

SK:DEL

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE APPLICATION
OF THE UNITED STATES OF AMERICA
FOR ARREST WARRANTS FOR YAKOV
MOROZ AND TAL OHANA AND FOR
SEARCH WARRANTS FOR THE PREMISES
KNOWN AND DESCRIBED AS 125
OCEANA DRIVE EAST, APT 5B,
BROOKLYN, NEW YORK AND 1733
SHEEPSHEAD BAY ROAD, SUITE 21,
BROOKLYN, NEW YORK

TO BE FILED UNDER SEAL

COMPLAINT AND AFFIDAVIT IN
SUPPORT OF APPLICATION FOR
ARREST WARRANTS AND
SEARCH WARRANTS

(T. 18, U.S.C. §§ 1343, 1349)

20 MJ 604

AFFIDAVIT IN SUPPORT OF ARREST WARRANTS
AND AN APPLICATION UNDER RULE 41 FOR
WARRANTS TO SEARCH AND SEIZE

EASTERN DISTRICT OF NEW YORK, SS:

Brian P. Smith, being duly sworn, deposes and states that he is a Special Agent with the Federal Bureau of Investigation (“FBI”), duly appointed according to law and acting as such.

Upon information and belief, in or about and between August 2019 and the present, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants YAKOV MOROZ and TAL OHANA, together with others, did knowingly and intentionally devise a scheme and artifice to defraud customers and potential customers of Great Movers Inc., also doing business as “Great Moving” and “Great Moving USA” (hereinafter “Great Movers”), and to obtain money and property from them by means of materially false and fraudulent pretenses, representations and promises, and for the purpose

of executing such scheme and artifice, did transmit and cause to be transmitted, by means of wire communication in interstate commerce, writings, signs, signals, pictures and sounds, contrary to Title 18, United States Code, Section 1343.

(Title 18, United States Code, Sections 1343 and 1349)

INTRODUCTION

A. Background of Affiant

1. I am a Special Agent with the FBI and have been since 2018. As part of my duties as an FBI Special Agent, I have participated in numerous investigations of violations of federal offenses including mail and wire fraud. I have completed the analysis of various devices and online accounts containing electronic data, including electronic mobile devices, computers, laptops, external storage devices, email accounts, and social media accounts. I also have experience conducting physical surveillance, interviewing witnesses, executing court-authorized search warrants and using other investigative techniques to secure relevant information. In addition to these skills, I have experience investigating and charging violations of federal law in connection with moving companies engaged in the transportation of household goods.

2. I make this affidavit in support of an application for arrest warrants for YAKOV MOROZ and TAL OHANA for violations of Title 18, United States Code, Sections 1343 and 1349, and for an application pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search:

- a. the premises known and described as 1733 Sheepshead Bay Road, Suite 21, Brooklyn, New York (“MOROZ OFFICE”), as described in Attachment A.I, for the items and information described in Attachment B; and

- b. the premises known and described as 125 Oceana Drive East, Apt 5B, Brooklyn, New York (“MOROZ RESIDENCE”), as described in Attachment A.II, for the items and information described in Attachment B.

3. This affidavit is based upon my personal knowledge, including my interviews with victims and review of written contracts, communications and other documents, as well as my conversations with other law enforcement personnel and my training and experience. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

B. The Subject Offenses

4. For the reasons detailed below, I submit that there is probable cause to believe that YAKOV MOROZ and TAL OHANA committed violations of Title 18, United States Code, Sections 1343 and 1349 (wire fraud and conspiracy) (the “SUBJECT OFFENSES”), and that the MOROZ RESIDENCE and the MOROZ OFFICE contains evidence, fruits, and instrumentalities of such violations.

PROBABLE CAUSE

A. Federal Regulations Governing Moving Companies

5. Companies engaged in the transportation of household goods in interstate commerce are subject to federal regulations set forth in Title 49, Code of Federal Regulations (C.F.R.), Section 375, which are enforced by Federal Motor Carrier Safety Administration (“FMCSA”), an administration within the U.S. Department of Transportation (“DOT”). A

company engaged in the transportation of household goods is required to provide customers with a written estimate of the charges for transportation and all related services based on a telephonic or physical inventory of the goods to be shipped, and to indicate whether the estimate is binding or non-binding.

6. A binding estimate is an agreement made prior to transportation that guarantees the total cost of the shipment based on the quantities and services listed in the estimate. For binding estimates, a company is required to deliver the household goods, as contracted, upon full payment of the original estimate amount. Any costs associated with the shipment of additional household goods or services that were not identified in the binding estimate are permitted to be billed only after the goods are delivered. 49 C.F.R. § 375.403. Accordingly, it is not permissible to require additional costs be paid before delivery or make delivery contingent on additional costs.

7. For non-binding estimates, the final charges are based on the actual weight or volume of the shipment, the services provided and the tariff provisions in effect. The final charges for a shipment involving a non-binding estimate are not permitted to be increased above the initial estimate by more than 10 percent. 49 C.F.R § 375.703(b).

B. Great Movers and New City Movers

8. On or about August 20, 2019, Great Movers filed a Motor Carrier Identification Report with the FMCSA noting the company formerly known as Arc Transport LLC would now operate as “Great Moving.” According to the filing, the company’s president is “Moye Gregory” and its principal office is located at 266 47th Street, Brooklyn, New York. I believe no individual named “Moye Gregory” is associated with Great Movers from my review of its records, and I visited the listed address in the application and after

reviewing the business on site, there was no indication that a business by that name (or any moving company) operates at that address.

9. In addition to the alleged Brooklyn address, in documentation provided to customers, Great Movers claims to have offices in Wisconsin and North Carolina. However, according to my own investigation and statements on the Better Business Bureau's website, both these offices are "virtual" offices, meaning there is no physical presence at those addresses. Furthermore, in communications from the same Great Movers representative (i.e., Allen Parks) to one customer, the representative listed his address as the North Carolina address, while header information listed on quotes and invoices listed the Wisconsin address. In my training and experience, these facts indicate Great Movers is attempting to obscure its physical location.

10. Furthermore, according to interviews with victims and associated emails and other documentation, Great Movers' employees included individuals named "Bill Randall" (billrandall@greatmovingusa.com), "Allen Parks" (allenparks@greatmovingusa.com) and "Patrick Murphy" (patrickmurphy@greatmovingusa.com). However, Great Movers' banking records consistent with payroll show no payments transferred such individuals. Accordingly, I believe Great Movers' employees used fictitious names in customer interactions to avoid discovery by customers and federal regulators.

11. In or about April and May 2020, Great Movers began utilizing the name New City Movers.¹ A phone call placed to a phone number associated with Great Movers on or

¹ New City Movers is assigned a DOT number that was most previously issued to Mini Movers LLC based in Blue Ash, Ohio. From January 2020 through April 2020, New City Movers filed more than four FMCSA registration forms, with each new form changing the owner's name, the principle address, the mailing address, and the telephone number. In my

about June 25, 2020, was answered by a representative with the greeting “New City Movers.” Domain registration records obtained by subpoena show the same entity purchased the website domains for both Great Movers and New City Movers. Furthermore, according to recent complaints filed by victims of New City Movers, the fraudulent scheme, discussed below in detail, remains the same.

12. In my training and experience, moving companies who defraud customers frequently change names to distance themselves from negative customer reviews and to ensure that future victims are not dissuaded from contracting for their services. As explained above, Great Movers was formed in or about August 2019 using a DOT number that had previously been assigned to a moving company of another name.

C. YAKOV MOROZ

13. YAKOV MOROZ resides at the MOROZ RESIDENCE, i.e., 125 Oceana Drive East, Apt. 5B, Brooklyn, New York, according to utility provider Con Edison and public databases. Furthermore, MOROZ is the subscriber for internet services at the MOROZ RESIDENCE with the internet protocol (“IP”) address 100.33.34.27 (“MOROZ IP ADDRESS”) and the email address speedy999@gmail.com (“MOROZ EMAIL ACCOUNT”), according to Verizon records obtained by subpoena. Additionally, on several occasions in July 2020, the MOROZ EMAIL ACCOUNT logged online via the MOROZ IP ADDRESS, according to Google records obtained by subpoena.

experience, this is consistent with efforts to obscure the identity of an owner or the location of the company to avoid law enforcement detection. On or about June 12, 2020, the FMCSA revoked New City Movers’s DOT number for failure to respond to requests for an audit.

14. There is probable cause to believe YAKOV MOROZ is the president of Great Movers, and as the president, directed and controlled the company's operations, including its financial operations. For instance:

- a. Bank Records: MOROZ controls the bank accounts for Great Movers. He listed himself as the president and signatory to operate Great Movers' bank accounts at two banking institutions, according to records obtained by subpoena. These banking records show financial transactions between Great Movers and known victims of Great Movers. In addition, the banking statements for Great Movers at one banking institution are mailed to the MOROZ RESIDENCE; and
- b. Email Accounts: From approximately September 2019 through April 2020, the MOROZ EMAIL ACCOUNT received emails from email addresses created under the Great Movers domain.² In or about April 2020, the MOROZ IP ADDRESS also accessed email addresses created under the Great Movers domain.

15. In addition to Great Movers and New City Movers, MOROZ is affiliated with multiple moving companies. According to bank records obtained by subpoena, MOROZ is listed as the president of American Choice Van Lines Inc. (signature card signed on October 26, 2018), C And D Moving Inc. (signature card signed on December 30, 2017), Compass Relocation (signature card signed on December 20, 2017), Cross Country Moving and

² On June 11, 2020, the Honorable Roanne L. Mann issued a search warrant to Microsoft in Case No. 20 MJ 430 for certain email accounts associated with Great Movers.

Storage Inc. (signature card signed on December 30, 2017; January 22, 2018; and November 21, 2018), Green Mover of America Inc. (signature card signed on April 11, 2019), Movers Consulting Inc. (signature card signed on December 30, 2017; January 1, 2018; and July 12, 2018); Nationwide Transportation Inc. (signature card signed on December 30, 2017), Roman Relocation Inc. (signature card signed on April 6, 2018), Saba Gabi Inc. (signature card signed on September 27, 2018), Transatlantic Moving Inc. (signature card signed on December 30, 2017) and Interstate Advisor (signature card signed on April 4, 2019 and May 1, 2019). MOROZ is also affiliated with Uber Movers, according to records obtained from the Better Business Bureau. In addition, a bank account for Movers Consulting Inc., one of MOROZ's companies, purchased the following domains: greatmovingusa.com, interstateadvisor.com, greenmoversofamerica.com, 1stclassmovesusa.com, greenmoversinc.com, newcitymoves.com and 1stclassmove.com.

16. Furthermore, the same phone number 917-853-1849 (the "MOROZ PHONE") is listed on bank account records for Interstate Advisor Inc., Movers Consulting Inc., New City Movers and Saba Gabi Inc. According to records obtained by subpoena, the MOROZ NUMBER has a listed subscriber of Movers Consulting Inc. and a listed address of the MOROZ RESIDENCE.

D. TAL OHANA

17. There is probable cause to believe TAL OHANA is an employee of Great Movers and participated in the fraudulent scheme, as discussed below. For instance:

- a. Bank Records: A review of bank records show at least two payments made from Great Movers and multiple other payments from Movers Consulting Inc.

- b. Email Accounts: A review of emails obtained by search warrant sent from the Great Movers email accounts show an individual named “Tal” had access to the advisor@greatmovingusa.com email account, the account that received and responded to a large number of complaints from victims related to the fraudulent scheme.
- c. Slack Messages:³ Messages sent over a Slack workspace affiliated with Great Movers Inc. show user “@Talo” communicating to other employees regarding customers of Great Movers and New City Movers. In addition, a Slack message notes that “@Talo” has a birthday on May 3, which, according to law enforcement records, is the same month and day of TAL OHANA’s birth date. Accordingly, I believe “@Talo” to be TAL OHANA.
- d. Social Media: OHANA has listed on publicly available social media sites that she has been employed by Interstate Advisor, a company affiliated with Great Movers Inc., since 2016.
- e. Photo: A user with an email account on greatmovingusa.com (patrickmurphy@greatmovingusa.com) attached OHANA’s photograph to an email.

E. The Fraudulent Scheme

18. YAKOV MOROZ and TAL OHANA, using several affiliated moving companies including Great Movers and its successor New City Movers, defrauded customers

³ Slack is an online communications platform commonly used by businesses to enable communications among employees. Slack offers multiple features including chat rooms organized by topic, private groups, and direct messaging. Slack can be accessed via computers and cellular telephones capable of hosting applications (i.e. smartphones).

and potential customers by misrepresenting the estimated charges for moving services and then requiring customers to pay additional fees, often more than 10 percent of the original estimate and/or requiring payment before delivery of goods, by refusing to return, and threatening to sell and auction, the customers' belongings if the fees were not paid.

19. As part of the scheme, YAKOV MOROZ registered or reinstated motor carrier numbers with the FMCSA, including but not limited to the number used by Great Movers, using fictitious names and business addresses.

20. According to more than 10 victim interviews, a review of dozens of additional victim complaints filed with the FMSCA and FBI and the associated documents and email messages, the scheme typically functioned as follows: After a customer contacted Great Movers by phone or through its website, a Great Movers representative provided a moving estimate, labeled binding, non-binding or unlabeled. The customer then paid a deposit for the movers. Great Movers then required the customer to pay additional fees at various points during the move, including at pick-up and before delivery. For customers with non-binding estimates, the additional fees often exceeded the 10 percent price increase restriction as set forth in Title 49, Code of Federal Regulations, Section 375.703(b). For customers with binding estimates, Great Movers required that additional costs on top of the original binding estimate be paid before delivery. If the customers refused to pay the fees, representatives of the companies refused to return the customers' belongings. Many customers ultimately paid the inflated and additional fees to ensure delivery of their property. In addition, the customers' property was delivered late and items were missing or damaged.

21. Furthermore, the victims' complaints share certain similarities. For instance, the company would often claim the same additional charges applied such as shuttle fees. I

understand a “shuttle fee” to be a fee that a long distance moving company or van line charges when it is necessary to load or unload the goods using a smaller truck because the larger tractor trailer cannot fit near the pickup and/or destination address.

22. A preliminary analysis of these complaints showed that Great Movers often increased a victim’s initial moving estimate by more than 70 percent during or after pick up and before delivery.

F. Premises to be Searched: The MOROZ OFFICE

23. The MOROZ OFFICE is located at 1733 Sheepshead Bay Road between Shore Parkway and Voorhies Avenue in Brooklyn, New York, in a building with a gray and glass façade. The first floor tenant is a business displaying the sign “Liquor World.” The doorway is marked with the address number “1733.” Upon entry, there is a digital display listing the businesses inside. “Interstate Advisor” is located on the second floor within Suite 21. Interstate Advisor is the MOROZ OFFICE. Photographs of the outside of the building and the digital display are included below and in Attachment A.I.





24. There is probable cause to believe that YAKOV MOROZ and TAL OHANA use the MOROZ office to operate the fraudulent scheme and evidence, instrumentalities, contraband and fruits of the fraudulent scheme will be found at the MOROZ OFFICE. For instance:

- a. Mail Delivery: As of July 2020, the MOROZ OFFICE receives mail addressed to YAKOV MOROZ, Great Movers, New City Movers, Interstate Advisor and Movers Inc., according to records obtained from the United States Postal Service.
- b. Bank Records: In or about April 2020, bank statements for Great Movers were mailed to the MOROZ OFFICE.
- c. Employee: TAL OHANA, who is an employee of Great Movers and participated in the fraudulent scheme, lists her employer as Interstate Advisor

on social media, which is the listed name of the MOROZ OFFICE. OHANA also physically visits the MOROZ OFFICE. On or about May 28, 2020, OHANA received a parking ticket outside the MOROZ OFFICE, according to New York City Police Department records. In or about July 2020, OHANA's vehicle was parked in the vicinity of the MOROZ OFFICE.

G. Premises to be Searched: The MOROZ RESIDENCE

25. The MOROZ RESIDENCE is located in Apartment 5B at 125 Oceana Drive East within the Oceana Condominium and Club complex. According to publicly available data, 125 Oceana Drive East is an eight-story complex which includes 108 units. It is accessible through a 24-hour attended gatehouse and security with video intercom system. The entrance to the Oceana Condominium and Club complex and the door of 125 Oceana Drive East is pictured below and in Attachment A.II.





26. As explained above in paragraph 13, YAKOV MOROZ resides at the MOROZ RESIDENCE, which is assigned the MOROZ IP ADDRESS, i.e., IP address 100.33.34.27. Other individuals, including a male relative, appear to have listed the MOROZ RESIDENCE as their address at times in the past four years, according to law enforcement records, however it is unclear whether anyone currently resides in the MOROZ RESIDENCE.⁴

⁴ Law enforcement records and further investigation show four individuals have listed the MOROZ RESIDENCE as their address at some time: an unrelated male who listed himself at the address starting in June 2016; an unrelated female who listed the address in 2017 and thereafter left the United States in 2017; an unrelated female who listed the address in 2018 and for which no other information is known; and an individual who appears to be a male relative, who listed the address in 2018, left the country and re-entered the United States for tourism with his family in January 2020.

27. There is probable cause to believe YAKOV MOROZ uses the MOROZ RESIDENCE to operate the fraudulent scheme and evidence, instrumentalities, contraband and fruits of the fraudulent scheme will be found at the MOROZ RESIDENCE. For instance:

- a. Bank Records: In or about May 2020, bank statements for Great Movers were mailed to the MOROZ RESIDENCE.
- b. Internet Activity: In or about April 2020, the MOROZ IP ADDRESS accessed email addresses created under the Great Movers domain and the MOROZ EMAIL ACCOUNT received emails from email addresses created under the Great Movers domain. The MOROZ IP ADDRESS logged into an account that controlled the domain registration for both Great Movers and New City Movers several times, as recently as June 2020.
- c. Phone number: As described above in paragraph 16, the MOROZ PHONE number listed on bank records for Interstate Advisor Inc., Movers Consulting Inc., New City Movers and Saba Gabi Inc. is associated with the MOROZ RESIDENCE.
- d. Training and Experience: Based on my training, experience, discussions with other law enforcement officers and participation in other moving fraud investigations, I know that moving companies perpetuating a fraudulent scheme commonly operate from both a residence as well as an office location. This is because the moving business is an online enterprise in large part and can be operated from either locations.

H. Summary

28. Based on the information set forth above, I respectfully submit that there is probable cause to believe that YAKOV MOROZ and TAL OHANA through Great Movers and affiliated companies have engaged in a fraudulent scheme to obtain money through fraudulent pretenses by inducing customers to contract for moving services and then seeking to force those customers to pay monies that were not agreed-upon.

29. For instance, Great Movers has made misstatements on its FMCSA registration forms, attempted to obscure its physical location, sought to hide the names of its employees, made an abrupt change in its name to New City Movers under a different DOT number which was later revoked for New City Movers' refusal to respond to requests for a FMCSA audit, and been the subject of more than 30 customer complaints which describe a similar fraudulent scheme. Moreover, Great Movers knowingly engaged with customers in various states through interstate means, including email and telephone.

TECHNICAL TERMS

30. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer maybe directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have

static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

31. As described above and in Attachment B, this application seeks permission to search for records that might be found on the MOROZ RESIDENCE and MOROZ OFFICE, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

32. *Probable cause.* I submit that if a computer or storage medium is found on the MOROZ RESIDENCE and MOROZ OFFICE, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via

the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

- e. Based on actual inspection of other evidence related to this investigation, such as emails to customers, I am aware that computer equipment was used in the wire fraud scheme. There is reason to believe that there is a computer system currently located on the MOROZ RESIDENCE and MOROZ OFFICE.

33. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the MOROZ RESIDENCE and MOROZ OFFICE because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a

computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to

specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

34. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who

has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

35. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence

described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

36. Because other individuals may share the MOROZ RESIDENCE, it is possible that the MOROZ RESIDENCE will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that the things described in this warrant may reasonably be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

CONCLUSION

37. Based on the foregoing, I respectfully submit that this affidavit supports probable cause for the Court to issue warrants to arrest YAKOV MOROZ and TAL OHANA for violations of Title 18, United States Code, Sections 1343 and 1349, and search warrants authorizing the search the MOROZ RESIDENCE and MOROZ OFFICE, as specified in Attachment A, to seize the items and information specified in Attachment B to this affidavit and to the Search and Seizure Warrant.

WHEREFORE, your deponent respectfully requests that the defendants YAKOV MOROZ and TAL OHANA be dealt with according to law.

I further request that the Court order that all papers in support of this Application, including the Affidavit, the Arrest Warrants, and Search Warrants, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to the target of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation by allowing the targets to flee before they can be arrested and the search of the MOROZ RESIDENCE and MOROZ OFFICE can be

[REDACTED]

BRIAN SMITH
Special Agent
Federal Bureau of Investigation

Sworn to before me by telephone on this

[REDACTED]

[REDACTED] E ROBERT M. LEVY
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

Properties to be searched

A.I. – The MOROZ OFFICE

The MOROZ OFFICE is located at 1733 Sheepshead Bay Road between Shore Parkway and Voorhies Avenue in Brooklyn, New York, in a building with a gray and glass façade. The first floor tenant is a business displaying the sign “Liquor World.” The doorway is marked with the address number “1733.” Upon entry, there is a digital display listing the businesses inside. “Interstate Advisor” is located on the second floor within Suite 21. Interstate Advisor is the MOROZ OFFICE. Photographs of the outside of the building and the digital display are included below.



A.II. – The MOROZ RESIDENCE

The MOROZ RESIDENCE is located in Apartment 5B at 125 Oceana Drive East within the Oceana Condominium and Club complex. According to publicly available data, 125 Oceana Drive East is an eight-story complex which includes 108 units. It is accessible through a 24-hour attended gatehouse and security with video intercom system. The entrance to the Oceana Condominium and Club complex is pictured below.



ATTACHMENT B

Property to be seized

I. Items to Be Seized

The items to be seized from the MOROZ OFFICE and MOROZ RESIDENCE include the following evidence, fruits, and/or instrumentalities of violations of violations of Title 18, United States Code, Sections 1343 and 1349 (wire fraud and conspiracy) (the “SUBJECT OFFENSES”), involving Great Movers Inc., New City Movers, American Choice Van Lines Inc., C And D Moving Inc., Compass Relocation, Cross Country Moving and Storage Inc., Green Mover of America Inc., Movers Consulting Inc., Nationwide Transportation Inc., Roman Relocation Inc., Sabi Gabi Inc., Transatlantic Moving Inc., Interstate Advisor and Uber Movers or YAKOV MOROZ, and occurring on or after December 1, 2017, including:

1. Documents, records or other items containing information concerning the SUBJECT OFFENSES;
2. Emails and communications with customers;
3. Records and information relating to the contracts and services agreed to with customers;
4. Bank records and ledgers showing company income and spending;
5. Notes, directions, and memoranda pertaining to the operation of the business;
6. Records and information relating to a conspiracy to defraud customers;
7. Records and information relating to the identity or location of the participants in the SUBJECT OFFENSES; and
8. Any correspondence between the above listed companies and/or MOROZ and any other moving company.
9. Any computer devices and storage media that may contain any electronically stored information (“ESI”) falling within the foregoing categories, including, but not limited to, desktop and laptop computers, disk drives, modems, thumb drives, personal digital assistants, smart phones, digital cameras and scanners. In lieu of seizing any such computer devices or storage media, this warrant also authorizes the copying of such devices or media for later review; any items or records needed to access the data stored on such seized or copied computer devices or storage media, including but not

limited to any physical keys, encryption devices, or records of login credentials, passwords, private encryption keys or similar information; any items or records that may facilitate a forensic examination of such computer devices or storage media, including any hardware or software manuals or other information concerning the configuration of the seized or copied computer devices or storage media; and any evidence concerning the identities or locations of those persons with access to, control over, or ownership of such seized or copied computer devices or storage media.