
**UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY**

UNITED STATES OF AMERICA : **TO BE FILED UNDER SEAL**
:
v. : Hon.
:
DENIS SOTNIKOV A/K/A : Mag. No. **20-XXXX**
"DENIS GEORGIYEVICH :
SOTNIKOV" : **CRIMINAL COMPLAINT**

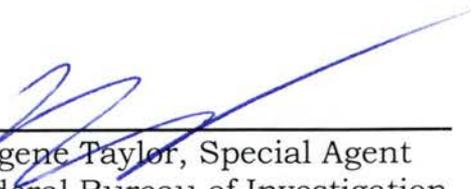
I, Eugene Taylor, being duly sworn, state the following is true and correct to the best of my knowledge and belief:

SEE ATTACHMENT A

I further state that I am a Special Agent with the Federal Bureau of Investigation, and that this Complaint is based on the following facts:

SEE ATTACHMENT B

continued on the attached pages and made a part hereof.



Eugene Taylor, Special Agent
Federal Bureau of Investigation

Sworn to before me, and
subscribed in my presence

March 11, 2020 at
Newark, New Jersey

HONORABLE MARK FALK
UNITED STATES MAGISTRATE JUDGE



Signature of Judicial Officer

ATTACHMENT A

COUNT ONE

(Conspiracy to Launder Monetary Instruments)

From in or around February 2019 through the present, in the District of New Jersey and elsewhere, defendant

DENIS SOTNIKOV

a/k/a

“DENIS GEORGIYEVICH SOTNIKOV”

did knowingly combine, conspire, and agree with other individuals to knowingly conduct and attempt to conduct financial transactions affecting interstate and foreign commerce, which transactions involved the proceeds of specified unlawful activity, that is, wire fraud, knowing that the transactions were designed in whole and in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of specified unlawful activity, and that while conducting and attempting to conduct such financial transactions, knew that the property involved in the financial transactions represented the proceeds of some form of unlawful activity, contrary to Title 18, United States Code, Sections 1956(a)(1)(B)(i).

In violation of Title 18, United States Code, Section 1956(h).

ATTACHMENT B

I, Eugene Taylor, being first duly sworn, depose and state the following:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"). I have been employed by the FBI as a Special Agent since August 2016. My experience as an FBI agent has included the investigation of cases involving mail fraud, wire fraud, and the use of computers to commit such offenses. I have received training and have gained experience in interview and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, computer crimes, computer evidence identification, computer evidence seizure and processing, and various other criminal laws and procedures. I have further received training and have gained experience in the investigation of financial crimes, including money laundering, as well reviewing bank records.

2. Since this Affidavit is submitted for the sole purpose of establishing probable cause to support the issuance of a federal criminal complaint and arrest warrant, I have not included each and every fact known by the Government concerning this investigation. Except as otherwise indicated, the actions, conversations, and statements of others identified in this Affidavit – even where they appear in quotations – are reported in substance and in part. Similarly, dates and times are approximations, and should be read as "on or about," "in or about," or "at or about" the date or time provided.

OVERVIEW OF THE FRAUD

3. From at least as early as April 2018 to the present, individuals both known and unknown (the "Subjects") have engaged in an internet-based, financial fraud scheme, in which at least 70 victims nationwide, including in New Jersey, have collectively transmitted funds in the approximate amount of \$30 million that they believed to be investments.

4. To lure potential victims, the Subjects created fraudulent websites (the "Fraud Websites") to solicit funds on the internet from individuals seeking to invest money. At times, the Fraud Websites were designed to closely resemble websites being operated by actual, well-known, and publicly reputable financial institutions; at other times, the Fraud Websites were designed to resemble legitimate-seeming financial institutions that did not, in fact, exist. Victims of the fraud typically discovered the Fraud Websites via internet searches. The Fraud Websites advertised various types of investment opportunities, most prominently the purchase of certificates of deposit ("CDs"). The Fraud Websites would advertise higher than average rates of return on CDs to enhance the attractiveness of the investment opportunities to potential victims.

5. Multiple victims of the scheme attempted to purchase CDs that were offered through one or more of the Fraud Websites. In many instances, the victim would contact an individual or individuals via telephone or email as directed on a Fraud Website (the "Fraud Contact"). The Fraud Contact would cause the victim to receive various documents, including, but not limited to, account applications, term sheets, and wiring instructions related to the purchase of a CD. The victim would complete and submit the paperwork, follow the wiring instructions, and wire funds to the bank account specified by the Fraud Contact. The funds would be moved out of the specified bank account to various international and domestic bank accounts. Law enforcement has determined that the funds transmitted by the victims in accordance with the above-described procedure were not used to procure CDs or any other advertised investment products, and none of the victims actually took ownership of the products that they intended to purchase.

6. The Fraud Websites identified through the course of the investigation often used identical or very similar wording and included many identical features. For example, many of the Fraud Websites included the phrase "extraordinary rates for your extraordinary life," and a vast majority of the Fraud Websites featured four tabs at the top of the website's home page, with the text "current CD rates," "high yield CDs," "why [followed by the name of the entity associated with the Fraud Website]," and "privacy." The Fraud Websites also often listed the same Fraud Contact name across multiple different Fraud Websites, which purported to be associated with entirely different financial institutions. Moreover, investors would be required to fill out the same paperwork and follow an identical procedure to apply for and wire funds related to the purchase of a CD through the Fraud Websites. The paperwork required to be filled out by the fraud victims was often identical in format, despite being associated with different entities. It was further determined that the Subjects paid for the Fraud Websites from many of the same bank accounts. Finally, many of the Fraud Websites listed the same physical address or same phone number for apparent different entities.

OVERVIEW OF THE MONEY LAUNDERING CONSPIRACY

7. Defendant DENIS SOTNIKOV ("SOTNIKOV") received funds from at least eighteen victims of the fraudulent scheme, totaling approximately \$6 million, in accounts at various domestic banks that were controlled by him or by a close relative (the "Relative") (the "SOTNIKOV Accounts"). Of this amount, approximately \$3.7 million was either frozen by the banks or returned to victims, and approximately \$707,380 was wired by SOTNIKOV to bank accounts in Hong Kong and Turkey. The remaining stolen funds—approximately \$1.5 million—were used by SOTNIKOV and the Relative to fund personal expenditures, including down payments on several luxury vehicles, purchases at high-end retail stores such as Louis Vuitton, Tiffany & Co., and Cartier, rent exceeding \$9,000 per month on a home in or around Hallandale Beach, Florida (the "Hallandale Beach Address"), several vacations, and everyday living expenses and bills.

8. SOTNIKOV received victim funds in accounts opened in the names of registered businesses for which SOTNIKOV served as agent or manager. SOTNIKOV then transferred a substantial amount of the victim funds to other accounts controlled by him or by the Relative, including accounts at various banks that they held in their personal capacities and not on behalf of a corporate entity. Throughout the scheme, SOTNIKOV used more than twenty different accounts at at least seven different banks to accept and move victim funds.

9. At times throughout the fraud, some of the SOTNIKOV Accounts were frozen or closed by banks due to allegations of fraud. Even after being told by bank representatives that certain accounts were being closed due to fraud, SOTNIKOV continued to open new accounts at different banks, which were thereafter used to accept victim funds. SOTNIKOV additionally provided at least one bank with fraudulent documentation regarding the source of a victim's money and provided still another bank with false personal identifying information when opening an account used to accept victim funds.

INDIVIDUALS, ENTITIES, AND BANK ACCOUNTS

10. At various times relevant to this Complaint:

a. SOTNIKOV was a resident of Florida.

b. SOTNIKOV was associated with various corporate entities that were used to maintain accounts at banks, as follows:

i. SOTNIKOV was the registered agent and manager of DN Industrial, LLC ("DN Industrial"), a Florida company, and maintained bank accounts under the name "DN Industrial, LLC" at Banks A, B, C, and D. The listed address for DN Industrial was a location in Sunny Isles Beach, Florida (the "Sunny Isles Address").

ii. SOTNIKOV was the manager of HRC Clearing House, LLC ("HRC"), a Florida company, and SOTNIKOV maintained a bank account under the name "HRC Clearing House, LLC" at Bank F. The listed address for HRC was the Sunny Isles Address.

iii. SOTNIKOV was the manager of Inteko Cargo, LLC ("Inteko"), a Florida company, and maintained a bank account under the names "Inteko Cargo, LLC" or "Inteco Cargo, LLC" at Banks A, B, C, F and G. The listed address for Inteko was the Sunny Isles Address.

iv. SOTNIKOV was the registered agent and manager of Expert Digital, LLC ("Expert Digital"), a New York company, and maintained a bank account under the name "Expert Digital, LLC" at Bank B. The listed address for Expert Digital was an address in or around Hollywood, Florida (the "Hollywood Address").

v. SOTNIKOV was a registered agent and president of BO & SA Corp. ("BO & SA"), a Florida corporation, and maintained a bank account under the name "BO & SA Corp." at Bank A. The listed address of BO & SA was the Hollywood Address.

vi. SOTNIKOV was the manager of ATL Business Group, LLC ("ATL"), a Wyoming company, and maintained a bank account under the name "ATL Business Group, LLC" at Bank D.

vii. SOTNIKOV was the manager of AGQ Business Group, LLC ("AGQ"), a Florida company, and maintained a bank account under the name "AGQ Business Group" and Bank C. The listed address for AGQ was the Hollywood Address.

c. The Relative was the registered agent and manager of Company-1, a Florida company, and maintained bank accounts under Company-1's name at Banks A, C, and D.

d. Banks A through G were financial institutions as defined in Title 18, United States Code, Section 1956(c)(7), and Title 31, United States Code, Section 5312.

e. Bank D maintained a wire processing facility located in Mount Laurel, New Jersey, which processed all wire transfers to and from Bank D.

f. Victims-1, -5, -6, and -12 were residents of Florida.

g. Victims-2 and -11 were residents of Texas.

h. Victim-3 was a resident of Washington.

i. Victim-4 was a resident of Louisiana.

j. Victim-7 was a resident of New York.

k. Victim-8 was a resident of Nebraska.

l. Victim-9 was a resident of Arizona.

m. Victim-10 was a resident of Delaware.

THE FLOW OF FRAUDULENTLY OBTAINED FUNDS

Victims-1 through -3

11. On or about February 15, 2019, Victim-1 authorized a transfer of \$250,000 to an account held at Bank A under the name DN Industrial, LLC (the "Bank A DN Industrial Account"). Victim-1 transferred the funds after visiting a Fraud Website ("Fraud Website-1") and receiving banking instructions from a Fraud Contact using a name with the initials M.K ("the M.K. Fraud Contact"). Victim-1 believed that the funds were for the purchase of a CD from a financial institution associated with Fraud Website-1.

12. SOTNIKOV was the signatory to the Bank A DN Industrial Account. At the time of the transfer from Victim-1, the Bank A DN Industrial Account had a balance of \$59.74 and previously had not maintained a balance higher than \$6,390.

13. On or about February 25, 2019 and on or about February 28, 2019, Victim-2 and Victim-3 wired \$383,000 and \$200,000, respectively, to the Bank A DN Industrial Account. Victims-2 and -3 wired the funds after visiting Fraud Website-1 and receiving wiring instructions from the M.K. Fraud Contact for what Victims-2 and -3 believed was the purchase of a CD.

14. Victims-1, -2, and -3 never received a CD or any other investment product after wiring the funds as described above.

15. After receiving the total of \$833,000 in funds from Victims-1, -2, and -3, SOTNIKOV wired \$707,380 to financial institutions in Hong Kong and Turkey in five separate wire transactions. The wire transactions initiated by SOTNIKOV occurred just days after the transfers by the victims, and, on two occasions, the next day. A portion of the remaining \$125,620 was used to pay an entity used by the Subjects to publish advertisements associated with the Fraud Websites. The remainder was wired to other accounts controlled by SOTNIKOV or the Relative and used for personal expenses, including the purchase of a 2019 Land Rover Range Rover on or about February 25, 2019.

16. SOTNIKOV made rapid transfers between different accounts that he controlled at Bank A with portions of the funds that he ultimately transferred to one of the overseas accounts. For example, on or about February 22, 2019, approximately one week after receiving funds from Victim-1, SOTNIKOV transferred \$130,000 to another business account held by him at Bank A. Four days later, SOTNIKOV transferred \$130,000 back to the Bank A DN Industrial Account. On the same day, SOTNIKOV initiated a wire transfer in the amount of \$130,000 to a bank in Hong Kong. The above transactions served to conceal and disguise the nature, location, source, ownership, and control of the funds transferred by Victims-1, -2, and -3.

Victim-4

17. On or about March 22, 2019, Victim-4 wired \$240,000 to an account held at Bank B under the name DN Industrial, LLC (the "Bank B DN Industrial Account") for what Victim-4 believed was for the purchase of a CD. Victim-4 discovered an advertisement for a Fraud Website ("Fraud Website-2"). After visiting the website, Victim-4 exchanged emails with the M.K. Fraud Contact, who provided Victim-4 with wiring instructions. After wiring the funds, Victim-4 never received a CD or any other investment product.

18. SOTNIKOV was the signatory to the Bank B DN Industrial Account. After SOTNIKOV received the funds from Victim-4, the funds were wired or transferred to other SOTNIKOV Accounts before ultimately being moved to an account held by the Relative, where they were used to pay for various personal expenses, including a down payment on the purchase of a 2019 Mercedes Benz S450V.

19. At the time of Victim-4's wire transfer, the Bank B DN Industrial Account had a balance of \$2,930.48. The account was funded by other SOTNIKOV Accounts and previously had not maintained a balance higher than approximately \$13,000. The account had minimal activity prior to the incoming wire from Victim-4.

Victim-5 and Victim-6

20. On or about March 21 and 27, 2019, Victim-5 wired a total of \$750,000 to an account held at Bank C under the name DN Industrial, LLC (the "Bank C DN Industrial Account"). Also on or about March 27, 2019, Victim-6 wired \$200,000 to the Bank C DN Industrial Account.

21. Victims-5 and -6 believed that the funds wired to the Bank C DN Industrial Account were for the purchases of CDs from a financial institution associated with one of the Fraud Websites ("Fraud Website-3"). Both Victims-5 and -6 exchanged emails with the M.K. Fraud Contact, who provided wiring instructions.

22. SOTNIKOV was the signatory to the Bank C DN Industrial Account. At the time of Victim-5's wire transfer on March 22, 2019, the Bank C DN Industrial Account had a balance of \$0 and minimal prior account activity.

23. SOTNIKOV made rapid transfers between different accounts that he controlled at Bank C on behalf of a different corporate entity with portions of the funds that he received in the Bank C DN Industrial Account. For example, after SOTNIKOV received the funds from Victims-5 and -6, SOTNIKOV initiated two bank transfers of \$20,000 and \$29,000, respectively, to two different Bank C Accounts controlled by SOTNIKOV and held under the business name "Inteco Cargo, LLC" (the "Inteco Accounts"). SOTNIKOV was the signatory on the Inteco Accounts. The funds transferred to the Inteco Accounts were frozen by Bank C before they could be spent or transferred further. The remaining funds in the

Bank C DN Industrial Account were also frozen by Bank C before they could be transferred or withdrawn. The above transactions served to conceal and disguise the nature, location, source, ownership, and control of the funds transferred by Victims-5 and -6.

24. Victims-5 and -6 did not receive a CD or any other investment product.

25. The Bank C DN Industrial Account was closed on or about April 24, 2019. On or about April 9 and 11, 2019, SOTNIKOV communicated with a Bank C representative via telephone regarding the Bank C DN Industrial Account. SOTNIKOV was informed by the Bank C representative on both occasions that the Bank C DN Industrial Account was being closed because the funds in the account had been recalled due to fraud.

Victim-7 and Victim-8

26. On or about May 8 and 10, 2019, Victims-7 and -8 wired \$200,000 and \$650,000, respectively, to an account held at Bank B under the name Expert Digital, LLC (the "Bank B Expert Digital Account"), for what Victims-7 and -8 believed to be purchases of CDs.

27. According to Victims-7 and -8, each visited a Fraud Website ("Fraud Website-4") and communicated with the M.K. Fraud Contact, who provided wiring instructions. Victims-7 and -8 did not receive a CD or any other investment product.

28. Fraud Website-4 used the name of a real, legitimate financial institution. However, the domain name associated with Fraud Website-4 and the email address used by the Fraud Contact were spoofed, that is, the Subjects used accounts that closely resembled but subtly differed from accounts used by the real, legitimate financial institution in an effort to deceive potential victims.

29. SOTNIKOV was the signatory to the Bank B Expert Digital Account.

30. After SOTNIKOV received the wire from Victim-7, SOTNIKOV initiated a bank transfer of \$70,000 to another Bank B account held under the business name Inteko Cargo, LLC (the "Bank B Inteko Account"). SOTNIKOV was the signatory to the Bank B Inteko Account and the registered agent for Inteko Cargo, LLC, a Florida company.

31. On or about May 8, 2019, Bank B froze the funds in the Bank B Expert Digital and Inteko Accounts, before any additional funds could be transferred or spent.

32. At the time of Victim-7's transfer on or about May 8, 2019, the Bank B Expert Digital Account had a balance of \$1,295.87 and minimal previous account activity.

Victim-9 and Victim-10

33. On or about May 10 and 15, 2019, Victims-9 and -10 wired \$207,000 and \$200,000, respectively, to an account held at Bank E in the name BO & SA Corp. (the "Bank E BOSA Account"). Victims-9 and -10 visited a Fraud Website ("Fraud Website-5") and communicated with the M.K. Fraud Contact, who provided wiring instructions for purchases of CDs.

34. Fraud Website-5 used the name of the same real, legitimate financial institution associated with Fraud Website-4. The domain name associated with Fraud Website-5 and the email address used by the Fraud Contact were also spoofed versions of accounts associated with the real, legitimate financial institution, although they differed from the spoofed accounts used for Fraud Website-4.

35. The Bank E BOSA Account was opened in the name of BO & SA Corp., and its signatory was Individual-1. The Bank E BOSA Account was funded by the Bank B Expert Digital Account. At the time of the transfer by Victim-9, the Bank E BOSA Account had a balance of \$1,010 and minimal previous account activity.

36. After the funds were wired by Victims-9 and -10, the person or persons controlling the Bank E BOSA Account: (a) initiated a \$50,000 wire transfer to an account held by SOTNIKOV at Bank F under the name HRC Clearing House (the "Bank F HRC Account"); (b) wrote a \$150,000 check to SOTNIKOV, which SOTNIKOV deposited in a personal account held by SOTNIKOV at Bank D; (c) wrote a \$20,000 check to the Relative, which SOTNIKOV deposited in an account held by the Relative at Bank D; and (d) wrote a \$178,000 check to HRC Clearing House, LLC, which was deposited in the Bank F HRC Account. The above transactions served to conceal and disguise the nature, location, source, ownership, and control of the funds transferred by Victims-9 and -10.

37. Following these transfers, the funds were used for personal expenses, either directly from the recipient accounts or after additional transfers to still other accounts held by SOTNIKOV and the Relative. For example, following the \$150,000 and \$20,000 deposits into the Bank D accounts referenced in the previous paragraph, approximately \$18,000 was transferred from the accounts to Tiffany & Co. for the purchase of jewelry.

Victim-11 and Victim-12

38. On or about January 10 and 21, 2020, Victims-11 and -12 wired \$250,000 and \$500,000, respectively, to an account held at Bank D in the name ATL Business Group (the "Bank D ATL Account"). Victims-11 and -12 visited a Fraud Website ("Fraud Website-6") and were provided wiring instructions for purchases of CDs. Fraud Website-6 solicited investment opportunities under the business name "ATL Wealth."

39. SOTNIKOV was the signatory to the Bank D ATL Account, which listed the Hallandale Beach Address as the account address. The Hallandale Beach Address was purchased in the name of the Relative in July 2019. The down payment on the apartment was made using victim funds, including funds that originated from Victims-9 and -10.

40. Following the wire transfers from Victims-11 and -12, SOTNIKOV initiated a series of rapid transactions from the Bank C DN Industrial Account. For example, three days after Victim-11's \$250,000 wire transfer, SOTNIKOV made a \$9,000 withdrawal and wired \$215,000 to an account held by the Relative at Bank C. One day after Victim-12's \$500,000 wire transfer, SOTNIKOV transferred \$5,000 to a personal account held by him at Bank D, wired \$15,000 to an account held by the Relative at Bank C, and wrote a \$470,000 check, which was deposited to an account held by SOTNIKOV at Bank F in the name Inteko Cargo, LLC (the "Bank F Inteko Account"). SOTNIKOV then wrote a check drawn upon the Bank F Inteko Account in the amount of \$465,000, which SOTNIKOV deposited into an account held by the Relative at Bank C. The above transactions served to conceal and disguise the nature, location, source, ownership, and control of the funds transferred by Victims-11 and -12.

41. At the time of Victim-11's wire transfer, the Bank D ATL Account had a balance of \$100.01 and was opened only two weeks prior to accepting funds from Victim-11.

42. A representative of Bank D (the "Bank D Representative") spoke with SOTNIKOV on or about January 27, 2020. The Bank D Representative advised SOTNIKOV that there was fraudulent activity in the ATL Account and that SOTNIKOV'S accounts at Bank D would be closed. SOTNIKOV thereafter provided Bank D with a fraudulent invoice, which purported to show that Victim-11's wired funds were for the purchase of stereo equipment. The invoice listed the Hallandale Beach Address as the address for ATL Business Group.

Other Activity

43. On or about January 28, 2020, SOTNIKOV opened a new bank account at Bank C under the name AGQ Business Group, LLC (the "Bank C AGQ Account"). The Bank C AGQ Account subsequently was used to accept funds from four additional victims, including a victim in New Jersey, totaling approximately \$1.8 million, of which \$1.3 million was frozen by Bank C.

44. At the time SOTNIKOV opened the Bank C AGQ Account, he provided Bank C with Spanish passport in his own name and listed his residence as an address in Italy. SOTNIKOV also provided Bank C with a false date of birth. SOTNIKOV is known to be a citizen of the Russian Federation and is currently living in the United States on a B1/B2 visa.

CONCLUSION

For the foregoing reasons, there is probable cause to believe that SOTNIKOV engaged in the offense of Money Laundering Conspiracy, contrary to Title 18, United States Code, Section 1956(a)(1)(B)(i), in violation of Title 18, United States Code, 1956(h).