

AO 91 (Rev. 11/11) Criminal Complaint

Sealed
Public and unofficial staff access
to this instrument are
prohibited by court order

UNITED STATES DISTRICT COURT

for the
Southern District of Texas

United States Courts
Southern District of Texas
FILED

September 05, 2019

David J. Bradley, Clerk of Court

United States of America)
v.)
Kenenty Hwan Kim (aka Myung Kim))

Case No. **4:19mj1691**

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of See offense description below in the county of Harris in the Southern District of Texas and elsewhere, the defendant(s) violated:

Code Section

Offense Description

From no later than June 2018 to present, within the Southern District of Texas and elsewhere, the above-captioned defendant did knowingly and willfully combine, conspire, and agree with others known and unknown to commit offenses against the United States in violation of 18 U.S.C. 1956(a)(1)(B)(i), all in violation of 18 U.S.C. 1956(h).

This criminal complaint is based on these facts:

See attached affidavit.

Continued on the attached sheet.



Complainant's signature

FBI Special Agent Dimitri Willis

Printed name and title

Sworn to before me telephonically:

Date: September 05, 2019



Judge's signature

City and state: Houston, Texas

U.S. Magistrate Judge Dena Palermo

Printed name and title

Affidavit

I, Dimitri L. Willis, a Special Agent with the Federal Bureau of Investigation (FBI), being first duly sworn, do hereby depose and state under oath as follows:

Summary

The FBI is investigating a business email compromise (BEC) scheme which targets businesses. Essentially, a business is tricked into sending money to what it believes is a bank account owned by a business partner, but in reality, is owned by a fraudster. Here, Kenenty Kim received money obtained via fraud from BEC victims. Once fraud money was available for withdrawal, he quickly withdrew the money before the transaction could be rescinded, and transferred the money to other accounts that they opened (sometimes, within a few days). After investigating the matter, the FBI seeks a warrant to arrest Kim.

Introduction and Agent Background

1. I am an FBI Special Agent assigned to the Houston Field Office, Bryan Resident Agency. I am an “investigative or law enforcement officer of the United States” within the meaning of 18 U.S.C. § 2510(7), as a Special Agent of the FBI. As such, I am empowered to conduct investigations of and to make arrests for offenses enumerated in 18 U.S.C. § 2516, including 18 U.S.C. §§ 1028A, 1029, 1030, 1343, 1344, 1349, 1956, and 1957, among others.
2. I have been employed as a Special Agent since January 2016. As a Special Agent of the FBI, I am charged with the duty of investigating violations of the laws of the United States, collecting evidence in cases in which the United States is or may be a party in interest, and performing other duties imposed by law. I investigate crimes involving wire and bank fraud, business email compromises, and financially motivated crimes. I have

worked a variety of matters, including, but not limited to, wire and mail fraud, money laundering, as well as matters that included a significant cyber component. I have training in the preparation, presentation, and service of criminal arrest and search warrants, and have been involved in the investigation of offenses against the United States.

3. The statements contained in this Affidavit are based in part on: information provided by other investigators and law enforcement personnel; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement officers and agents, information gathered from the service of legal process; the results of physical and/or electronic surveillance conducted by law enforcement agents; independent investigation and analysis by FBI agents/analysts and computer forensic professionals; and my observations, experience, training and background as a Special Agent (SA) with the FBI. References to my training and experience also include the training and experience of Special Agent James Hopp who is also working on this matter.
4. Since this affidavit is being submitted for the limited purpose of securing authorization for the requested search warrant, I have not included each and every fact known to me concerning this investigation. Rather, I have set forth only those facts necessary to establish probable cause. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

Probable Cause

5. Based on my training and experience and the facts in this affidavit, I submit that there is probable cause to believe that Kenenty¹ Hwan Kim (a.k.a. Myung Kim) and others known and unknown, are committing 18 U.S.C. § 1956(h) (conspiracy to commit money laundering) (the “Subject Offense”).

Business Email Compromises, generally

6. A business email compromise (BEC) is a scheme to defraud businesses. Fraudsters often use “spoofed” email addresses (email addresses with confusingly similar domains and/or hacked email accounts), to invent a fictitious transaction, or hijack a legitimate one in an effort to convince the victim to send funds to an account that is actually controlled by the fraudsters.

Solid Bridge Construction BEC

Victim Solid Bridge Construction is defrauded into sending \$210,312.00 to a fraudulent account opened in the name of Chance Contracting

7. Solid Bridge Construction LLC, is a general contracting company located in the City of Huntsville within the Southern District of Texas. It is involved in developing large scale commercial projects from the ground up, and subcontracts many of its services to other construction companies.
8. Chance Contracting LLC, is a business located in the Pinehurst, Texas. Chance Contracting is involved in the construction of road surfaces (grading and paving roads

¹ Whether inadvertently or on purpose, Kim appears to spell his name differently, spelling it as Kenenty, Kennenty, Kennety, and Kennedy, among other variations. Notably, he also differently spells the names of companies that he has opened (e.g. “invest” vs. “ivest”).

and parking lots), commonly referred to as “site work,” for large commercial construction projects.

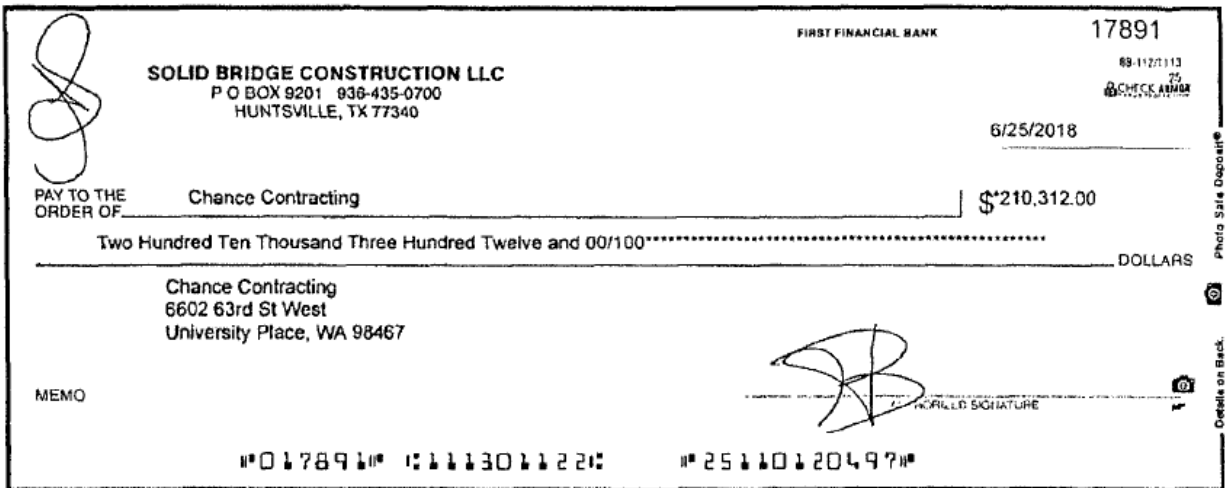
9. Solid Bridge reported that it received email(s) that appeared to come from the email account of Brett Chance, the owner of Chance Contracting. In reality, however, the emails were sent from a confusingly similar domain. These emails claimed that Chance Contracting was having “issues” receiving check payments, and asked Solid Bridge to instead mail a check to Chance Constructing at 6602 63rd St West, University Place, Washington 98467.
10. Solid Bridge complied, sending a check for \$210,312.00. According to Solid Bridge representatives, the company believed it was making a payment associated with a legitimate invoice from Chance Contracting. It later learned that Chance Contracting never received this money.

Solid Bridge’s check was deposited by Kim into a Columbia Bank account that Kim had opened – and had recently added a new D.B.A. in the name of Chance Contracting

11. This check was cashed by Kim at Columbia Bank account, last four digits -0332.
12. Bank records show that, in March 2018, Kim had opened this Columbia Bank account under the name “Kenenty H Kim DBA Reg Construction Solution.” On several of these account opening records, he listed his email address as KenKimWA@gmail.com.
13. On Columbia Bank’s account owner information sheet, Kim also listed his street address as “6602 63rd St. West, University Pl, WA” – the same address where Solid Bridge was asked to send its check.
14. Bank records show that on June 29, 2018, that Solid Bridge’s \$210,312.00 check was deposited into Kim’s Columbia Bank -0332 account.

It was Kim who personally transacted Solid Bridge’s \$210,312.00 check

15. According to a Columbia Bank representative’s affidavit, on June 29, 2018, it was Kim who deposited this check. He visited the Columbia Bank branch at 84th and Pacific located in Tacoma, Washington and deposited check #17891 in the amount of \$210,312.00. As instructed by the fraudulent email, Solid Bridge made the check payable to Chance Contracting with an address of 6602 63rd St West, University Place, Washington 98467.



Account Number	25110120497	OF6	0
Amount	\$210,312.00	Trans	0
Post Date	20180629	Routing Number	111301122
Sequence	29280127	Serial	17891

That same day, Kim added “Chance Contracting” as his personal D.B.A. on his Columbia Bank account -0332

16. Before the check was deposited, “Chance Contracting” was not listed as an accountholder – but this changed on June 29, 2018, when the check was deposited. Before depositing the check, Kim had added a D.B.A. (Doing Business As) “Chance Contracting” to his account profile at the bank. According to the bank representative’s

affidavit, Kim substantiated this by providing the bank a copy of a Business License Application from the State of Washington, Department of Revenue indicating he was the owner of Chance Contracting, 6602 63rd St. West, University Place, WA 98467.

The FBI corroborated this with Washington state records showing that Kim had, on the same day as his deposit, filed an application for a D.B.A. in the name of Chance Contracting

17. To corroborate the bank representative's affidavit, the FBI obtained certified copies of Kim's business licenses and applications from the Washington state Department of Revenue. One business that Kim registered was Chance Contracting, the same name as the company who was supposed to receive payment from Solid Bridge in this case.
18. Originally, Kim applied online for a Washington state business license for a business named Reg Construction Solution. He listed KenKimWA@gmail.com as a means of contact. Washington state assigned this license Unified Business ID #: 604196675.
19. Around June 29, 2018, the same date that Kim visited the Columbia Bank branch, Kim then modified this business license application to add Chance Contracting as a trade name to this business license. This is reflected on Business License Application Unified Business ID # 604196675. (In addition, Washington state records identified three other businesses that Kim had registered: Fivestar Construction, MHK Re Construction Solution, and Reg Construction Solution.)

On July 11, 2018, Kim transferred \$190,000 of the \$210,312 deposit to another account he opened at UniBank, account -9678 – and from there, withdrew another \$10,000

20. A few days after adding Chance Contracting to his Columbia Bank -0332 account and depositing the check of victim Solid Bridges, Kim withdrew over the counter \$4,500 on July 2, 2018, and \$10,000 on July 11, 2018, in addition to several debit card transactions.

21. Around July 11, 2018, Kim wired \$190,000 from his Columbia Bank account -0332 to UniBank account -9678.
22. According to UniBank records, Kim opened UniBank account -9678 around December 15, 2017 and listed the same mailing address as he used when he opened the Columbia Bank -0332 account: 6602 63rd St. West, University Place, WA – and the same address that was given to Solid Bridges.²

Kim then wired a total of \$100,000 from his UniBank account to “Siyabonga Dlamini” in South Africa; the remaining \$86,504 was frozen; this UniBank account was opened using kennetykim@hotmail.com

23. The day after the \$190,000.00 wire transfer was received by Kim’s UniBank -9678 account, Kim wired out \$60,000.00 and \$40,000.00 (plus fees) to Siyabonga Dlamini with an address in South Africa.

Electrolux BEC Fraud

Kim works with Unindicted Co-Conspirator A to defraud Electrolux

24. Around January 8, 2019, victim Electrolux Major Appliances North America (Electrolux) was tricked by a fraudulent email into wiring around \$333,208.85 to KeyBank account -1294. According to documents provided by Electrolux, Electrolux thought it was paying one of its vendors. Records from KeyBank show that this KeyBank account was opened around December 28, 2017 by Unindicted Co-Conspirator A.

² On July 16, 2018, Columbia Bank notified UniBank of the suspected fraudulent activity involving Kim. UniBank was able to freeze \$86,504 before Kim depleted his UniBank account. The funds were wired back to Columbia Bank where they remain frozen in a temporary account.

25. The next day, around Jan. 9, 2019, Unindicted Co-Conspirator A and someone who from a bank photo appears to be Kim, visited a KeyBank branch and from Back's KeyBank -1294 account, obtained a \$220,000 cashier's check made out to Myung Kim (a name that Kim has used in the past according to documents found in Kim's KenKimWA@gmail.com,). They also withdrew \$30,000 in cash.
26. Kim deposited the \$220,000 check, as well as \$10,000 in cash, into his Wells Fargo Bank -1884 account. (Kim had opened this account using his alias of Myung Kim.)
27. On Jan. 10, 2019, Unindicted Co-Conspirator A wired \$50,000 from his account to Siyabonga Dlamini, the same person in South Africa to whom Kim had wired proceeds of the Solid Bridges BEC fraud. Thus, it appears that Kim and Unindicted Co-Conspirator A have been conspiring with each other and with Dlamini.

Kim then took steps to transfer this money to yet another account, KeyBank -7661, an account that he opened in January 2019

28. Around Jan. 16, 2019, Kim registered KUGU PALPAL INVESTDEVELOP LLC (and other company names) with Washington state. He evidently applied as "Myung (Kennety) Kim" as this is how Washington's Secretary of State Office, Corporations & Charities Division responded to him in a document found in Kim's KenKimWA@gmail.com account.
29. According to KeyBank records, two days later, around Jan. 18, 2019, Kim opened KeyBank account -7661 in the name of KUGU PALPAL INVEST DEVELOP.
30. That same day, Kim made 3 withdrawals of \$170,000, \$38,000, and \$6,000 from his Wells Fargo -1884 account.
31. Around Jan. 22, 2019, Kim deposits \$170,000 cash into KeyBank -7661. (Again, this money is traceable from the \$333,208.85 Electrolux BEC to this account.)

Kim moved \$172,700 from his KeyBank -7661 account to his Bank of America -6638 account and then wired \$160,000 to Siyabonga Dlamini in South Africa

32. Around Jan. 23, 2019, Kim withdrew \$172,700 from his KeyBank -7661 account and deposited it into a new account at Bank of America -6638 account which he opened on the same day.
33. Around Jan. 30, 2019, Kim wires \$160,000 to Siyabonga Dlamini in South Africa from his Bank of America -6638 account which otherwise has little activity.

Background Regarding Computers, the Internet, and Email

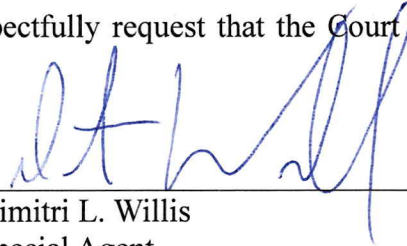
34. The term “computer” as used herein is defined in 18 U.S.C. § 1030(e)(1), and includes an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.
35. Based on my training and knowledge and the experience of investigators and other law enforcement personnel assisting in this investigation, I know the following:
- a. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. In order to access the Internet, an individual computer user must subscribe to an access provider, which operates a host computer system with direct access to the Internet. The World Wide Web (“www”) is a functionality of the Internet which allows users of the Internet to share information;
 - b. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any number of means, including modem, local area network, wireless and numerous other methods; and
 - c. Email is a popular form of transmitting messages and/or files in an electronic environment between computer users. When an individual computer user sends email, it is initiated at the user’s computer, transmitted to the subscriber’s mail server, and then transmitted to its final destination. A server is a computer that is attached to a dedicated network and serves many users. An email server may allow users to post and read messages

and to communicate via electronic means.

- d. **Domain name:** An identification label (such as www.example.com) that allows users to easily locate a website. Domain names resolve back to specific IP addresses; thus, for example, www.example.com would resolve back to one IP address. There can be many domain names that resolve back to the same IP address.
- e. **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 computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be 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.
- f. **Server:** A computer, or a series of computer systems, that operates or “hosts” websites and software applications. Unlike a personal computer, a server allows software applications or websites running on it to be accessed by multiple people simultaneously. The term “server” often refers to either the computer hardware itself or the software running on it. For the purposes of this affidavit, I use the term server to refer to a “web” server, which hosts web pages and applications that can be accessed through the Internet.
- g. **Spoofed E-mail:** an e-mail designed to appear to be coming from an entity or person that it is not truly coming from (*e.g.*, through unauthorized use of a domain name and/or creation of a user name selected to appear to be a person trusted by a target of the scheme).
- h. **Confusingly similar domains:** domains that are registered to, at first glance, be domains of other entities, but differ in small ways which are often and easily overlooked. For instance, if jimsproshop.com is a legitimate domain, jimsproshops.com could be a confusingly similar domain.

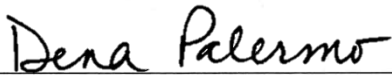
Conclusion

36. For these reasons, I submit there is probable cause to believe that Kenenty Kim has committed the Subject Offenses and respectfully request that the Court issue an arrest warrant.



Dimitri L. Willis
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me telephonically on September 5th, 2019.
I find probable cause and order the issuance of an arrest warrant.



United States Magistrate Judge Dena Palermo