

UNITED STATES DISTRICT COURT

for the

District of Maryland

United States of America
v.

Case No.

19-150-SAG

Ahmad KAZZELBACH

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 July 2016 through June 2017 in the county of Anne Arundel in the District of Maryland, the defendant(s) violated:

| <i>Code Section</i> | <i>Offense Description</i> |
|---|---|
| 18 U.S.C. § 1030(a)(2)(C); 18 U.S.C. § 1028A; and 18 U.S.C. § 2261A(2)(B) | Obtaining Information from a Protected Computer; Aggravated Identity Theft; and Cyberstalking |

FILED ENTERED
LOGGED RECEIVED

JAN 14 2019

AT BALTIMORE
CLERK, U.S. DISTRICT COURT
DISTRICT OF MARYLAND
BY *CRS* DEPUTY

This criminal complaint is based on these facts:

See attached Affidavit.

Continued on the attached sheet.

[Signature]

Complainant's signature

Michael Fowler, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date:

January 14, 2019

[Signature]

Judge's signature

City and state:

Baltimore, MD

Stephanie A. Gallagher U.S. Magistrate Judge

Printed name and title

✓ FILED LOGGED ENTERED RECEIVED
JAN 14 2019

19-150-SAG-40 19-153-SAG

AT BALTIMORE
CLERK U.S. DISTRICT COURT
DISTRICT OF MARYLAND
CRP

**AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT
AND APPLICATIONS FOR SEARCH WARRANTS**

BY I, Special Agent Michael Fowler, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. This affidavit is submitted in support of a criminal complaint and arrest warrant, as well as applications pursuant to Rule 41 of the Federal Rules of Criminal Procedure for warrants authorizing the search of the following locations (the "TARGET LOCATIONS"):

a. The premises known as 1040 Vena Lane, Pasadena, Maryland 21122 (the "TARGET PREMISES"), and

b. The person of Ahmad KAZZELBACH ("KAZZELBACH"), born in January 1993, and residing at the TARGET PREMISES, for:

i. Buccal or oral swabs in sufficient quantity for scientific testing as it relates to deoxyribonucleic acid ("DNA"), and

ii. Electronic evidence,

further described in Attachment A, for the things described in Attachment B.

2. I submit, pursuant to the facts set forth in this Affidavit, that there is probable cause to believe that KAZZELBACH has committed violations of 18 U.S.C. §§ 1030(a)(2)(C) (Obtaining Information from a Protected Computer), 1028A (Aggravated Identity Theft), and 2261A(2)(B) (Cyberstalking), and that evidence, fruits, and/or instrumentalities of these offenses will be found in the TARGET LOCATIONS.

3. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), and have been since March 2016. I am currently assigned to the Baltimore Division of the FBI, Joint Terrorism Task Force, where I investigate threats to national security. Prior to this assignment, I worked for FBI Baltimore's Cyber Crime Squad, where I investigated computer crimes including computer intrusions and identity theft. I am an "investigative or law enforcement officer" of the

United States within the meaning of Title 18, United States Code, Section 2510(7). As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

4. I have experience in such investigations through training in seminars, classes, and day-to-day work related to investigations of this type of case and other technical matters. Prior to employment as a Special Agent with the FBI, I was employed for five-and-a-half years as an Intelligence Analyst with the FBI, assigned to FBI Headquarters Cyber Division.

5. The facts set forth in this affidavit are based upon my personal knowledge and knowledge obtained during my participation in this investigation, including my review of documents related to this investigation, communication with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and experience. This affidavit does not contain all of the information known to me regarding this investigation. I have included in this affidavit facts that I believe are sufficient to support a probable cause finding for the issuance of the requested criminal complaint, arrest warrant, and search warrants, but I do not purport to include each and every matter of fact observed or known to me or other law enforcement agents involved in this investigation.

PROBABLE CAUSE

6. J.K. is a resident of Baltimore, Maryland, and works for Bankers Life, an insurance company that, at relevant times, was located at 898 Airport Park Road, Glen Burnie, Maryland. J.K. began working at Bankers Life in or about June 2015. AHMAD KAZZELBACH was J.K.'s training agent at Bankers Life. KAZZELBACH and J.K. subsequently became romantically involved and moved in together in or about December 2015. In or about May 2016, KAZZELBACH and J.K. broke up after J.K. became aware of KAZZELBACH's alleged

infidelity. Shortly thereafter, KAZZELBACH moved out of their shared apartment. Both KAZZZELBACH and J.K. continued to work at Bankers Life until in or about September 2016, when KAZZELBACH was asked to resign from the company.

7. Based on the investigation, as well as my knowledge, training, and experience, I believe that, shortly after KAZZELBACH moved out of the apartment he shared with J.K., KAZZELBACH began a year-long scheme to harass J.K. by compromising several of her personal online accounts, forging policy cancellation letters on behalf of her clients, and filing false reports with various police departments that ultimately resulted in J.K. being wrongfully arrested and incarcerated on multiple occasions before charges against her were dismissed by state authorities.

COMPROMISE OF J.K.'S ACCOUNTS

8. On July 27, 2016, less than two months after her relationship with KAZZELBACH ended, J.K. contacted the Anne Arundel County Police Department ("AACPD") to report suspicious activity within her Yahoo, Instagram, and Facebook accounts. J.K. reported that she attempted to log into her Yahoo e-mail account, [REDACTED]@yahoo.com, and discovered that the password had been changed without her knowledge. J.K. then attempted to log into her Instagram account and found that the user name had been changed to "Jvvwhore," and that the password had also been changed. J.K. then logged into her Facebook account and discovered that the text "You took my boyfriend" had been added under her profile photo. J.K. reported that she believed her accounts had been accessed by KAZZELBACH's new girlfriend.

9. Records associated with J.K.'s Instagram account revealed the following login information:

| Time Stamp | IP Address |
|------------------------|----------------|
| 7/27/2016 16:52:28 UTC | 107.77.202.198 |
| 7/27/2016 16:56:56 UTC | 107.77.202.198 |

10. J.K. subsequently identified other suspicious activity on accounts she held with Nelnet, Apple, BB&T, and TurboTax, including some activity that investigators later traced to the same IP address, 107.77.202.198. The suspicious activity included locked accounts, changes in profile information, changed user names, and changed passwords.

11. For example, records obtained from Nelnet, which serviced J.K.'s student loans, revealed that, on July 25, 2016, J.K.'s mailing address, phone number, and e-mail address were changed through her online account to the following:

898 Airport Road
Glen Burnie, MD 21060
(410) 760-6020
[REDACTED]@yahoo.com.

12. Pursuant to a search warrant issued by this Court, Yahoo provided account records that included a July 25, 2016, e-mail from Nelnet to [REDACTED]@yahoo.com, confirming a password change for Nelnet.com.

13. J.K.'s legitimate Yahoo e-mail account was [REDACTED]@yahoo.com, not [REDACTED]@yahoo.com. Based the investigation described below, I believe that KAZZELBACH created the [REDACTED]@yahoo.com account to facilitate the compromise of J.K.'s real accounts.

14. For example, Yahoo records relating to [REDACTED]@yahoo.com reflect the following account registration information:

| | |
|-----------------------------------|---|
| Registration IP Address: | 50.197.5.245 |
| Account Created: | 7/25/2016 20:32:57 GMT |
| Alternate Communication Channels: | 1 (410) 818-7105 (verified). ¹ |

¹ When provider records indicate that a phone number is "verified," that means the provider in some way authenticated that phone number as being associated with the individual accessing the account. For instance, most providers will send a text message code to the phone number. The

15. Records provided by AT&T indicated that, between November 2011 and May 2017, the subscriber to the phone number (410) 818-7105 was "Mustafa Kazzalbach," who is AHMAD KAZZELBACH's uncle.

16. Public records also revealed that IP address 50.197.5.245 was registered to Internet Service Provider ("ISP") Comcast Cable Communications Inc. ("Comcast"). Comcast's records indicate that this was a "static IP" address. A static IP address is a permanent IP address assigned by an ISP to a customer, whose IP address does not change over time unless it is affirmatively modified by the ISP. Comcast's static IP address history reflects as follows:

| IP Address | Grant Date (UTC) | Expiration Date (UTC) |
|--------------|--------------------|-----------------------|
| 50.197.5.245 | 4/10/2013 23:59:59 | 7/3/2018 00:00:00 |

Subscriber Name: Bankers Life and Casu
 Service Address: 898 Airport Park Rd, 210 -A, Glen Burnie, MD 21061.

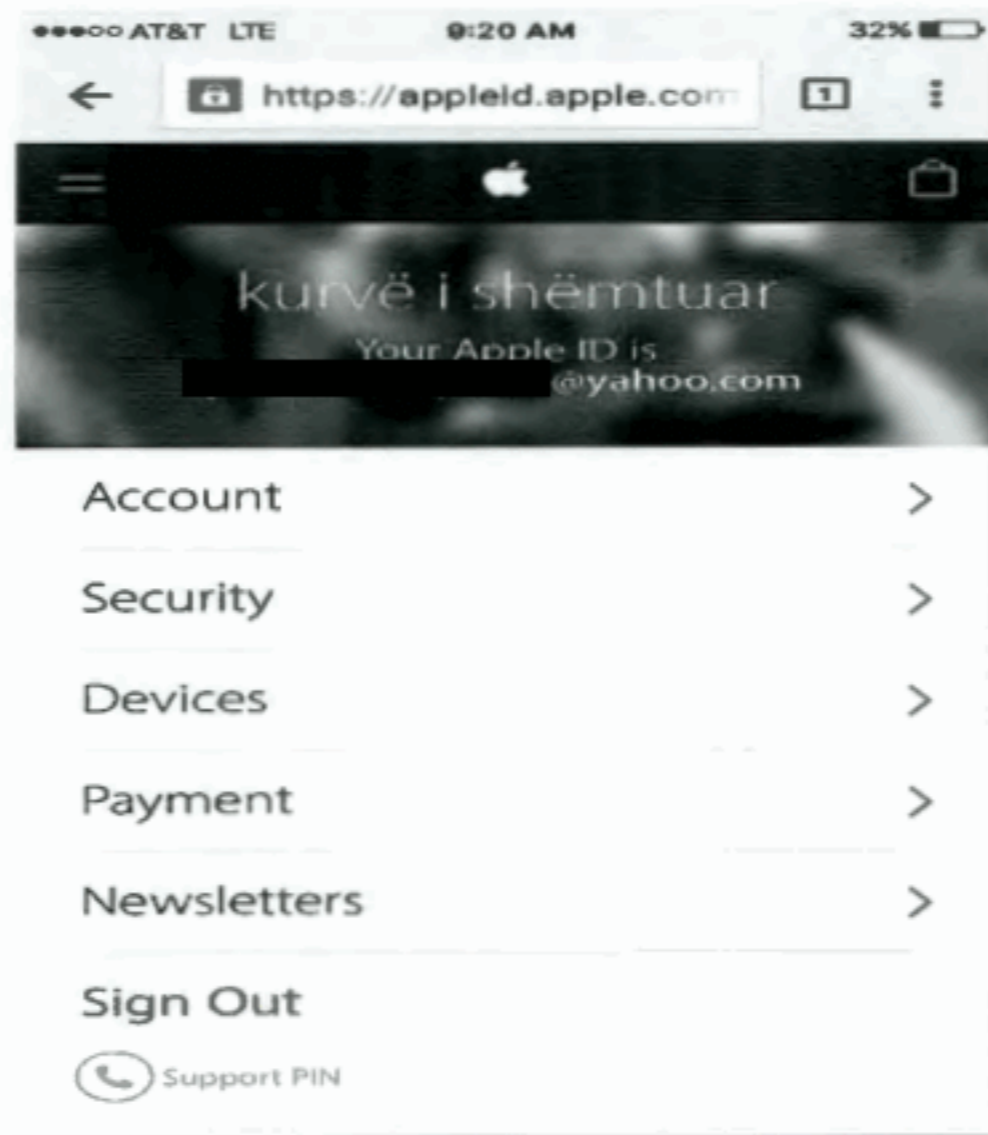
17. IP addresses 50.197.5.245 and 107.77.202.198 were also used in connection with suspicious activity that took place in J.K.'s Apple account in late July 2016. J.K.'s Apple account records reflect the following Apple ID and iForgot (a password-reset application) activity:

| Time Stamp | Account Name | App | Client IP | Credential ID |
|---------------------------|--------------------------|----------|--------------|--------------------------|
| 7/25/2016 20:30:30 GMT | ██████████@ yahoo.com | Apple ID | 50.197.5.245 | ██████████@ yahoo.com |
| 7/25/2016 20:30:30 GMT | ██████████@ yahoo.com | Apple ID | 50.197.5.245 | ██████████@ yahoo.com |
| 7/25/2016 20:30:30 GMT | ██████████@ yahoo.com | Apple ID | 50.197.5.245 | ██████████@ yahoo.com |
| 7/25/2016 20:33:59 GMT | ██████████@ yahoo.com | Apple ID | 50.197.5.245 | ██████████@ yahoo.com |
| 7/25/2016 20:34:14 GMT | ██████████@ yahoo.com | Apple ID | 50.197.5.245 | ██████████@ yahoo.com |

individual with access to that code will then enter the code when logged into the account. Once complete, the provider will have "verified" the phone number with that account.

| | | | | |
|---------------------------|--------------------------|---------|----------------|--------------------------|
| 7/27/2016 17:27:56 GMT | [REDACTED]@ yahoo.com | iForgot | 50.197.5.245 | [REDACTED]@ yahoo.com |
| 7/29/2016 13:17:25 GMT | [REDACTED]@ yahoo.com | iForgot | 107.77.202.198 | [REDACTED]@ yahoo.com |

18. On July 29, 2016, at 13:22:53 GMT, less than six minutes after the iForgot activity identified in the preceding paragraph, KAZZELBACH sent the following picture to J.K.'s iPhone:



This image is a screenshot of J.K.'s Apple account that could have been accessed only by someone with the ability to log into her account after its credentials had been changed.

19. Pursuant to a search warrant issued by this Court, Yahoo provided account records that included a July 29, 2016, e-mail from Apple to [REDACTED]@yahoo.com, confirming a password reset for J.K.'s Apple account.

20. Based on these records, your Affiant believes that: (1) on July 25, 2016, using IP address 50.197.5.245, KAZZELBACH changed J.K.'s Apple Account Name from [REDACTED]@yahoo.com to [REDACTED]@yahoo.com, and (2) on July 27 and July 29, 2016, using IP addresses 50.197.5.245 and 107.77.202.198, respectively, KAZZELBACH

ال

changed J.K.'s Apple Credential ID from [REDACTED]@yahoo.com to [REDACTED]@yahoo.com, and conducted an account password reset.²

21. According to records provided by BB&T, IP address 50.197.5.245 also was used to access J.K.'s BB&T account on September 1, 2016. On September 9, 2016, J.K.'s BB&T account was locked after multiple unsuccessful logins.

22. Finally, J.K. reported suspicious activity regarding her TurboTax account, the records of which reflect the following failed logins on October 1, 2016:

| Action Code | Create Date | Remote IP | Details (abbreviated) |
|--------------|----------------|--------------|--|
| Login Failed | 10/1/2016 6:04 | 107.77.204.7 | Location Pasadena, MD True_ip 71.244.237.141; proxy |
| Login Failed | 10/1/2016 6:04 | 107.77.204.7 | Location Pasadena, MD True_ip 71.244.237.141; proxy |

23. Based on training and experience, I know that "True_ip" data reflects the actual IP address of a user attempting to access the account through a proxy server at the date and time indicated in the log data. I also know from training and experience that cyber criminals typically utilize proxy servers to obfuscate their true location and identity.

24. Public records revealed that IP address 71.244.237.141 was registered to ISP MCI Communications Services, Inc. d/b/a Verizon ("Verizon"). Records provided by Verizon revealed that between June 29 and October 13, 2016, IP address 71.244.237.141 was assigned to the following subscriber:

Customer Name: KEZZALBACH HICHAM
Account Address: 1040 VENA LN, PASADENA, MD 21122.

² Based on information and belief, an "Account Name" is what appears on an account as the user's profile name. A "Credential ID" is the identifier used to validate the account password for logging into an account.

25. As the investigation described below revealed, law enforcement later discovered that, in September 2016, IP address 71.244.237.141 also was used to create a billing profile for KAZZELBACH's own iTunes account.

PURPORTED CLIENT CANCELLATION LETTERS

26. In or about August 2016, two cancellation letters were faxed to Bankers Life purportedly from two separate clients of J.K., hereafter referred to as VICTIM 1 and VICTIM 2. The cancellation letters were typed and contained what appeared to be typed, as opposed to handwritten, signatures. As a result, VICTIM 1's health insurance policy with Bankers Life was cancelled.

27. VICTIM 1 and VICTIM 2 were interviewed in or about April 2018. VICTIM 1 and VICTIM 2 were separately shown the cancellation letter purportedly authored by each of them and submitted to Bankers Life. Both VICTIM 1 and VICTIM 2 denied authoring, signing, or submitting the letter that purported to be from each of them. VICTIM 1 advised that, as a result of the policy cancellation, VICTIM 1 was required to pay the underlying policy premium, in addition to the regularly scheduled monthly payment. As a result, VICTIM 1's checking account was overdrafted.

28. In or about April 2017, the Bankers Life office in Glen Burnie, Maryland, received an envelope that was returned to sender due to insufficient postage. The envelope was addressed to Bankers Life's processing office, with a return address of the Bankers Life office in Glen Burnie. The envelope was opened and found to contain cancellation letters for four policies, some of which belonged to clients of J.K. None of the policies ultimately were cancelled.

29. The envelope returned to Bankers Life was submitted to the FBI Laboratory for forensic examination, including examination for nuclear deoxyribonucleic acid ("DNA"). That

examination yielded a mixture of DNA containing male DNA, and was deemed suitable for comparison purposes. Accordingly, the requested search warrant would permit law enforcement to obtain a sample of DNA from KAZZELBACH to compare that sample with the mixture recovered from the envelope containing the four policy cancellation letters.

CHARGES AGAINST KAZZELBACH

30. On August 22, 2016, KAZZELBACH entered his and J.K.'s previously shared apartment and attempted to remove belongings. J.K. was notified by the building's management company and returned to the residence; eventually, AACPD was summoned.³ J.K. subsequently identified numerous personal belongings as missing, and filed theft and harassment charges against KAZZELBACH. As a result, a criminal summons issued for KAZZELBACH on August 25, 2016. The charges eventually were placed on the *stet* docket on December 7, 2016. KAZZELBACH later admitted to law enforcement that he had attempted to remove items from J.K.'s apartment in August 2016, but claimed that he did not take any of her belongings.

31. On September 14, 2016, J.K. and a new boyfriend/roommate reported to AACPD that a number of items had been stolen from their apartment, which was the same one in which KAZZELBACH had previously resided. In response, burglary and theft charges were filed against KAZZELBACH and, on September 15, 2016, a warrant issued for KAZZELBACH's arrest.

³ Later that day, KAZZELBACH filed a Petition for Protection from Domestic Violence against J.K. in the District Court of Maryland for Anne Arundel County (case number D-07-FM-16-001773). In the Petition, KAZZELBACH alleged that J.K. had directed violent threats and actions against him. KAZZELBACH listed his home address as 1040 Vena Ln, Pasadena, MD 21122, and provided (410) 370-9022 as his home phone number. J.K. also filed a Petition for Protection from Domestic Violence that same day; the Petition was never granted. KAZZELBACH, however, was granted a Temporary Protective Order, and a Final Protective Order hearing was scheduled for August 29, 2016. On August 29, 2016, however, KAZZELBACH's Petition was dismissed by Judge Laura M. Robinson, who found that KAZZELBACH had not carried his burden of proof.

KAZZELBACH was arrested and made his initial appearance in the District Court of Maryland for Anne Arundel County that same day, and bonded out of custody.⁴ KAZZELBACH later admitted to law enforcement that he had removed items from J.K.'s apartment in September 2016, but claimed the items were his.

32. On September 30, 2016, J.K. received a text message from a Florida-based number, (305) 504-7458, stating, "Prepare yourself for what's coming [REDACTED] the last 3 months were just the beginning. I have bigger plans for you [REDACTED]. I love how easily manipulated you can be".

33. (305) 504-7458 is a Voice Over Internet Protocol ("VOIP") number registered to an entity named Neutral Tandem Florida, LLC. From training and experience, I know that VOIP numbers are utilized to make calls over an Internet connection as opposed to using a standard phone line, and are frequently used by individuals attempting to disguise their identities. Google Voice, for example, provides telephone and text communications services through VOIP.

FALSE CHARGES AGAINST J.K.

34. Based on the investigation, I believe that, beginning no later than December 2016, and continuing through at least May 2017, KAZZELBACH engaged in a course of conduct to harass J.K. by obtaining protective orders against J.K. and then filing multiple police reports falsely alleging that J.K. had violated those orders through email and text communication with KAZZELBACH, including what appeared to be communication through SMS and iMessage. KAZZELBACH's conduct ultimately resulted in the issuance of at least six individual warrants for J.K.'s arrest, as well as her incarceration at detention facilities in January and June 2017.

35. On December 10, 2016, KAZZELBACH filed a Petition for Protection from Domestic Violence against J.K. in Anne Arundel District Court (case number 0701-SP05954-

⁴ The charges eventually were placed on the *stet* docket on December 7, 2016.

2016). In the Petition, KAZZELBACH alleged that he had received violent threats from J.K. via text message and social media, and that J.K. had physically abused him as well.

36. The same day, December 10, 2016, KAZZELBACH was granted an Interim Protective Order against J.K., with a Temporary Protective Order hearing scheduled for December 13, 2016. KAZZELBACH was granted the Temporary Protective Order, and a Final Protective Order hearing was scheduled for December 29, 2016.

37. Before that hearing took place, however, on December 22, 2016, KAZZELBACH filed an application for statement of charges against J.K. in Anne Arundel District Court. KAZZELBACH alleged that J.K. had continued to harass and threaten him in violation of the Temporary Protective Order. The same day, an arrest warrant issued for J.K. on charges of harassment, destruction of property, and two counts of violating a protective order (case number D-07-CR-16-012195). KAZZELBACH listed his home address as 1040 Vena Ln, Pasadena, MD 21122, and provided (443) 875-9604 as his telephone number.

38. On December 23, 2016, AACPD responded to a call for service at KAZZELBACH's residence. KAZZELBACH advised the responding officer that J.K. had violated the Temporary Protective Order issued against her. KAZZELBACH showed the officer text messages allegedly sent by J.K., threatening his life and referencing their December 29, 2016, court date. On December 24, 2016, the officer submitted an application for statement of charges against J.K. in Anne Arundel District Court (case number D-07-CR-16-009234). J.K. was charged with violation of a protective order, arson threat, and harassment. The same day, a warrant issued for J.K.'s arrest.

39. On December 24, 2016, AACPD responded again to KAZZELBACH's residence in reference to a violation of a protective order. KAZZELBACH showed a responding officer a

text message allegedly sent by J.K. again threatening KAZZELBACH's life. Later that day, the officer submitted an application for statement of charges against J.K. in Anne Arundel District Court for violation of a protective order (case number D-07-CR-16-009237). As a result, another warrant issued for J.K.'s arrest.

40. On December 28, 2016, AACPD responded yet again to KAZZELBACH's residence in reference to a violation of a protective order. KAZZELBACH told a responding officer that he received a text message allegedly sent by J.K. again threatening KAZZELBACH's life and referencing their December 29, 2016, court date. Later that day, the officer submitted an application for statement of charges in Anne Arundel District Court charging J.K. with violation of a protective order (case number D-07-CR-16-012534). Yet another warrant issued for J.K.'s arrest.

41. The hearing on KAZZELBACH's Temporary Protective Order was held before Judge John P. McKenna, Jr. on December 29, 2016. Under oath, and representing herself *pro se*, J.K. categorically denied committing any of the conduct underlying KAZZELBACH's request for a protective order. Nonetheless, Judge McKenna granted KAZZELBACH's Petition and issued a Final Protective Order against J.K. that was effective through December 29, 2017.

42. On January 3, 2017, J.K. was arrested by the Baltimore County Police Department ("BCPD") pursuant to the December 22, 2016, warrant referenced above (case number D-07-CR-16-012195).

43. On January 4, 2017, while in custody, J.K. was served with two more arrest warrants. The first was based on the above-referenced protective order violation, arson threat, and harassment charges filed on December 24, 2016 (case number D-07-CR-16-009234). The second was based on the above-referenced protective order violation charge also filed on December 24,

2016 (case number D-07-CR-16-009237). On January 4, 2017, J.K. made her initial appearance in the District Court of Maryland for Baltimore County on the December 22 warrant and both December 24, 2016, warrants, and was held without bond pending a commitment hearing.

44. Also on January 4, 2017, AACPD responded again to KAZZELBACH's residence in reference to a violation of a protective order. KAZZELBACH advised the responding officer that J.K. had messaged him twice that day and that he had an active Protective Order against her. KAZZELBACH showed the officer messages allegedly sent by J.K. via text and e-mail, some of which purported to be threats against KAZZELBACH's life. Later that day, the responding officer submitted an application for statement of charges against J.K. in Anne Arundel District Court (case number D-07-CR-17-000673). As a result, J.K. was charged with violation of a protective order, harassment, and electronic mail harassment. On January 5, 2017, yet another warrant issued for J.K.'s arrest.

45. However, on January 4, 2017, at the time that KAZZELBACH alleged he received threatening text and e-mail messages from her, J.K. was in custody and did not have access to her computer or iPhone. Toll records associated with KAZZELBACH's cell phone, ending in 9604, also reflect no text communication between J.K. and KAZZELBACH that entire day.

46. On January 5, 2017, J.K. was released from commitment by Baltimore County and transferred to the custody of Anne Arundel County based on two of the warrants: (1) alleging violation of a protective order, issued on December 28, 2016 (case number D-07-CR-16-012534); and (2) alleging violation of a protective order, harassment, and electronic mail harassment, issued on January 5, 2017 (case number D-07-CR-17-000673). The same day, J.K. made her initial appearance in Anne Arundel District Court on the December 28, 2016, and January 5, 2017,

charges, and was held without bond pending a commitment hearing. On January 6, 2017, J.K. was released from commitment.

47. On January 7, 2017, AACPD responded again to KAZZELBACH's residence in reference to a protective order violation. KAZZELBACH showed the responding officer a copy of the Final Protective Order against J.K., and then showed the officer four messages that KAZZELBACH allegedly received from J.K. again threatening his life. Later that day, the officer submitted an application for statement of charges in Anne Arundel District Court charging J.K. with violating a protective order, harassment, witness retaliation, and electronic mail harassment (case number D-07-CR-17-000704). An arrest warrant for J.K. issued the same day, but was ultimately recalled; a criminal summons later issued on January 11, 2017.

48. On January 10, 2017, AACPD responded again to KAZZELBACH's residence in reference to a violation of a protective order. KAZZELBACH stated that he received a text message allegedly sent by J.K. that day asking KAZZELBACH to get back together with her. Later that day, the responding officer submitted an application for statement of charges in the Anne Arundel District Court charging J.K. with violating a protective order (case number D-07-CR-17-000064). On January 11, 2017, another criminal summons issued for J.K.

49. On January 11, 2017, AACPD responded again to KAZZELBACH's residence in reference to a violation of a protective order. KAZZELBACH stated that he received a text message allegedly sent that day by J.K. encouraging KAZZELBACH to take his own life. Later that day, the responding officer submitted an application for statement of charges in Anne Arundel District Court charging J.K. with violation of a protective order (case number D-07-CR-17-000074). The same day, another criminal summons issued for J.K.

50. On February 24, 2017, AACPD responded again to KAZZELBACH's residence in reference to a protective order violation. KAZZELBACH stated that, on February 22, 2017, he received a text message allegedly from J.K. again threatening his life. Later that day, the responding officer submitted an application for statement of charges in Anne Arundel District Court charging J.K. with violation of a protective order (case number D-07-CR-17-003503). The same day, an arrest warrant issued for J.K. On March 1, 2017, the arrest warrant was recalled, and on March 3, 2017, yet another criminal summons issued.

51. In or about March 2017, a prosecutor from the State's Attorney's Office for Anne Arundel County asked for permission to download KAZZELBACH's iPhone in connection with the investigation of his complaints. KAZZELBACH refused to consent to a full download of his iPhone, but stated that he would permit a restricted download. The prosecutor advised KAZZELBACH that, if he did not permit a full search of his phone, the charges against J.K. would be dismissed.

52. On May 12, 2017, the prosecutor was notified that KAZZELBACH would not allow for a full search of his phone.

53. On May 14, 2017, KAZZELBACH went to AACPD's headquarters, where he met with an officer. KAZZELBACH advised the officer that he had a valid Protective Order against J.K. and that, on May 12, 2017, he received a message that purported to be sent from J.K.'s work e-mail address: [REDACTED]@bankerslife.com. Later that day, the officer filed an application for statement of charges in Anne Arundel District Court charging J.K. with violation of a protective order (case number D-07-CR-17-002021). The same day, another warrant issued for J.K.'s arrest.

54. On May 15, 2017, cases D-07-CR-16-012195, D-07-CR-16-009234, D-07-CR-16-009237, D-07-CR-16-012534, D-07-CR-17-000673, D-07-CR-17-000064, D-07-CR-17-000074,

and D-07-CR-17-003503—each relating to alleged violations of protective orders and other related charges against J.K. in Anne Arundel County—were dismissed *nolle prosequi*. The same day, KAZZELBACH walked into the BCPD and reported that J.K. had violated the Anne Arundel County Protective Order, alleging again that J.K. had sent him a threatening message from her work e-mail account.

55. On May 17, 2017, KAZZELBACH again walked into the BCPD and reported a Protective Order violation, alleging that J.K. sent him a message on May 16, 2017, using her work e-mail account.

56. On May 18, 2017, cases D-07-CR-17-000704 and D-07-CR-17-002021, the two remaining Anne Arundel County cases against J.K., were dismissed *nolle prosequi*.

57. On May 24, 2017, a BCPD detective met with KAZZELBACH. KAZZELBACH advised the detective that J.K. had continued to violate the Protective Order. In support, KAZZELBACH described messages that he allegedly received from J.K.'s work e-mail account on April 22, and May 23, 2017.

58. On June 14, 2017, KAZZELBACH filed a report with the BCPD alleging witness intimidation based on the messages that J.K. allegedly sent on April 22, 2017. On June 16, 2017, a BCPD detective filed a statement of charges alleging violation of a protective order and witness intimidation. Pursuant to these charges, J.K. was arrested by BCPD on June 22, 2017, and was transferred to the Baltimore County Detention Center. The following day, J.K. appeared before a judge and was granted release with home detention and electronic monitoring.

BCPD INVESTIGATION

59. BCPD subsequently conducted its own investigation. During the course of the investigation, BCPD detectives reviewed toll records associated with KAZZELBACH's phone,

and found no successful or attempted text communication between KAZZELBACH and J.K. on the occasions that KAZZELBACH alleged to police he had received text messages from her.

60. A review of J.K.'s work e-mail account also indicated that there were no successful or attempted e-mail communications between J.K. and KAZZELBACH on the dates that KAZZELBACH reported receiving messages from that account.

61. During its investigation, BCPD communicated with KAZZELBACH via e-mail address ahmad.kazzelbach@gmail.com. Subscriber records obtained from Google, the provider of the Gmail service, indicate that ahmad.kazzelbach@gmail.com was registered to "Ahmad Kazzelbach," and that the account's recovery email address was "dr.kazzelbach@gmail.com."⁵

62. Subscriber records obtained from Apple indicate that ahmad.kazzelbach@gmail.com is the primary email address associated with an iCloud account belonging to "Person ID" 1095296304, an account that was first registered on January 22, 2011. Apple records also indicate that Person ID 1095296304 is linked to an iTunes account with the following identifying information:

| First Name | Last Name | Address | Phone Number | Billing Profile Create | Billing Profile Create IP Address | Person ID |
|------------|-----------|---------------------------------------|--------------------|----------------------------|-----------------------------------|------------|
| Janna | Toyir | 1040 Vena Ln Pasadena, MD 21122 | (410) 370- 9022 | 2016-09-26 08:14:06 PST | 71.244.237.141 | 1095296304 |

63. IP address 71.244.237.141 is the same IP address from which unsuccessful attempts were made to log into J.K.'s TurboTax account on October 1, 2016; (410) 370-9022 and 1040

⁵ The purpose of a recovery email address is to permit a user to regain access to a primary account if, for some reason, the user loses access. In such instances, a communications provider typically will e-mail a password-reset link to the recovery email address.

Vena Ln Pasadena, MD 21122 were KAZZELBACH's phone number and address in September 2016.

64. On June 28, 2017, KAZZELBACH appeared at BCPD and signed a form authorizing BCPD to search his iPhone. BCPD imaged the iPhone, but found almost no data on it. The phone did, however, contain messages that KAZZELBACH allegedly received from J.K.'s work and personal e-mail accounts, as well as a message that KAZZELBACH purportedly sent to J.K.'s work e-mail address on June 28, 2017, asking J.K. to not contact him again.

65. KAZZELBACH's phone also contained as a contact the phone number (410) 818-7105, which had been verified by the user who registered [REDACTED]@yahoo.com. In KAZZELBACH's phone, the number (410) 818-7105 was associated with the contact name "Mott" and the email address "mkazzelbach@gmail.com." Based on the investigation, I believe that "Mott" is Mahmoud Kazzelbach, AHMAD KAZZELBACH's brother.

66. J.K. also appeared at BCPD on June 28, 2017. J.K. was Mirandized, waived her rights, and agreed to be interviewed. During her interview, J.K. denied making any of the changes to her online accounts referenced above, and denied ever communicating any threats to KAZZELBACH.

67. On June 29, 2017, J.K. signed a form authorizing BCPD to search her iPhone. A review of J.K.'s phone did not reveal any successful or attempted text or e-mail communication with KAZZELBACH on the occasions that KAZZELBACH reported to law enforcement having received messages from J.K. J.K.'s phone did, however, contain data reflecting ordinary, unrelated usage.

68. On August 1, 2017, KAZZELBACH was Mirandized, waived his rights, and was interviewed by BCPD and the FBI.

69. KAZZELBACH was asked why the device that he consented to be searched appeared to have almost no data on it. KAZZELBACH stated that it was his habit to routinely delete data from his phone. KAZZELBACH also told law enforcement that, between August 2016 and August 2017, he had used three different iPhones: specifically, until in or about September 2016, an iPhone with telephone number (410) 370-9022; until in or about February 2017, an iPhone with telephone number ending in -9604 (later identified as (443) 875-9604); and since in or about February 2017, an iPhone with telephone number (443) 775-1334.

70. KAZZELBACH stated that he changed phone numbers in September 2016 in response to the alleged harassment from J.K. As to his phone-number change in February 2017, KAZZELBACH provided two different justifications at separate points during the interview. First, KAZZELBACH stated that he changed his number in February 2017 due to J.K.'s continued harassment. Later, however, KAZZELBACH stated that he changed phone numbers in February 2017 because he damaged his phone when he dropped it into the water when he was boating. KAZZELBACH stated that he did not know how J.K. would have learned about his new phone numbers after September 2016.

71. KAZZELBACH also was asked about his understanding of why Anne Arundel County had dropped its charges against J.K. KAZZELBACH stated that, although the local prosecutor had asked to review his phone, he refused because his lawyer had stated that he did not trust the prosecutor. KAZZELBACH added that he was willing to permit a "restricted" download of his device, but that the prosecutor would not agree to this limitation.

72. KAZZELBACH also stated that he knew what "spoofing" was, and admitted that, on at least one occasion, he might have visited the spoofing website "emkei.cz" after a friend told

him that the site could be used to spoof e-mail addresses.⁶ I know from training and experience, and this investigation, that emkei.cz is a website that, free of charge, allows a user to send an email, including with attachments, to any recipient, in which the email appears as though it originates from any email address and name entered by the user.

THE TARGET LOCATIONS

73. As further described below, physical surveillance and information from the Maryland Department of Transportation, Motor Vehicle Administration (“MVA”) both indicate that KAZZELBACH has been associated with the TARGET PREMISES from at least August 22, 2016, through January 9, 2019:

a. On August 22, 2016, KAZZELBACH filed a Petition for Protection from Domestic Violence against J.K. in Anne Arundel District Court (case number D-07-FM-16-001773). In the petition, KAZZELBACH listed his home address as 1040 Vena Lane, Pasadena, MD 21122, the TARGET PREMISES.

b. On October 12, 2018, during physical surveillance of the TARGET PREMISES, agents observed a 2016 Toyota Rav-4, bearing Maryland license plate 3CK9225 and registered to KAZZELBACH, located on the street in front of the residence. The same day, agents also observed a male matching the description and photograph of KAZZELBACH from MVA records exiting the TARGET PREMISES and departing in the aforementioned 2016 Toyota Rav4.

c. As of January 8, 2019, MVA records listed the TARGET PREMISES as KAZZELBACH’s address. The following day, on January 9, 2019, during physical surveillance

⁶ “Spoofing” refers to the technique of using computer software to send an email that appears to be sent from another account, or to send a text message that appears to be sent from another phone number.

of the TARGET PREMISES, an agent observed a 2016 Toyota Rav-4, bearing Maryland license plate 3CK9225 and registered to KAZZELBACH, located on the street in front of the residence.

74. On October 12, 2018, agents observed KAZZELBACH walking from the TARGET PREMISES to his vehicle carrying a cell phone.

75. Based on my training and experience, I know that individuals who engage in computer hacking, aggravated identity theft, and cyberstalking often store evidence, fruits, and/or instrumentalities of their crimes at their residences. This evidence can be in paper or electronic form. Furthermore, individuals who use electronic devices and electronic modes of communication (including, but not limited to, e-mail) in furtherance of their illegal activities often keep these devices in private places, including at their residences and on their person. As further described below, computers and other electronic storage media often contain files or remnants of files for months or even years. For all of these reasons, I respectfully submit that evidence, fruits, and/or instrumentalities of the target offenses will be located at the TARGET LOCATIONS.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

76. As described above and in Attachment B, this application seeks permission to search for items that might be found at the TARGET LOCATIONS, in whatever form they are found. One form in which they 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 media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

77. *Probable cause.* I submit that, if a computer or storage medium is found at the TARGET LOCATIONS, 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 true 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, a computer’s internal hard drive—contains electronic evidence of how the 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 systems configurations, artifacts from operation 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.”

78. *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 at the TARGET LOCATIONS 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 logs: 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 the 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, too. Lastly, 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 the 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.

f. I know that when an individual uses a computer to obtain unauthorized access to a victim computer over the internet, the individual's computer will generally serve as both an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of internet discussions about the crime; and other records that indicate the nature of the offense.

79. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premise 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 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 at the

TARGET LOCATIONS. 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.

80. *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.


81. KAZZELBACH, his spouse, and his parents are known to utilize the TARGET PREMISES as a residence. It is possible that the TARGET PREMISES will contain storage media that are not predominantly used, or perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for here would permit the seizure and review of those items as well.

CONCLUSION

82. Based on the facts set forth above, I submit that there is probable cause to believe that KAZZELBACH has committed violations of 18 U.S.C. §§ 1030(a)(2)(C) (Obtaining Information from a Protected Computer), 1028A (Aggravated Identity Theft), and 2261A(2)(B) (Cyberstalking), and that evidence, fruits, and/or instrumentalities of these offenses will be found at the TARGET LOCATIONS, including, but not limited to, computers, computer-related equipment, and internet-enabled devices that will be searched for the items in Attachment B.

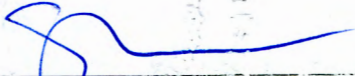
Therefore, I respectfully request issuance of the above-described criminal complaint, arrest warrant, and warrants to search the TARGET LOCATIONS, including the person of Ahmad KAZZELBACH, for the items listed in Attachment B.

Respectfully submitted,



Michael Fowler, Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on January 14, 2019.



Stephanie A. Gallagher
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A-1

Property to Be Searched

The property to be searched is **1040 Vena Lane, Pasadena, Maryland 21122**, further described as a duplex, located on a cul-de-sac, with green vinyl and brick siding, with the house number “Ten Forty” present in italic font near the front entrance (the “TARGET PREMISES”).



ATTACHMENT A-2

Person to Be Searched

Ahmad KAZZELBACH, DOB: 01/03/1993, SSN: 863-04-0487, male, approximately 73 or 74 inches tall, weighing approximately 170 pounds, with brown eyes and black hair.



ATTACHMENT B-1

Property to Be Seized

1. All records and information relating to violations of 18 U.S.C. §§ 1030(a)(2)(C) (Obtaining Information from a Protected Computer), 1028A (Aggravated Identity Theft), and 2261A(2)(B) (Cyberstalking), involving KAZZELBACH and occurring after June 2015, including records or information relating to the following:

- a. J.K. or Bankers Life;
- b. E-mail accounts associated with J.K. and KAZZELBACH, including, but not limited to, jordan_koopman@yahoo.com and jordan.koopman@yahoo.com;
- c. Access of J.K. or Bankers Life accounts, including electronic accounts;
- d. Any possession, transfer, or use of account credentials, including, but not limited to, those belonging to J.K.;
- e. Clients and/or policyholders of J.K. or Bankers Life;
- f. Possession of hacking tools, techniques, procedures, guides;
- g. Possession of spoofing tools, techniques, procedures, guides;
- h. Communication with other individuals conspiring to commit the crime(s) under investigation;
- i. Records and information relating to communications with Internet Protocol addresses 107.77.202.198, 50.197.5.245, 107.77.204.7, 71.244.237.141; and
- j. Any other items, which can be readily identifiable as connected to the aforementioned crimes or which are subject to seizure pursuant to the laws of the United States of America.

2. All images, messages, and communications regarding methods to avoid detection by law enforcement.

3. Any and all documents, records, or correspondence pertaining to KAZZELBACH's occupancy, ownership, or other connection to the TARGET PREMISES.

4. Computers(s), computer hardware, software, related documentation, passwords, data security devices (as described below), videotapes, and/or video recording devices, and data that may constitute instrumentalities of, or contain evidence related to the specified criminal offenses. The following definitions apply to the terms as set out in this affidavit and attachment:

- a. *Computer hardware*: Computer hardware consists of all equipment, which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic

magnetic or similar computer impulses or data. Hardware includes any data-processing devices (including but not limited to cellular telephones, central processing units, laptops, tablets, eReaders, notes, iPads, and iPods; and internal and peripheral storage devices such as external hard drives, thumb drives, SD cards, flash drives, USB storage devices, CDs and DVDs, and other memory storage devices); peripheral input/output devices (including but not limited to keyboards, printer, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).

b. *Computer software*: Digital information, which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

c. *Documentation*: Computer-related documentation consists of written, recorded, printed, or electronically stored material, which explains or illustrates how to configure or use computer hardware, software, or other related items.

d. *Passwords and Data Security Devices*: Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation or data. Data security devices may consist of hardware, software or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

As used above, the terms “records, documents, messages, correspondence, data, and materials” includes records, documents, messages, correspondence, data, and materials, created, modified, or stored in any form, including electronic or digital form, and by whatever means they may have been created and/or stored. This includes any handmade, photographic, mechanical, electrical, electronic, and/or magnetic forms. It also includes items in the form of computer hardware, software, documentation, passwords, and/or data security devices.

5. For any computer, computer hard drive, or other physical object upon which computer data can be recorded (hereinafter, “COMPUTER”) that is called for by this warrant, or that might contain things otherwise called for by this warrant:

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

- c. evidence of the lack of such malicious software;
- d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- e. evidence of counter forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- f. evidence of the times the COMPUTER was used;
- g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- i. contextual information necessary to understand the evidence described in this attachment.

6. Routers, modems, and network equipment used to connect computers to the internet.

7. With respect to the search of any of the items described above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment (including CDs, DVDs, thumb drives, flash drives, hard disk drives, or removable digital storage media, software, or memory in any form), the search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein, while permitting government examination of all the data necessary to determine whether that data falls within the items to be seized):

- a. surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);
- b. “opening” or curiously reading the first few “pages” of such files in order to determine their precise contents;
- c. “scanning” storage areas to discover and possibly recover recently deleted files;
- d. “scanning” storage areas for deliberately hidden files; or
- e. performing key word searches or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

If, after performing these procedures, the directories, files, or storage areas do not reveal evidence of obtaining information from a protected computer, intentional damage to a protected computer, cyberstalking, aggravated identity theft, or other criminal activity, the further search of that particular directory, file or storage area, shall cease.

ATTACHMENT B-2.a

Property to Be Seized

A sample of the deoxyribonucleic acid ("DNA") of the person identified in Attachment A-2 (KAZZELBACH), to be collected from him via a buccal or oral swab in accordance with established procedures and to be analyzed forensically in accordance with the applicable valid established procedures.

ATTACHMENT B-2.b

Property to Be Seized

1. All records and information relating to violations of 18 U.S.C. §§ 1030(a)(2)(C) (Obtaining Information from a Protected Computer), 1028A (Aggravated Identity Theft), and 2261A(2)(B) (Cyberstalking), involving KAZZELBACH and occurring after June 2015, including records or information relating to the following:

- a. J.K. or Bankers Life;
- b. E-mail accounts associated with J.K. and KAZZELBACH, including, but not limited to, jordan_koopman@yahoo.com and jordan.koopman@yahoo.com;
- c. Access of J.K. or Bankers Life accounts, including electronic accounts;
- d. Any possession, transfer, or use of account credentials, including, but not limited to, those belonging to J.K.;
- e. Clients and/or policyholders of J.K. or Bankers Life;
- f. Possession of hacking tools, techniques, procedures, guides;
- g. Possession of spoofing tools, techniques, procedures, guides;
- h. Communication with other individuals conspiring to commit the crime(s) under investigation;
- i. Records and information relating to communications with Internet Protocol addresses 107.77.202.198, 50.197.5.245, 107.77.204.7, 71.244.237.141; and
- j. Any other items, which can be readily identifiable as connected to the aforementioned crimes or which are subject to seizure pursuant to the laws of the United States of America.

2. All images, messages, and communications regarding methods to avoid detection by law enforcement.

3. Computers(s), computer hardware, software, related documentation, passwords, data security devices (as described below), videotapes, and/or video recording devices, and data that may constitute instrumentalities of, or contain evidence related to the specified criminal offenses. The following definitions apply to the terms as set out in this affidavit and attachment:

- a. *Computer hardware*: Computer hardware consists of all equipment, which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic magnetic or similar computer impulses or data. Hardware includes any data-processing devices (including but not limited to cellular telephones, central processing units, laptops, tablets, eReaders, notes, iPads, and iPods; and internal and peripheral storage devices such as external hard

drives, thumb drives, SD cards, flash drives, USB storage devices, CDs and DVDs, and other memory storage devices); peripheral input/output devices (including but not limited to keyboards, printer, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).

b. *Computer software*: Digital information, which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

c. *Documentation*: Computer-related documentation consists of written, recorded, printed, or electronically stored material, which explains or illustrates how to configure or use computer hardware, software, or other related items.

d. *Passwords and Data Security Devices*: Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation or data. Data security devices may consist of hardware, software or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

As used above, the terms “records, documents, messages, correspondence, data, and materials” includes records, documents, messages, correspondence, data, and materials, created, modified, or stored in any form, including electronic or digital form, and by whatever means they may have been created and/or stored. This includes any handmade, photographic, mechanical, electrical, electronic, and/or magnetic forms. It also includes items in the form of computer hardware, software, documentation, passwords, and/or data security devices.

4. For any computer, computer hard drive, or other physical object upon which computer data can be recorded (hereinafter, “COMPUTER”) that is called for by this warrant, or that might contain things otherwise called for by this warrant:

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of counter forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. evidence of the times the COMPUTER was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i. contextual information necessary to understand the evidence described in this attachment.

5. Routers, modems, and network equipment used to connect computers to the internet.

6. With respect to the search of any of the items described above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment (including CDs, DVDs, thumb drives, flash drives, hard disk drives, or removable digital storage media, software, or memory in any form), the search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein, while permitting government examination of all the data necessary to determine whether that data falls within the items to be seized):

a. surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);

b. "opening" or curiously reading the first few "pages" of such files in order to determine their precise contents;

c. "scanning" storage areas to discover and possibly recover recently deleted files;

d. "scanning" storage areas for deliberately hidden files; or

e. performing key word searches or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

If, after performing these procedures, the directories, files, or storage areas do not reveal evidence of obtaining information from a protected computer, intentional damage to a protected

computer, cyberstalking, aggravated identity theft, or other criminal activity, the further search of that particular directory, file or storage area, shall cease.