AUSA AKe

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

IN THE MATTER OF THE SEARCH OF **BLACKBERRY SMARTPHONE MODEL** **SQN100-1, SN 356112051190539**	**Case No. TDC 14-0529**

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH

I, DAVID N. GADREN, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the United States Department of Energy Office of the Inspector General, and have been since November 2008. My responsibilities include investigating allegations of fraud against the government, corruption of DOE officials, embezzlement of government funds, money laundering, and illegal exportation of DOE technology, technical data, and other controlled commodities. I attended the Criminal Investigator Training Program and the Inspector General Investigator's Training Academy at the Federal Law Enforcement Center in Glynco, Georgia. In addition, I have also received additional specialized training relating to subjects most relevant to the DOE's concerns, including fraudulent practices committed against the federal government and financial crimes, crimes involving federal contracts, foreign counterintelligence practices, foreign corrupt

practices, the functions and practices of organized criminal enterprises, and the federal criminal statutes that pertain to embezzlement, conversion, and purloining of federal funds, and the methods by which criminals seek to launder money from criminal activity, including the use of offshore "shell" companies, the exchange of "kickbacks," and multiple bank accounts. I have become familiar with these practices as they have been implemented in both the private and public sectors in the former Soviet republics to include the Russian Federation and other countries. I have participated in several investigations of violations of United States laws relating to unlawful misuse, conversion, and/or embezzlement of United States funds, as well as the laundering of such funds to facilitate criminal activity and to avoid detection by law enforcement or other regulatory entities. Prior to my employment as a Special Agent with the DOE-OIG, I was employed as a paralegal specialist with the United States Attorney's Offices for both the Southern District of New York and the Northern District of California, from 2004 until 2008, regularly assisting in criminal investigations in those districts. I am currently assigned to the Washington Field Office ("WFO") of the Federal Bureau of Investigation ("FBI") as a Task Force Officer ("TFO").

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched is a BlackBerry Smartphone Model SQN100-1, SN 356112051190539, hereinafter the "Device." The Device is currently located at FBI's Washington Field Office but was recovered at 7200 Wisconsin Avenue, Bethesda, Maryland, and will be forensically examined in the District of Maryland.

5. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. The Device's owner, Vadim Mikerin ("MIKERIN"), has been charged by indictment with Conspiracy to Commit Extortion in violation of 18 U.S.C. § 1951. MIKERIN was arrested by criminal complaint on October 27, 2014, and a grand jury in this District returned an indictment against him on November 12, 2014. The basic facts supporting the charge of the indictment are that MIKERIN, acting as the U.S. representative of JSC Techsnabexport ("TENEX"), a Russian state-owned enterprise responsible for selling Russian nuclear materials, contracted with a U.S. public relations expert in 2009 to provide public relations and marketing consulting services to TENEX in the United States. After executing the contract on TENEX's behalf with the contractor, MIKERIN confronted the contractor and demanded that the contractor return 1/3 of the $150,000 contract amount to MIKERIN as a condition of payment and maintaining the contract. The contractor ("CS-1") approached the FBI and received authorization to participate in the scheme. MIKERIN used email correspondence with CS-1 to direct CS-1 to make the kickback payments to shell corporations, including Wiser Trading Limited ("WISER") and Leila Global Limited ("LEILA"), with bank accounts in Cyprus and Latvia, respectively. Over the course of three separate multi-month contracts, CS-1 made wire transfers to accounts at MIKERIN's direction as follows:

Date	To	Recipient	Financial Institution	Amount
September 21, 2009	Alpha Bank Ltd., Cyprus	Wiser	Mercantile	$25,000
September 29,2009	Alpha Bank, Ltd., Cyprus	Wiser	Mercantile	$25,000
October 5, 2009	Alpha Bank, Ltd., Cyprus	Wiser	Mercantile	$25,000
November 27, 2009	Alpha Bank Ltd., Cyprus	Wiser	Wachovia	$35,000
May 6, 2010	Alpha Bank Ltd., Cyprus	Wiser	Wachovia	$50,000
June 23, 2010	Alpha Bank Ltd., Cyprus	Wiser	Wachovia	$50,000
January 14, 2011	Eurobank EFG, Cyprus	Wiser	Wachovia	$50,000
February 28, 2011	Eurobank EFG, Cyprus	Wiser	Wachovia	$50,000
April 25, 2011	Eurobank EFG, Cyprus	Wiser	Wachovia	$50,000
July 14, 2011	ABLV Bank, Riga, Latvia	Leila	Wells Fargo	$50,000
September 2, 2011	ABLV Bank, Riga, Latvia	Leila	Wells Fargo	$50,000
October 25, 2011	ABLV Bank, Riga, Latvia	Leila	Wells Fargo	$25,000

These amounts ultimately represented up to one-half of the contract payments CS-1 received from TENEX.

7. In addition to the wire transfers made under the third contract, MIKERIN directed CS-1 to pay him a portion of the agreed kickbacks directly in cash. These payments included a $25,000 cash payment by CS-1 to MIKERIN on January 25, 2011; a $25,000 payment on October 28, 2011, and a $50,000 cash payment on January 23, 2012. CS-1 made the cash payments directly to MIKERIN, packaged in yellow envelopes per MIKERIN's instructions.

For the January 25, 2011 cash payment, MIKERIN directed CS-1 to divide up a $25,000 cash into five yellow envelopes containing $5,000 each. MIKERIN informed CS-1 that he would remit these envelopes to TENEX officials coming to the United States.

8. MIKERIN explained these instructions to CS-1 in a January 2, 2011 email, where MIKERIN disguised his identity as a "Friend." MIKERIN wrote, "We have informed you are ready to proceed with 50K . . . please use the same way as the 'window' is opened for you till Monday, January 17 . . . It was also coordinate (sic) internally and Final Transfer 2010 in your favour (50K) is on the way (following our best knowledge will arrive next Tuesday – Wednesday) and that is why we would like to request you to arrange 25K in 5 yellow envelopes (you should be aware) the next week to finalize all outstanding balances." The cash payments made from CS-1 to MIKERIN were as follows:

Date	Amount	Location
January 25, 2011	$25,000	Washington, DC
October 28, 2011	$25,000	Washington, DC
January 23, 2012	$50,000	Arlington, VA

9. In addition to the indicted extortion scheme described above, MIKERIN is also under investigation for conspiracy to commit fraud by wire and honest services fraud in violation of 18 U.S.C. §§ 1343, 1346, and 1349, as well as violations of the Foreign Corrupt Practices Act, in violation of 15 U.S.C. § 78dd-2, and money laundering, in violation of 18 U.S.C. §§ 1956 and 1957.

10. Evidence obtained during the investigation of the extortion scheme above has yielded probable cause to believe that MIKERIN and others carried out a scheme to enrich

MIKERIN and other officials at TENEX. As part of the scheme, MIKERIN, with the consent of higher level officials at TENEX and ROSATOM (both Russian state-owned entities), would offer no-bid contracts to U.S. businesses in exchange for kickbacks in the form of money payments made to some of the same offshore bank accounts to which MIKERIN was directing CS-1 to make payments between 2009 and 2011.

11. Records obtained from warranted searches of MIKERIN's offices and email accounts show that MIKERIN directed officers of Fulton, Maryland-based Transport Logistics International ("TLI") and another U.S. business to make such payments to offshore accounts held in the name of WISER, LEILA, and Ollins Development Ltd. ("OLLINS") to disguise the recipients of the funds. These payments typically took the form of wire payments made to the offshore bank accounts belonging to WISER, LEILA, and OLLINS, from which MIKERIN apparently then shared the proceeds with other coconspirators also associated with TENEX in Russia and elsewhere.

12. TLI, through its officers knowingly paid kickbacks to these accounts in exchange for noncompetitive contracts with TENEX for the period from October 30, 2002, to October 1, 2014. According to business records retrieved from TLI's office in Fulton, Maryland, pursuant to a search warrant executed on October 29, 2014, the FBI determined that TLI paid $2,064,452.36 via wires to various offshore entities and three payments totaling $12,550 recorded as made payable to "cash" in TLI's accounting records. These payments, along with email communications with MIKERIN regarding the kickback scheme and payments themselves, were wire communications sent in furtherance of a scheme to defraud in violation of 18 U.S.C. § 1343. The total amount of these kickbacks was no less than $2,064,452.36 paid alternatively to offshore shell companies WISER, LEILA and OLLINS. Various TENEX and

ROSATOM officials are believed to have ultimately received these kickbacks in exchange for assisting MIKERIN to provide TLI with noncompetitive contracts with TENEX.

13. DOE and private sector officials familiar with the performance components of the HEU Agreement advised there is no legitimate reason why a subcontractor to USEC like TLI would be wiring payments to entities ostensibly under the control of TENEX officials. TLI would neither require any goods nor services from TENEX or its related entities to perform the transportation services TLI contracted to perform for USEC.

14. A former TENAM employee reported that TENEX officials specifically directed TENAM to seek contracts across multiple sectors which would allow for padded pricing to include kickbacks.

15. Records obtained from warranted searches show that MIKERIN made extensive use of email communications to carry out the scheme. Several of MIKERIN's email accounts have been searched and show that he used coded language to refer to the kickback payments, which he alternately referred to as "cake" or "LF," the latter of which MIKERIN has explained in post-arrest interview stood for "Lucky Figure."

16. Emails between MIKERIN and TLI principals show that a figure of 5% for each quarter's invoices from 2006 to 2011 and 7% for quarterly invoices from 2012 to 2014 would be returned as a kickback to MIKERIN via a wire transfer from TLI to LEILA, WISER, and OLLINS. MIKERIN would also send TLI officials false invoices via email to support payments from TLI to the shell entities he directed payment be made to. Each one of these invoices corresponded to a kickback payment TLI sent to either WISER or LEILA. Each invoice appeared on Techsnabexport (TENEX) letterhead and was captioned: "Tenex fee for providing support services." MIKERIN signed each invoice "on behalf of Techsnabexport (TENEX)."

17. A review of TENAM's records obtained via a warrant surreptitiously executed on TENAM's offices in the District of Maryland on February 1, 2014, revealed that MIKERIN conducted the extortion/kickback scheme clandestinely and presumably without the knowledge of other U.S.-based TENAM employees. MIKERIN maintained sequestered files locked away in his personal office reflecting transactions between various U.S. based companies and shell companies, to include LEILA, WISER and OLLINS DEVELOPMENT LIMITED, located in Switzerland. Many of these files were contained on flash or "thumb" drives locked in a safe found in MIKERIN's office.

18. In addition to sending invoices, MIKERIN and his coconspirators would communicate the completion of kickback payments to him using email communication. Most of the emails containing communications regarding the kickbacks were sent via MIKERIN's personal accounts, rather than on his official TENEX/TENAM accounts, and were only obtained via search warrant of those individual accounts. These emails correspond to records of more than twenty separate wire transmissions to LEILA, WISER, and OLLINS.

19. Based on preliminary search results of MIKERIN's office computer, it appears to agents who viewed the defendant's Microsoft Outlook account that the Device is was synched with his office computer. MIKERIN's office computer's "Contacts" directory showed many suspected coconspirators, both in the United States and in the Russian Federation. Although it is likely that the emails contained on the Device are mirrored on the computer already obtained via search warrant, MIKERIN's Device is likely to contain 1) call records showing contacts between MIKERIN and these suspected coconspirators, 2) text messages between MIKERIN and coconspirators that are likely to contain more sensitive information than what was contained in MIKERIN's work email account, 3) other sensitive files and attachments similar to those found

on the thumb drives stored in MIKERIN's office safe, 4) Image files, either stored as attachments or recorded with the Device's digital camera, showing MIKERIN with other coconspirators and showing the date of the contact

20. The Device is currently in the lawful possession of the FBI. It came into the FBI's possession when MIKERIN was arrested pursuant to criminal complaint on October 29, 2014, and execution of a search warrant of TENAM's offices. It has been in the FBI's possession since that date. While MIKERIN was in a place authorized to be searched and the Device is likely within the scope of the authorized electronic storage receptacles authorized to be seized and searched pursuant to that warrant, out of an abundance of caution, I seek this additional warrant to be certain that an examination of the Device will comply with the Fourth Amendment and other applicable laws.

21. The Device is currently in storage at the FBI's Washington Field Office, but was seized in Bethesda, Maryland, and will be examined in the District of Maryland. The Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the FBI and DOE OIG.

TECHNICAL TERMS

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

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling

communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include

various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software,

giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

23. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

24. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

25. There is probable cause to believe that things that were once stored on the Device may still be stored there, 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 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."

26. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device 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).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic 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 device 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.

27. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent

with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

28. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

29. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

DAVID N. GADREN
Special Agent
Department of Energy OIG

Subscribed and sworn to before me
on January 22, 2015:

JILLYN K. SCHULZE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched is a BlackBerry Smartphone Model SQN100-1, SN 356112051190539, hereinafter the "Device." The Device is currently located at FBI's Washington Field Office but was recovered at 7200 Wisconsin Avenue, Bethesda, Maryland, and will be forensically examined in the District of Maryland.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of 18 U.S.C. §§ 1343, 1346, 1349 (Wire and Honest Services Fraud); 18 U.S.C. §§ 1956 and 1957 (Money Laundering), and 15 U.S.C. § 78dd-2 since 2002, including:

   a. Text messages, emails, documents and attachments containing directions to make or confirming completed wire transfers, discussing contract negotiations, or concerning the use of proceeds of the offenses;

   b. Pictures showing coconspirators and the dates and GPS data showing when and where the phone was used to take such pictures, if appropriate.

   c. Records of specific transactions and amounts;

   d. any information regarding MIKERIN's contacts, including names, addresses, phone numbers, or any other identifying information as well as records of contacts;

   e. any information recording MIKERIN's schedule or travel from the date the device was first used to the present;

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history; and

3. Records evidencing the use of the device to connect to the internet, to include records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.