaptive Technology is the nominal owner of bank accounts controlled by Sotnikov that directly received investor funds. Sotnikov has sole signatory authority over the Adaptive Technology bank accounts used in the scheme alleged in this Complaint.

14. **AGQ Business Group LLC** is a Florida LLC, with a Hallandale Beach, Florida address listed in its incorporation papers. Sotnikov organized AGQ Business Group and he is listed in its incorporation papers as its "manager." AGQ Business Group is the nominal owner of a bank account controlled by Sotnikov that directly received investor funds. Sotnikov has sole signatory authority over the AGQ Business Group bank account used in the scheme alleged in this Complaint.

15. **ATL Business Group LLC** is a Wyoming limited liability corporation, with a Hallandale Beach, Florida address listed on its incorporation papers – the same address used by Adaptive Technology. Sotnikov organized ATL Business Group and he is listed in its incorporation papers as its "manager." ATL Business Group is the nominal owner of a bank account controlled by Sotnikov that directly received investor funds. Sotnikov has sole signatory authority over the ATL Business Group bank account used in the scheme alleged in this Complaint.

16. **BO&SA Corporation** is a Florida corporation, with a Hollywood, Florida address listed in its incorporation papers – the same address used by AGQ Business Group.

Sotnikov was a founding member of BO&SA and was an officer of BO&SA at various times throughout its history, including from its creation on December 10, 2018 through March 13, 2019, and from May 21, 2019 through August 2, 2019. BO&SA is the nominal owner of bank accounts that directly received investor funds and that were accessed at various times by Sotnikov.

17. **DN Industrial LLC** was a Florida limited liability corporation, with a Hallandale Beach, Florida address listed in its incorporation papers – the same address used by AGQ Business Group, Expert Digital, and BO&SA. Sotnikov organized DN Industrial and was listed as its "manager" in its incorporation papers until it was dissolved on October 3, 2019.[5] DN Industrial is the nominal owner of bank accounts controlled by Sotnikov that directly received investor funds.

18. **Expert Digital LLC** was a New York limited liability corporation, with a Hollywood, Florida address – the same address used by AGQ Business Group and BO&SA. Sotnikov organized Expert Digital and was listed in its incorporation papers as its "manager" until it was voluntarily dissolved on September 13, 2019. Expert Digital was the nominal owner of bank accounts controlled by Sotnikov that directly received investor funds.

RELIEF DEFENDANTS

19. **Natalia Aleksandrovna Mazitova**, age 37, is a Russian national who resides in Hallandale Beach, Florida.

20. **Great Imperial LLC** is a Florida limited liability corporation, with a Lauderhill, Florida address. Relief Defendant Mazitova organized Great Imperial and she is listed in its

[5] Where an LLC is described in this Complaint as "dissolved," it means that, upon information and belief, the entity failed to file required annual paperwork with the government of the state in which the entity was organized.

incorporation papers as its "manager." Great Imperial is the nominal owner of bank accounts controlled by Mazitova that indirectly received investor funds.

21. **HRC Clearing House LLC** is a Florida limited liability corporation, with a Hallandale Beach, Florida address – the same address used by Adaptive Technology and ATL Business Group. Sotnikov organized HRC Clearing and he is listed in its incorporation papers as its "manager." HRC Clearing is the nominal owner of at least seven bank accounts controlled by Sotnikov, some of which indirectly received investor funds. Sotnikov has sole signatory authority over all HRC Clearing bank accounts used in the scheme.

22. **Inteko Cargo LLC** is a Florida limited liability corporation, with a Sunny Isles Beach, Florida address – the home address of Sotnikov and Mazitova. Sotnikov organized Inteko Cargo and he is listed in its incorporation papers as its "manager." Inteko Cargo is the nominal owner of at least six bank accounts controlled by Sotnikov, some of which indirectly received investor funds. Sotnikov has sole signatory authority over all Inteko Cargo bank accounts used in the scheme.

FACTUAL ALLEGATIONS

I. The Fraudulent Scheme To Sell Fake Certificates Of Deposit To U.S. Investors

23. Since at least November 2014 and continuing through March 2020, unidentified perpetrators have been spoofing websites of actual broker-dealers, investment advisers, and banks, or creating websites for fake financial firms, to offer fictitious CDs to U.S. investors.[6] These perpetrators have registered numerous domain names that are similar to the domain names of real financial institutions and then have used those domain names to create websites that purport to offer jumbo CDs at rates slightly higher than market rates. The websites typically use

[6] All investors referred to in this Complaint resided in the United States at the time of their investments.

the actual logos of the spoofed firms, and claim that the firms are FDIC, FINRA, SIPC, or New York Stock Exchange members, and that deposits are FDIC insured. The websites often use the spoofed firms' actual FINRA and/or FDIC member identification numbers.

24. In furtherance of the scheme, the perpetrators of the scheme have purchased internet advertising from, among others, the top two providers of internet search and advertising services, causing advertisements for the spoofed websites to appear at the top of search results for phrases such as "best CD rates," "highest cd rates," or other similar phrases.

25. As a result, unsuspecting investors, when conducting internet searches for CDs with attractive rates, received advertisements for the spoofed websites and clicked on links that directed them to the spoofed websites operated by the perpetrators of the scheme. They then called the telephone numbers provided on the spoofed websites and spoke to an individual claiming to be a representative of the spoofed firm, often impersonating an actual employee of the spoofed firm and using the real employee's name and FINRA CRD number.[7]

26. Investors then received an email from the purported account executive providing an application to open an "account" to purchase the CDs and wiring instructions to purported "clearing firms" with either foreign or U.S.-based accounts. After investors funded their CD accounts by wiring in their investments, the funds were quickly transferred to other bank accounts, including accounts overseas.

27. In addition to using the names of spoofed real or nonexistent financial firms and posing as actual employees of spoofed firms, the perpetrators have gone to significant lengths to

[7] FINRA operates the Central Registration Depository ("CRD"), the central licensing and registration system used by the U.S. securities industry and its regulators, which contains the registration records of broker-dealer firms and their associated individuals (*e.g.*, brokers and investment advisors).

hide their identities. For example, they have used: (1) virtual private networks ("VPNs") to anonymize their digital footprints, such as internet protocol ("IP") addresses; (2) prepaid gift cards to pay for domain-name registration services, state incorporation filings, internet ads, and VPN, website, and call-answering services; (3) prepaid phones or encrypted communication products to communicate; and (4) fake invoices and websites to explain large money transfers in response to inquiries by banks that received large wire transfers of investor funds.

28. In some cases, the real financial firms being spoofed learned about the spoofed website from victims or potential victims of the scheme, and took steps to shut down the spoofed websites by contacting the domain-name registrar and asserting trademark or copyright infringement. Even though the spoofed websites were typically up for only a few weeks before they were taken down, the perpetrators raised and wired abroad millions of dollars from duped U.S. investors. Since November 2014, the perpetrators have created websites spoofing at least 24 U.S.-based financial firms or using at least 8 fictitious entities, resulting in at least $26 million in known investor losses and $44.9 million in attempted investments.[8] As described below, Sotnikov and the Defendant LLCs are directly linked to 7 of the spoofed websites, through which investors have lost over $1.8 million. Many of the victimized investors were elderly and were investing their retirement savings.

II. Sotnikov's Role In The Fraudulent Scheme

29. Beginning no later than February 2019 and continuing through at least February 2020, Defendant Sotnikov participated in a scheme involving spoofs of at least seven different

[8] Investor losses are less than the total amount sent by investors to bank accounts controlled by the perpetrators of the larger scheme because investors, banks, or government agencies became suspicious or flagged specific transactions and some accounts were frozen before investor funds could be sent to foreign accounts or otherwise dispersed.

U.S.-based financial firms, with each spoofed website offering fictitious CDs to investors in a manner consistent with the scheme outlined above.

30. Sotnikov formed many U.S. limited liability companies, including the Defendant LLCs and several of the Relief Defendant LLCs.

31. In forming the Defendant LLCs and/or in opening bank accounts for them, Sotnikov claimed that the Defendant LLCs were engaged in legitimate businesses unrelated to the offer and sale of securities or the clearing of securities transactions:

a. DN Industrial - "Industrial Construction Business Equipment" (Bank account opening documents) and "Kitchen and restaurant equipment sales" (Bank account opening documents);

b. BO&SA - "Development and sale of software, provision of virtual space for sales representatives, development of web resources" (Florida incorporation documents);

c. Expert Digital - "IT Consulting, Computer, Technology and Program Consulting" business (Bank 1 account opening documents);

d. Adaptive Technology - "Custom computer programming services" (Bank account opening documents);

e. ATL Business Group - "custom computer programming services." (Bank account opening documents); and

f. AGQ Business Group - "Flooring and Kitchen construction" (Bank account opening documents).

Upon information and belief based on available bank records, however, none of these entities engaged in any legitimate business activity. Instead, their primary function was to serve as a conduit for the proceeds of the fraudulent scheme undertaken by Sotnikov and other perpetrators.

32. One of the Defendant LLCs, ATL Business Group, was also named as the entity *offering* the CDs on two spoofed websites — amrbusinessgroup.com and atlbusinessgroup.com. Each of the Defendant LLCs was based in a residential apartment or condominium in the Miami Beach area, including several at the same address, one of which is Sotnikov's personal residence.

33. Upon information and belief based on review of available records, Defendant DN Industrial, another of the Defendant LLCs controlled by Sotnikov, made payments to a leading provider of Internet search and advertising services for advertising that directed potential investors to at least one of the spoofed websites described below in this Complaint.

34. As with the Defendant LLCs, Sotnikov and Mazitova claimed that the Relief Defendant LLCs they created and controlled were engaged in legitimate businesses:

a. Great Imperial - "Marketing Consulting" in the "Professional, Scientific, and Technical Services" industry and "prefabricated wood building manufacturing" (Bank account opening documents); [9]

b. Inteko Cargo – "Transportation and warehousing" (Bank account opening documents); and

c. HRC Clearing – "[C]ustomer computer programming services" (Bank account opening documents).

But again, upon information and belief based on available bank records, the Relief Defendant LLCs created by Sotnikov and Mazitova were not engaged in any legitimate business activity. Instead, they were used by Sotnikov as conduits for his transfer of investor funds initially received into the Defendant LLC bank accounts. And as with the Defendant LLCs, each of the Relief Defendant LLCs was based in a residential apartment or condominium in the Miami Beach area, including several at the same address, one of which is Sotnikov's personal residence.

35. Sotnikov opened and controlled bank accounts on behalf of the Defendant LLCs, other than BO&SA, into which investors were instructed to wire their funds, and opened and controlled bank accounts on behalf of the Relief Defendant LLCs, other than Great Imperial, into which investor funds were ultimately transferred.

[9] Relief Defendant Mazitova is listed in state incorporation records as having organized Relief Defendant Great Imperial. Defendant BO&SA was organized by Sotnikov and two other individuals. The other Defendant LLCs and Relief Defendant LLCs were organized by Sotnikov.

36. After investor funds were wired into accounts nominally owned by the Defendant LLCs, Sotnikov laundered the funds by transferring money to accounts he or Relief Defendant Mazitova controlled that were nominally owned by the Relief Defendant LLCs, including accounts in the names of Great Imperial, HRC Clearing, and Inteko Cargo, or to other accounts at overseas banks. Some of the investor funds received into accounts controlled by Sotnikov and nominally owned by the Defendant LLCs were ultimately transferred to overseas accounts, either directly or after one or more transfers through bank accounts controlled by Sotnikov and nominally owned by the Relief Defendant LLCs:

37. In addition to transferring funds between the various LLC accounts, and transferring funds overseas, Sotnikov also transferred funds to his and Mazitova's personal bank accounts, and used those funds to pay for personal items, such as doctors' bills, jewelry and vacations.

38. Sotnikov also transferred funds from his personal bank account and the Relief Defendant LLCs' accounts he controlled into Defendant LLC accounts he controlled.

III. Spoofed Bank 1 – Sotnikov and DN Industrial

39. Defendants Sotnikov and DN Industrial were instrumental in an iteration of the spoofing scheme targeting Spoofed Bank 1, a real bank headquartered in California.

40. Sotnikov formed Defendant DN Industrial in Florida on July 26, 2018, listing himself as the sole manager of the company.

41. On August 9, 2018, Sotnikov opened an account at a well-known national bank ("Bank 1") in the name of DN Industrial. In the account opening documents, Sotnikov claimed that DN Industrial was in the "industrial construction business equipment business." On

December 6, 2018, Sotnikov opened an account at another major national bank ("Bank 2") in the name of DN Industrial. Sotnikov had sole signatory authority over each of these bank accounts.

42. Upon information and belief, DN Industrial is not a clearing firm, nor does it offer or sell legitimate CDs or other securities. Bank records demonstrate that Sotnikov used DN Industrial's bank accounts for personal purposes. For example, in addition to transferring money from DN Industrial's bank accounts into his personal accounts, he also transferred money from his personal accounts into DN Industrial's accounts on several occasions. And on January 14, 2019, Sotnikov used a check card linked to DN Industrial's Bank 2 account to pay $599 to a service provider to fly an aerial banner over a South Florida beach that read "Natalia will you marry me Denis."

43. In February 2019, the perpetrators of the spoofing scheme created several websites spoofing Spoofed Bank 1, in order to lure investors into purchasing fictitious CDs.

44. The domain names for these spoofed websites were designed to closely approximate Spoofed Bank 1's real domain name, using techniques such as adding initials after the real domain name, and the content of the websites was designed to mimic a real bank offering CDs to investors.

45. Each domain name created as part of the scheme to spoof Spoofed Bank 1 was registered in the U.S. by an individual using the name of a real registered representative employed by Spoofed Bank 1 who, upon information and belief, was not involved in the scheme ("Alias 1"). The person who registered the domain name paid the domain registrar to create an email account with an address using the names of Alias 1 and Spoofed Bank 1 ("Email Address 1") to communicate with investors, and provided a business address of 601 S. Figueroa Street, Los Angeles, California.

46. On February 11, 2019, a prospective investor viewed one of the spoofed websites, which used a domain name that was a slight variation on Spoofed Bank 2's real domain name ("Spoofed Website 1"), and which offered no penalty, above-market-rate CDs with a minimum deposit of $200,000, and inquired about investing in a nine-month jumbo CD.

47. The investor received an introductory email from Email Address 1, signed by an individual using Alias 1, and claiming to be a "Senior Account Executive" at Spoofed Bank 1.

48. In the email, the person using Alias 1 provided the potential investor with a real FINRA CRD number belonging to the real registered investment advisor affiliated with Spoofed Bank 1 in New Mexico, whose name matched Alias 1.

49. The email from the person using Alias 1 instructed the potential investor to complete and submit the attached "CD application," which required the potential investor to provide personally identifiable information ("PII"), including a Social Security Number and his mother's maiden name. The email also falsely stated that the entity offering the CDs:

> [I]s a Registered FDIC Institution. *Securities offered through [Bank 1] & [Bank 2].* ***DN Industrial LLC*** *Clearing or CM International – Member FINRA/SIPC.* Investment Advisory Services offered through [Spoofed Bank Alias 1] Los Angeles.
>
> (emphasis added).

In fact, DN Industrial was not a clearing firm, nor did it offer or sell legitimate CDs or other securities, and "Spoofed Bank Alias 1," named in the email and using a slight variation on Spoofed Bank 1's name, was not a real, FDIC-insured bank.

50. In addition to the CD application, the introductory email from Alias 1 also attached a fictitious CD Term Sheet, an example of FDIC coverage, a spoofed "Statement of Condition," which included a spoofed picture and statement from the spoofed bank's purported CEO, and a spoofed summary of the bank's assets and liabilities. The spoofed "Statement of

Condition" was copied nearly verbatim from the Statement of Condition of the real Spoofed Bank 1, but provided a different picture and misidentified Spoofed Bank 1's CEO.

51. Via email, the potential investor asked the person using Alias 1 to provide the FDIC number[10] of Spoofed Bank Alias 1, as he was unable to find the bank on the FDIC's website. The person using Alias 1 responded by email, providing the FDIC number for the real Spoofed Bank 1, headquartered in California.

52. The suspicious potential investor forwarded his communications with the person using Alias 1 to the real Spoofed Bank 1. Shortly thereafter, on February 13, 2019, Spoofed Website 1 was suspended by its domain-name registrar.

53. Another potential investor was not so fortunate. On February 12, 2019, when this investor emailed the person using Alias 1 to ask why his funds would not be "sent directly to" the bank listed on the spoofed website, the person using Alias 1 responded as follows:

> *The funds clear through the [Bank 1] clearinghouse* (***DN Industrial LLC***) for the sole purpose to facilitate the exchange of payments, and secure the purchaser . . . . The clearing house stands between two parties (also known as member firms or participants of FDIC). Its purpose is to eliminate the risk of, and honor settlement obligations in larger transactions.
>
> (emphasis added).

54. On February 15, 2019, based on the assurances provided by the person using Alias 1, and believing that he was buying a legitimate CD based on the information provided on Spoofed Website 1, this investor wired his life savings of $250,000 to DN Industrial's Bank 2 account – an account opened and controlled by Sotnikov.

[10] The FDIC assigns a registration number to each bank or savings association it insures. The "BankFind" tool on the FDIC's website allows visitors to obtain information about all FDIC-insured institutions based on a bank's name and/or FDIC number.

55. Within days after the investor's $250,000 wire was received into DN Industrial's account at Bank 2, rather than providing the investor with the promised CDs, Sotnikov made a series of fraudulent transfers that depleted the investor's funds: (i) on February 21, 2019, he wired $100,000 to an account at a Hong Kong bank; (ii) on February 21, 2019 and February 22, 2019, he wired a total of almost $40,000 to his and Relief Defendant Mazitova's joint checking account at Bank 2; and (iii) on February 22, 2019, he wired $130,000 to an account at Bank 2 in Relief Defendant Inteko Cargo's name, an account he opened and controlled. Later on February 22, 2019, Sotnikov transferred $43,000 from the Inteko Cargo account into his and Mazitova's personal joint checking account at Bank 2, and then transferred $30,200 from his and Mazitova's joint checking account back into DN Industrial's Bank 2 account.

56. With Spoofed Website 1 suspended, the perpetrators turned to the other domain names related to Spoofed Bank 1 that they had previously registered to continue the scheme. Like Spoofed Website 1, these spoofed websites offered no penalty, above-market-rate CDs with a minimum deposit of $200,000. The website also claimed that Spoofed Bank Alias 1 was a "Member FDIC" and had offices located at 601 S. Figueroa St., Los Angeles, California.

57. In late February 2019, upon inquiring about the CDs offered on these websites, at least four elderly retired investors received the same introductory email from the person using Alias 1, including the following language: "*Securities offered through [Bank 1] & [Bank 2].* ***DN Industrial LLC*** *Clearing* or CM International – Member FINRA/SIPC" (emphasis added). These emails attached the same CD application as that used earlier in the scheme. On February 25, 2019, after returning the completed applications, each investor received an email from the person using Alias 1, containing the Bank 2 logo and welcoming them to "[Spoofed Bank Alias 1] . . . Cleared by [Bank 2] ***DN Industrial LLC***" (emphasis added).

58. The emails received by these investors also stated that their CD accounts were "now active and ready for funding," and attached wire instructions to fund their CD accounts "with our clearing partner [Bank 2]." Like the previous wire instructions, these instructions directed the investors to wire their funds to DN Industrial's Bank 2 account, and identified DN Industrial as: "DN Industrial LLC . . . A [Bank 2] Company" and "Member FINRA Member FDIC." In fact, DN Industrial is not a FINRA or FDIC member, its bank accounts are controlled by Sotnikov, and the only business activity observable from its banking records is the laundering by Sotnikov of funds received from duped investors. Further, Bank 2 had no knowledge of or involvement in the scheme, and DN Industrial was not a "[Bank 2] company," but rather simply had an account at Bank 2.

59. On February 25, 2019, an elderly couple wired $383,000 to the DN Industrial account at Bank 2 controlled by Sotnikov after receiving the CD application and wire instructions from the person using Alias 1. Rather than providing the investor with the promised CDs, Sotnikov made a series of fraudulent transfers that rapidly depleted the investor's funds. On February 26, 2019, the day after the investor's wire was received, Sotnikov transferred $382,900 of the investor's funds to another account he controlled – Relief Defendant Inteko Cargo's account at Bank 2. Two days later, Sotnikov transferred $35,000 from that Inteko Cargo account to his and Relief Defendant Mazitova's joint checking account at Bank 2, some of which was used to make purchases at a luxury jewelry retailer and a luxury clothing and accessories retailer.

60. On February 28, 2019, after being contacted by the person using Alias 1, another elderly investor wired $200,000 into the DN Industrial account at Bank 2 controlled by Sotnikov. Again, rather than providing the investor with the promised CDs, Sotnikov made a series of

fraudulent transfers that rapidly depleted the investor's funds. The day after the investor's funds were received, March 1, 2019, Sotnikov wired $171,880 of that investor's funds from DN Industrial's Bank 2 account to an account at a Turkish bank with the following payment detail: "PMNT FOR EQUIPMENT INVOICE 37 POPSERVICES."

61. Shortly after each investor's funds were received into Sotnikov's DN Industrial's Bank 2 account controlled by Sotnikov, each investor received a fictitious account statement from "[Spoofed Bank Alias 1] FDIC," via email from the person using Alias 1. Although each investor's funds had in fact been rapidly depleted by Sotnikov, the fictitious account statements reflected each investor's purported "opening balance," "interest earned" and "credits" reimbursing them for their wire transfer costs.

62. On February 26, 27 and 28, 2019 Sotnikov wired a total of $15,000 to a leading provider of Internet search and advertising services, using funds from the same DN Industrial Bank 2 account that received the investors' funds. Records obtained from that provider indicate that these payments were made to purchase advertising that directed potential investors to at least one of the spoofed websites described below.

IV. Spoofed Bank 2 – Sotnikov and DN Industrial

63. Defendants Sotnikov and DN Industrial were also instrumental in another iteration of the spoofing scheme targeting Spoofed Bank 2, a real bank headquartered in Green Bay, Wisconsin.

64. By early March 2019, the perpetrators began spoofing Spoofed Bank 2, again directing investors to wire money to a DN Industrial bank account controlled by Sotnikov.

65. On March 4, 2019, a person using Alias 1, still using the 601 S. Figueroa Street address in Los Angeles and spoofed Email Address 1, registered a domain name using a slight

variation on Spoofed Bank 2's name ("Spoofed Website 2"). The domain registration fee was paid with a prepaid gift card purchased a day earlier at a grocery store in Irvine, California.

66. The new website claimed to offer above-market-rate CDs from "[Spoofed Bank Alias 2], Member FDIC," with no penalties and a minimum deposit of $200,000. The website claimed that Spoofed Bank Alias 2 was affiliated with another bank with a slightly different variation on Spoofed Bank 2's name ("Spoofed Bank Alias 3") and claimed that Spoofed Bank Alias 3 had offices at 601 S. Figueroa Street, Los Angeles, California. In fact, neither Spoofed Bank Alias 2 nor Spoofed Bank Alias 3 was a real, FDIC-insured bank.

67. The documents and correspondence used for the Spoofed Bank 2 iteration of the scheme were nearly identical to those used in the Spoofed Bank 1 iteration of the scheme. The introductory email to potential investors was again signed by the person using Alias 1. He stated that he was a "Senior Account Executive," provided the FINRA CRD number of the real person with the same name as Alias 1, and attached a nearly identical CD application. In this iteration of the scheme, however, the person using Alias 1 claimed to be associated with "Spoofed Bank Alias 4," another slight variation on Spoofed Bank 2's name, and provided the FDIC number of the real Spoofed Bank 2.

68. After completing and submitting the application, investors received a "welcome" email from the person using Alias 1, stating that the investor's CD account was "now active and ready for funding," and attaching wiring instructions "with our clearing partner DN Industrial, LLC and [Bank 1] to fund" the CD. The wire instructions directed investors to fund their CD "account with DN Industrial, LLC" by wiring money to DN Industrial's Bank 1 account, an account controlled by Sotnikov. The wire instructions for DN Industrial's Bank 1 account used the real Bank 1 logo and identified DN Industrial as "DN Industrial LLC . . . Member FINRA

Member FDIC." In fact, upon information and belief, none of the spoofed bank aliases are associated with a real, FDIC-insured bank, and DN Industrial is not a clearing firm, is not a FINRA or FDIC member, and it does not offer or sell legitimate CDs or other securities. Instead, DN Industrial's bank accounts are controlled by Sotnikov, and the only business activity observable from DN Industrial's banking records is the laundering by Sotnikov of funds received from duped investors.

69. Between March 22 and March 27, 2019, at least three additional investors wired a total of $990,000 to DN Industrial's bank accounts in connection with the iteration of the scheme related to Spoofed Bank 2.

70. On March 22, 2019, two married investors wired $250,000 to DN Industrial's account at another well-known national bank ("Bank 3"), and another investor wired $240,000 to DN Industrial's Bank 1 account, an account controlled by Sotnikov. And on March 27, 2019, the same married couple invested an additional $500,000 by wiring the funds to DN Industrial's Bank 3 account, another account controlled by Sotnikov.

71. Within days of receiving these investor funds, rather than providing the investors with the promised CDs, Sotnikov fraudulently transferred a substantial portion of the investor funds received into DN Industrial's Bank 1 account to other accounts that he and his wife controlled: On March 27, 2019, he transferred $25,000 to an account in his wife's name at a Russian bank; on March 28 and 29, 2019, he transferred a total of $35,000 to the Bank 1 account of Inteko Cargo, which he controlled; and on April 1, he transferred $8,200 to Expert Digital's Bank 1 account, another account he controlled.

72. Also on April 1, 2019, Sotnikov transferred $16,500 from Inteko Cargo's Bank 1 account to Great Imperial's Bank 2 account, and transferred another $8,000 from Expert

Digital's Bank 1 account to Great Imperial's Bank 3 account. Relief Defendant Mazitova, who organized and controls Great Imperial, proceeded to transfer a majority of those funds to her personal savings account over the next several days.

73. On April 3, 2019, Sotnikov transferred an additional $10,500 from DN Industrial's Bank 1 account to Inteko Cargo's Bank 1 account, and transferred $14,100 from DN Industrial's Bank 1 account to Expert Digital's Bank 1 account. Shortly thereafter, Sotnikov transferred $13,100 from Expert Digital's Bank 1 account to Great Imperial's Bank 3 account, an account controlled by Relief Defendant Mazitova.

74. Also on April 3, 2019, Mazitova used funds from Great Imperial's Bank 1 account for purchases at a cell phone provider and department store, and transferred $15,000 to her personal savings account at Bank 3.

V. Spoofed Bank 3 – Sotnikov, Expert Digital, and BO&SA

75. Defendants Sotnikov, Expert Digital, and BO&SA were instrumental in another iteration of the spoofing scheme targeting a bank headquartered in St. Louis, Missouri ("Spoofed Bank 3").

76. On September 12, 2018, Sotnikov formed Expert Digital in New York. Two days later, Sotnikov opened an account for Expert Digital at Bank 1, over which he had sole signatory authority. In the account opening documents, Sotnikov described Expert Digital as being in the "IT consulting, computer, technology and program consulting" business. He listed three companies based in Kazan, Russia as being Expert Digital's major suppliers, and claimed that his major customers were primarily retail-based. On December 7, 2018, Sotnikov opened another account for Expert Digital at Bank 2, over which he again had sole signatory authority.

77. On December 6, 2018, Sotnikov and two other individuals formed Defendant BO&SA in Florida. BO&SA's business was described as the "development and sale of software, provision of virtual space for sales representatives, [and] development of web resources." On March 28, 2019, an account was opened in BO&SA's name at another well-known national bank ("Bank 4").

78. Although Sotnikov was not BO&SA's sole organizer or control person, as he was with the other Defendant LLC's, he served as either president or vice president of BO&SA of from December 10, 2018 through March 13, 2019, and from May 21, 2019 through August 2, 2019.[11] In addition, BO&SA's address was listed in corporate records as 1201 S. Ocean Drive, 2107 S, Hollywood, FL 33019 – the same address as that of three of the other Defendant LLCs organized by Sotnikov – Expert Digital, DN Industrial, and AGQ Business Group.[12] In addition, a significant portion of the investor funds wired into BO&SA's account was transferred to Relief Defendant HRC Clearing, an entity controlled by Sotnikov.

79. As noted above, on February 26, 27 and 28, 2019, Sotnikov wired a total of $15,000 to a leading provider of Internet search and advertising services. Records obtained from that provider indicate that the payments were for advertising that directed potential investors to at least one of the spoofed websites related to this iteration of the scheme.[13]

---

[11] Sotnikov was removed as an officer of BO&SA shortly before BO&SA opened a bank account at Bank 4 that received investor funds, and was later re-installed as an officer of BO&SA.

[12] Account opening documents submitted to Bank 4 listed a different address for BO&SA – 18401 Collins Ave., Apt. 1243, Sunny Isles Beach, FL 33160 – the same street address as Relief Defendant Great Imperial, albeit with a different apartment number.

[13] These payments were made with funds from DN Industrial's Bank 2 account, the same account that received investor funds from an earlier iteration of the scheme involving Spoofed Bank 1.

80. Beginning in late February 2019, the perpetrators began using websites spoofing Spoofed Bank 3. In certain instances, they directed investors to wire money to Expert Digital's Bank 1 account, an account controlled by Sotnikov. In other instances, they directed investors to wire money to BO&SA's Bank 4 account. Although Sotnikov was no longer listed as an officer of BO&SA as of late February 2019, corporate records listed the managing members of BO&SA as two individuals who were officers of BO&SA at the same time as Sotnikov.

81. Between mid-March 2019 and May 2019, using four different domain-name registration providers based in the U.S., Russia and Israel, the perpetrators registered at least six domain names designed to convince investors that they were dealing with the real Spoofed Bank 3 by using slight variations on the bank's name. The domain names registered in the U.S. were again registered by an individual using Alias 1, and were paid for using two prepaid gift cards purchased at a grocery store in California. In registering the domain names, the person using Alias 1 again identified his business address as 601 S. Figueroa Street, Los Angeles, California.

82. Like the previous websites, these new websites offered no penalty, above-market-rate CDs with a minimum deposit of $200,000, claimed that the fictitious offering bank was a "Member FDIC," and claimed that deposits were FDIC-insured. The websites also claimed to use real U.S. banks (Bank 1, Bank 2, and Bank 3) and other entities as "clearing partners."[14]

83. Investors who inquired about the CDs offered on these Spoofed Bank 3-related websites received an introductory email from an email address that featured Alias 1 and Spoofed Bank 3 ("Email Address 2"). For example, an investor and a prospective investor received emails on May 8, 2019 claiming that the person using Alias 1 was a "Senior Account Executive"

[14] The websites again used the same business address – 601 S. Figueroa Street, Los Angeles, California – used previously by the person using Alias 1.

at Spoofed Bank 3 and again provided the FINRA CRD number of the real person with the same name as Alias 1's and Spoofed Bank 3's real FDIC number.[15]

84. The email also attached a CD application nearly identical to that used in the prior spoofs, stating that the purported bank "is a Registered FDIC Institution. *Securities offered through [Bank 1], or [Bank 4],* ***Expert Digital LLC*** *or* ***BO&SA*** *Clearing – Member FINRA/SIPC.* Investment Advisory Services offered through [Spoofed Bank Alias 4]" (emphasis added).

85. In fact, upon information and belief, "Spoofed Bank Alias 4," named in the email and using a slight variation on Spoofed Bank 3's name, is not a real, FDIC-insured bank, neither Expert Digital nor BO&SA is a clearing firm, and neither LLC offers or sells legitimate CDs or any other securities.

86. After submitting the completed application, investors again received a "welcome" email from the person using Alias 1, explaining that their CD accounts were "now active and ready for funding" and attaching wire instructions.

87. An email and wiring instructions sent to at least one investor on May 8, 2019 claimed that the bank's transactions were "Cleared by [Bank 1] through Expert Digital LLC Clearing" and instructed investors to wire funds to Expert Digital's Bank 1 account. As noted above, Expert Digital is not a clearing firm. Its bank accounts are controlled by Sotnikov, and the only business activity observable from its banking records is the laundering by Sotnikov of funds received from duped investors.

[15] Upon information and belief, the real registered representative impersonated by the person using Alias 1 has no business relationship with the real Spoofed Bank 3.

88. Wire instructions sent to two other investors on May 15, 2019 instructed the investors to wire their funds to "BO&SA Corp. Clearing through [Bank 4]." The wire instructions used Bank 4's logo, and stated "BO&SA Corp. Clearing through [Bank 4]" and "Member FINRA." As noted above, BO&SA is not a clearing firm, nor is it a member of FINRA. Instead, BO&SA was organized by Sotnikov and two other individuals, and the only business activity observable from BO&SA's banking records is the laundering of funds received from duped investors.

89. In May 2019, three investors wired a total of $850,000 to Expert Digital's Bank 1 account, an account controlled by Sotnikov. One investor wired $200,000 on May 8, 2019, and two investors (a husband and wife) wired $650,000 on May 9, 2019. On May 8, Sotnikov transferred $70,000 from Expert Digital's Bank 1 account to Inteko Cargo's Bank 1 account. Shortly thereafter, Expert Digital's Bank 1 account was frozen.

90. Also in May 2019, three additional investors wired a total of $407,000 to BO&SA's Bank 4 account. One investor wired $207,000 on May 13, 2019, and two other investors (again a husband and wife) wired $200,000 on May 16, 2019. Of the $407,000 in investor funds wired into BO&SA's Bank 4 account, $228,000 was sent to an account at another well-known national bank ("Bank 7") in the name of Relief Defendant HRC Clearing, another entity controlled by Sotnikov – $50,000 by wire on May 15, 2019, and $178,000 by check dated June 10, 2019. Sotnikov used certain of the funds transferred to HRC Clearing to pay for a trip to New York City. On June 5, $150,000 was transferred from BO&SA's Bank 4 account to Sotnikov's personal account at another well-known national bank ("Bank 5"). On June 10, 2019, $20,000 was transferred from BO&SA's Bank 4 account to Relief Defendant Great Imperial's Bank 5 account, an account controlled by Relief Defendant Mazitova. She subsequently used

funds from Great Imperial's account to pay for personal medical services and a purchase at a luxury goods retailer.

VI. AMR Business Group/ATL Business Group Spoofs – Sotnikov, Adaptive Technology, and ATL Business Group

91. Defendants Sotnikov, Adaptive Technology, and ATL Business Group were instrumental in the next iteration of the spoofing scheme.

92. On November 7, 2019, Sotnikov formed Defendant Adaptive Technology as a Wyoming LLC, providing his Florida address as the business address and naming himself as the manager. On November 27, 2019, Sotnikov opened a bank account for Adaptive Technology at Bank 5. The account opening documents claimed that the company's purpose was to provide "custom computer programming services" and that it "create[d] apps for Apple and other companies." Sotnikov had sole signatory authority over the account.

93. On November 25, 2019, Sotnikov formed another Wyoming LLC, Defendant ATL Business Group, using the same Florida address as Adaptive Technology, and again naming himself as manager. On December 27, 2019, Sotnikov opened a bank account for ATL Business Group at Bank 5, claiming in account opening documents that ATL Business Group LLC also provided "customer computer programming services." Sotnikov had sole signatory authority over the account.

94. Starting in January 2020, the perpetrators modified their scheme, but continued to use websites offering fictitious CDs to investors. Rather than spoofing real banks and brokerage firms, however, the perpetrators created multiple websites, often using fictional financial firms. They also created at least one website using the name of Defendant ATL Business Group, an entity organized and controlled by Sotnikov, and at least three of the websites in this iteration of

the scheme employed Defendant LLCs organized and controlled by Sotnikov to receive investor funds.

95. Other than moving away from spoofing the websites of actual, legitimate U.S. financial institutions, the scheme generally remained unchanged. After accessing the spoofed website, the investor received an email from a fake account executive impersonating a real registered investment adviser. The email stated that the "securities were being offered" by one of the Defendant LLCs organized and controlled by Sotnikov, and attached a CD account application. After submitting the completed application, the investor received instructions to wire their funds to an account in the name of the Sotnikov-controlled entity; and upon receipt of the funds into the account, the investor received a fictitious account statement reflecting their opening balance.

96. On January 6, 2020, the perpetrators registered the domain name amrbusinessgroup.com with a Cyprus-based domain registrar and created a website for AMR Business Group, which appears to be a fictitious entity. The website did not spoof an actual financial institution, but mimicked a website of a real financial institution. The website falsely claimed that AMR Business Group was "an insured FDIC institution" and "FDIC Member," that offered jumbo CDs. The website repeated many of the same specific phrases the perpetrators had used in many of their previous websites, including offering no penalty, above-market-rate CDs.

97. The following day, on January 7, 2020, the perpetrators registered the domain name — atlbusinessgroup.com — corresponding with the Wyoming LLC Sotnikov had organized six weeks earlier. The domain was registered with a Russia-based domain registrar. The ATL Business Group website that subsequently appeared in this iteration of the scheme was

practically identical to the spoofed AMR Business Group website, using the same business telephone number and address and similar text.

98. On January 8, 2020, an investor expressed interest in the CDs being offered by either AMR Business Group or ATL Business Group and received an email with an attached CD application from an email address ("Email Address 3") that used the name of a real person who worked as an investment adviser at an affiliate of Bank 5 who, upon information and belief, had no knowledge of the scheme ("Alias 2"). The person using Alias 2 claimed to be a "Senior Account Executive" at "AMR Wealth – [Bank 5] Group," and provided a Los Angeles address for a Bank 5 branch, Bank 5's actual FDIC number, and the real registered investment advisor's FINRA CRD number. In fact, the spoofed domain name and the Email Address 3 account had been registered by the perpetrators on January 6, 2020.

99. After receiving the email, the investor completed and submitted a CD application identical to the previous applications, with the exception that this version of the CD application used Bank 5's logo. The very next day, the investor received a welcoming email from the person using Alias 2 which, like the past iterations, stated that "your account is now active, and ready for funding," and attached instructions to fund the CD purchase by wiring funds to "our clearing partner Cleared by ATL Business Group LLC through [Bank 5]." The wire instructions directed the investor to wire the funds to Defendant ATL Business Group's account at Bank 5, an account opened by Sotnikov just two weeks earlier and for which he had sole signatory authority.

100. On January 10, 2020, the investor wired $250,000 to ATL Business Group's Bank 5 account. The next business day – Monday, January 13, 2020 – the investor received an "account statement" showing his opening balance of $250,000, as well as a $25 credit to refund the investor's wire transfer fee.

101. On January 13, 2020, Sotnikov withdrew $9,000 from ATL Business Group's Bank 5 account and wired $20,000 to a corporate account at a Russian bank. On the same day, Sotnikov withdrew $9,000 from ATL Business Group's account at a Bank 5 branch in Hallandale Beach, Florida. On January 14, 2020, Sotnikov wired $215,000 to Relief Defendant Great Imperial's account at Bank 3, an account controlled by Relief Defendant Mazitova.

102. The amrbusinessgroup.com website was taken down on January 13.

103. On January 21, 2020, another investor submitted an account opening application to the person using Alias 2 at Email Address 3. On January 21, after the person using Alias 2 confirmed (falsely) that the investor's CD account had been opened, the investor wired $500,000 to ATL Business Group's Bank 5 account, an account opened and controlled by Sotnikov.

104. On January 21, 2020, the same day the investor funds were received into ATL Business Group's Bank 5 account, Sotnikov withdrew $5,000 from the account at a Bank 5 branch in Sunny Isles, Florida. On January 22, 2020, Sotnikov wrote a $470,000 check from ATL Business Group's Bank 5 account for deposit into the Bank 4 account of Relief Defendant Inteko Cargo, another account controlled by Sotnikov in the name of an entity he organized and controls.

105. On January 22, 2020, the day after the investor's funds were received into Relief Defendant ATL Business Group's Bank 5 account, and as Defendants Sotnikov and ATL Business Group were actively depleting the investor's funds, the investor received an "account statement" showing an "opening balance" of $500,000 and a $25 credit to refund the investor's wire fee. The "account statement" did not disclose that Sotnikov and ATL Business Group had diverted most of the investor's funds.

106. On January 27, 2020, two additional investors (a married couple) received an email from the person using Alias 2 at Email Address 3 that said "Thank you so much for allowing us to help you with your recent inquiry and account opening procedures. . . . ATL Wealth Management Group-[Bank 5] is a full service, global financial institution." The email attached an application to open an account for a $200,000 Jumbo CD with "ATL Wealth, A [Bank 5] Company – Member FDIC." After completing and returning the application to purchase a $225,000 CD, the investors received another email from the person using Alias 2 describing "ATL Wealth Group" as a "registered FDIC Institution of [Bank 5]." Upon information and belief, "ATL Wealth Group" does not exist, and Defendant ATL Business Group is neither an FDIC member nor an affiliate of the real Bank 5. Instead, Defendant ATL Business Group's bank accounts are controlled by Sotnikov, and the only business activity observable from ATL Business Group's banking records is the laundering by Sotnikov of funds received from duped investors.

107. The following day, January 28, 2020, the investors received a letter from Alias 2 informing them that "on behalf of our entire ATL-[Spoofed Bank 4] & [Bank 5] staff," their application had been approved and their account was now open.[16] The letter claimed that the investors' CD purchases were "cleared by [Bank 2] through Adaptive Technology LLC." And the attached wire instructions stated: "Cleared by AMR Business Group LLC through [Bank 4]" and instructed the investors to wire their funds to Adaptive Technology's [Bank 2] account. Defendant Adaptive Technology is not a clearing firm, nor does it offer or sell legitimate CDs or other securities. Adaptive Technology's bank accounts are controlled by Sotnikov, and the only

[16] This email also used a name almost identical to that of a large financial institution offering investment banking and other services ("Spoofed Bank 4"), a firm that was featured in a subsequent iteration of the scheme described below.

business activity observable from its banking records is the laundering by Sotnikov of funds received from duped investors.

108. On January 27, 2020, Bank 5 closed Adaptive Technology's account.

109. On January 28, 2020, Sotnikov opened a new bank account for Adaptive Technology at Bank 2. Shortly thereafter, the person using Alias 2 used Email Address 3 to direct investors to wire funds to the new Adaptive Technology account at Bank 2.

110. On January 28, 2020, after receiving updated instructions from the person using Alias 2, the investors wired their $225,000 investment to Adaptive Technology's new account at Bank 2. On January 29, 2020, the investors received an "account statement" showing their $225,000 deposit.

111. On January 30, 2020, Sotnikov transferred $22,500 from Adaptive Technology's Bank 2 account to a bank account in Russia. Shortly thereafter, Adaptive Technology's account was frozen by Bank 2.

112. Also on January 30, 2020, the atlbusinessgroup.com website was taken down.

VII. Spoofed Bank 4 – Sotnikov and Adaptive Technology

113. Defendants Sotnikov and Adaptive Technology were also instrumental in the next iteration of the spoofing scheme.

114. On or about on January 28, 2020, the perpetrators registered another spoofed website with a U.S. domain registrar, using a name almost identical to that of a large financial institution offering investment banking and other services ("Spoofed Bank 4"), and created an email account ("Email Address 4") that combined the name of Spoofed Bank 4 and the name of a real broker affiliated with Spoofed Bank 4 who, upon information and belief, had no knowledge of the scheme ("Alias 3").

115. The website purported to offer high interest rate CDs from Spoofed Bank 4. The website was similar to the previous websites, offering no penalty, above-market-rate CDs. However, unlike the websites used in prior iterations of the scheme, this website identified Bank 2, Bank 4, Bank 5, and another well-known bank ("Bank 6"), all legitimate U.S. financial institutions, as clearing partner banks. The website provided the same telephone number as one of the prior websites and the same address as the real Spoofed Bank 4's Los Angeles office.

116. Two potential investors found the website through an Internet search of CD rates, called the number provided, and spoke to a person who identified himself as Alias 3, the name of an actual registered investment adviser at Spoofed Bank 4.

117. On January 29, 2020, one of the investors received a follow up email from Email Address 4, in which the person using Alias 3 identified himself as a "Senior Account Executive" at Spoofed Bank 4, and provided Spoofed Bank 4's real FINRA CRD number.

118. The email to the investor, which enclosed a CD account application, stated that the fictitious bank offering the CDs "is a Registered FDIC Institution of [Spoofed Bank 4]. *Securities offered through Adaptive Technology LLC Clearing through [Bank 2]. Member FINRA/SIPC.* Investment Advisory Services offered through [Spoofed Bank 4]" (emphasis added).

119. In fact, Defendant Adaptive Technology, an entity Sotnikov formed three months earlier and that he controlled, was not a clearing firm, nor did it offer or sell legitimate CDs or other securities. Adaptive Technology had no affiliation with Spoofed Bank 4 and no affiliation with Bank 2 other than maintaining an account at Bank 2.

120. On January 29, 2020, the investor returned the completed application to purchase a $350,000 CD, and later that day received another email from an individual using Alias 3. The

second email stated that his account was "now active, and ready for funding" and instructed him to wire his investment to "our clearing partner Cleared by [Bank 2] through Adaptive Technology LLC."

121. The wire instructions directed the investor to send the funds to Adaptive Technology's Bank 2 account, an account that Sotnikov had opened the previous day and that he controlled.

122. Luckily, the potential investor conducted additional due diligence before transferring any funds pursuant to the instructions received from the person using Alias 3. The potential investor contacted the real Spoofed Bank 4 investment advisor whose identity was being used by the perpetrators, learned that the website was fake, and did not wire any funds to Adaptive Technology.

123. The Spoofed Bank 4 website was taken down on February 4, 2020 after Spoofed Bank 4 complained to the domain registrar.

VIII. Spoofed Bank 5 – Defendants Sotnikov and AGQ Business Group

124. Defendants Sotnikov and AGQ Business Group were instrumental to the latest iteration of the scheme, which is markedly similar to other iterations described in this Complaint.

125. On February 3, 2020, Sotnikov formed Defendant AGQ Business Group, listing himself as "manager" in papers filed with the State of Florida. On February 19, 2020, Sotnikov opened a bank account for AGQ Business Group at Bank 3. The account opening documents state that AGQ Business Group is in the "[f]looring and kitchen construction" business. Sotnikov has sole signatory authority over the account.

126. Based on information and belief and available bank records, Sotnikov is a 36-year-old Russian citizen who lives in Florida, but in opening the Bank 3 account for AGQ

Business Group, he falsely claimed to be a 34-year old Spanish citizen living in Milan, Italy and presented a false Spanish passport.

127. On February 11, 2020, using a domain registrar in Russia, the perpetrators registered a website using a domain name similar to that of a well-known national bank ("Spoofed Bank 5").

128. The website described high-interest-rate, no-penalty CDs with a minimum deposit of $200,000 purportedly offered by an affiliate of Spoofed Bank 5. The website claimed that all accounts were FDIC-insured and that deposits in those accounts were maintained by Spoofed Bank 5 and cleared by "[Spoofed Bank 5] Clearing Systems (DGQ & ***AGQ***)" (emphasis added).

129. On February 13, two investors who inquired about the CDs offered on the website received introductory emails from an individual claiming to be a "Senior Account Executive" at Spoofed Bank 5 and using the name of a real registered investment adviser employed by an affiliate of Spoofed Bank 5 ("Alias 4") who, upon information and belief, had no knowledge of the scheme. The person using Alias 4 used the FINRA CRD number for the real investment adviser of the same name.

130. The email attached a CD application nearly identical to the applications used by the perpetrators in prior iterations of the scheme, and stated: "Securities offered through *clearing via DGQ,* ***AGQ****, & [Spoofed Bank 5] FDIC. Member FINRA/SIPC.* Investment Advisory Services offered through [Spoofed Bank 5] Direct Banking Group & Wealth Management" (emphasis added).

131. After submitting a completed application on February 19, the investors received the standard welcoming email explaining that their CD account was "now active and ready for funding," and attaching wire instructions. The emails and wiring instructions from the person

using Alias 4 claimed that the CDs were "[c]leared by ***AGQ Business Group LLC*** through [Bank 3]" (emphasis added). The wiring instructions directed the investors to wire their funds to the AGQ Business Group account at Bank 3.From February 21 to 26, 2020, six investors wired a total of $1,838,000 to AGQ Business Group's Bank 3 account, an account controlled by Sotnikov: On February 21, 2020, two investors wired $450,000; on February 25, 2020, another investor wired $232,000; on February 25, 2020, another investor wired $931,000; and on February 26, 2010, another investor wired $225,000 into the account. Within a business day of wiring their funds, investors received fictitious "account statements" showing their opening balance and a credit for the wire transfer fee. At least one of the fictitious account statements included an amount for "interest earned" in the "account balance."

132. On February 21, 2020, the two investors wired $450,000 to AGQ Business Group's Bank 3 account. On February 24, 2020 these investors received a fictitious "account statement" showing their "opening balance," "interest earned," and a "credit" for the wire transfer fee.

133. On February 21, 2020, two additional investors who had inquired about the CDs offered on the website received a similar introductory email from the person using Alias 4. On February 25, 2020, after submitting the completed application, these investors received the standard welcoming email attaching wire instructions. On February 25, 2020, these two investors wired $931,000 to the AGQ Business Group account.

134. On February 24, 2020, another investor who inquired about the CDs offered on the website received a similar introductory email from a person using Alias 4. After submitting the completed application, this investor received the standard welcoming email attaching wire

instructions. On February 25, 2020, this investor wired $232,000 to the AGQ Business Group account at Bank 3, and received a fictitious "account statement" on February 26, 2020.

135. Another investor who inquired about the CDs offered on the website received a similar introductory email from an individual using Alias 4. After submitting the completed application on February 25, 2020, this investor received the standard welcoming email attaching wire instructions. On February 26, 2020 this investor wired $225,000 to the AGQ Business Group account at Bank 3, and received a fictitious "account statement" on February 27, 2020.

136. On February 21, 2020, Defendant Sotnikov wrote a check for $250,000 from AGQ Business Group's Bank 3 account to Relief Defendant Inteko Cargo, another LLC he controls. The check was deposited into an Inteko Cargo account at Bank 5, an account opened and controlled by Sotnikov. That same day, Sotnikov wrote a check to himself from the Inteko Cargo account at Bank 5 for $190,000, which was deposited into an unidentified account at a Florida bank. Upon information and belief, the remaining funds in AGQ Business Group's account at Bank 3 have been frozen.

FIRST CLAIM FOR RELIEF

Violations of Section 17(a)(1) and 17(a)(3) of the Securities Act

(Defendants Sotnikov, Adaptive Technology, AGQ Business Group, ATL Business Group, BO&SA, DN Industrial, and Expert Digital)

137. The Commission re-alleges and incorporates paragraphs 1 through 136 as if fully set forth herein.

138. Sotnikov and the Defendant LLCs, by use of the means or instrumentalities of interstate commerce or of the mails, in the offer or sale of securities, directly or indirectly, with scienter, employed devices, schemes, or artifices to defraud; and/or engaged in any transaction,

practice, or course of dealing which operated or would operate as a fraud or deceit upon the purchaser.

139. By reason of the actions alleged herein, Sotnikov and the Defendant LLCs violated Section 17(a)(1) and 17(a)(3) of the Securities Act [15 U.S.C. § 77q(a)(1), (3)] and unless restrained and enjoined will continue to do so.

SECOND CLAIM FOR RELIEF

Violations of Section 10(b) of the Exchange Act and Rule 10b-5(a) and 10b-5(c)

(Defendants Sotnikov, Adaptive Technology, AGQ Business Group, ATL Business Group, BO&SA, DN Industrial, and Expert Digital)

140. The Commission re-alleges and incorporates paragraphs 1 through 136 as if fully set forth herein.

141. By engaging in the conduct described above, Sotnikov and the Defendant LLCs, with scienter, by use of the means or instrumentalities of interstate commerce, in connection with the purchase or sale of a security: (a) employed devices, schemes, or artifices to defraud; (b) made untrue statements of material fact or omitted to state material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading; and/or (c) engaged in acts, practices or courses of conduct which operated or would operate as a fraud or deceit.

142. By reason of the actions alleged herein, Sotnikov and the Defendant LLCs violated Section 10(b) of the Exchange Act [15 U.S.C. § 78j(b)] and Rules 10b-5(a) and 10b-5(c) thereunder [17 C.F.R. § 240.10b-5(a), (c)] and unless restrained and enjoined will continue to do so.

THIRD CLAIM FOR RELIEF

Aiding and Abetting Violations of Section 17(a) of the Securities Act

(Defendant Sotnikov)

143. The Commission realleges and incorporates by reference each and every allegation in paragraphs 1 through 136, inclusive, as if they were fully set forth herein.

144. Sotnikov, by engaging in the conduct described above, singly or in concert, directly or indirectly, knowingly or recklessly provided substantial assistance to the Defendant LLCs, each of which by use of the means or instrumentalities of interstate commerce, or by use of the mails, in the offer or sale of securities, knowingly or recklessly employed devices, schemes, or artifices to defraud; and knowingly, recklessly or negligently engaged in transactions, practices, or courses of business which operated or would operate as a fraud or deceit upon purchasers of securities.

145. By engaging in the conduct described above, Sotnikov aided and abetted, and, unless restrained and enjoined, will continue aiding and abetting, violations of Sections 17(a) of the Securities Act [15 U.S.C. § 77q(a)].

FOURTH CLAIM FOR RELIEF

Aiding and Abetting Violations of Section 10(b) of the Exchange Act

(Defendant Sotnikov)

146. The Commission realleges and incorporates by reference each and every allegation in paragraphs 1 through 136, inclusive, as if they were fully set forth herein.

147. Sotnikov, by engaging in the conduct described above, singly or in concert, directly or indirectly, knowingly or recklessly provided substantial assistance to the Defendant LLCs, who in connection with the purchase or sale of securities, by use of the means or instrumentalities of interstate commerce, or of the mails, or of any facility of any national

securities exchange, knowingly or recklessly employed devices, schemes, or artifices to defraud; and knowingly or recklessly engaged in acts, practices, or courses of business which would operate as a fraud or deceit upon other persons.

148. By engaging in the conduct described above, Sotnikov aided and abetted, and, unless restrained and enjoined, will continue aiding and abetting, violations of 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].

FIFTH CLAIM FOR RELIEF

Unjust Enrichment

(Relief Defendants Mazitova, Great Imperial, HRC Clearing, and Inteko Cargo)

149. The Commission realleges and incorporates by reference each and every allegation in paragraphs 1 through 136, inclusive, as if they were fully set forth herein.

150. Between February 2019 and February 2020, the Defendants have diverted to accounts held in the name of the Relief Defendants proceeds from the Defendants' fraudulent scheme as part of, and in furtherance of, the securities law violations alleged above.

151. The Relief Defendants have no legitimate claim to these ill-gotten gains, which are proceeds of the securities fraud alleged above, and it is not just, equitable, or conscionable for the Relief Defendants to retain the funds.

152. Accordingly, the Relief Defendants are liable as Relief Defendants for unjust enrichment and must disgorge the amount of their ill-gotten gains.

PRAYER FOR RELIEF

WHEREFORE, the SEC respectfully requests that the Court enter a judgment:

(i) Finding that Sotnikov, Adaptive Technology, AGQ Business Group, ATL Business Group, BO&SA, DN Industrial, and Expert Digital violated the provisions of the federal securities laws as alleged herein;

(ii) Finding that Sotnikov aided and abetted the violations of the federal securities laws committed by the Defendant LLCs as alleged herein;

(iii) Permanently restraining and enjoining Sotnikov, Adaptive Technology, AGQ Business Group, ATL Business Group, BO&SA, DN Industrial, and Expert Digital from violating Section 10(b) of the Exchange Act and Rule 10b-5 thereunder and Section 17(a) of the Securities Act;

(iv) Permanently restraining and enjoining Sotnikov from, directly or indirectly, aiding and abetting violations of Section 17(a) of the Securities Act, Section 10(b) of the Exchange Act and Rule 10b-5 thereunder;

(v) Ordering Sotnikov, Adaptive Technology, AGQ Business Group, ATL Business Group, BO&SA, DN Industrial, and Expert Digital to disgorge an amount equal to the proceeds of the conduct alleged herein and to pay prejudgment interest thereon;

(vi) Ordering Sotnikov, Adaptive Technology, AGQ Business Group, ATL Business Group, BO&SA, DN Industrial, and Expert Digital to pay a civil monetary penalty pursuant to Section 21A of the Exchange Act and Section 20(b) of the Securities Act;

(vii) Ordering the Relief Defendants to disgorge all ill-gotten gains to which they do not have a legitimate claim received as a result of the conduct alleged in the Complaint, together with prejudgment interest; and

(viii) Granting such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, the Commission demands trial by jury in this action of all issues so triable.

Dated: March 13, 2020

Respectfully submitted,

/s/John J. Bowers

John J. Bowers
Thomas A. Bednar
100 F Street, NE
Washington, DC 20549-4473
Telephone: 202-551-4645 (Bowers)
Email: bowersj@sec.gov

COUNSEL FOR PLAINTIFF SECURITIES AND EXCHANGE COMMISSION

DESIGNATION OF AGENT FOR SERVICE

Pursuant to Local Rule 101.1(f), because Plaintiff 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 an alternative to the Commission to receive service of all notices or papers in the captioned action. Therefore, service upon the United States Attorney's Office or its authorized designee:

David E. Dauenheimer
Deputy Chief, Government Fraud Unit
United States Attorney's Office
District of New Jersey
970 Broad Street, Suite 700
Newark, NJ 07102-2534

shall constitute service upon the Commission for purposes of this action.

Dated: March 13, 2020

Respectfully submitted,

/s/John J. Bowers

John J. Bowers
100 F Street, NE
Washington, DC 20549-4473
Telephone: 202-551-4645
Email: *bowersj@sec.gov*

COUNSEL FOR PLAINTIFF SECURITIES AND EXCHANGE COMMISSION