

AFFIDAVIT OF POSTAL INSPECTOR FREDERICK T. BUSCH

I, Postal Inspector Frederick T. Busch, being duly sworn, depose and states as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am employed as a Postal Inspector with the United States Postal Inspection Service (“USPIS”), and have been so employed since March of 2006. During my employment as a Postal Inspector, I have received training in conducting investigations involving crimes that adversely affect, or fraudulently use, the United States mail and Postal Service. I have conducted or participated in criminal investigations involving various violations of Title 18 involving financial crimes including mail, bank and wire fraud, identity theft, money laundering, and credit card fraud, as well as investigations involving narcotics trafficking and child pornography.

2. In the course of my employment and in conducting or participating in these investigations, I have received training and have been involved in the use of investigative techniques such as interviewing informants and cooperating witnesses; conducting physical surveillance; consensual monitoring and recordings utilizing both telephonic and non-telephonic communications; analyzing telephone and pen register data; and analyzing records including bank records. I have prepared and/or executed numerous search and arrest warrants.

3. I make this affidavit in support of a criminal complaint charging Ming Xun Zheng, also known as Kellerman Jason Zheng (“KELLERMAN”) with mail and wire fraud, in violation of 18 U.S.C. §§ 1341 and 1343.

4. I also make this affidavit, pursuant to Rule 41 of the Federal Rules of Criminal Procedure, in support of an application for a warrant to search the residence of KELLERMAN’s [REDACTED] located at [REDACTED] Boston, MA 02115 (the “SUBJECT

LOCATION”), which is more fully described below and in Attachment A, and to seize evidence, instrumentalities, fruits of crime and contraband, as more fully described in Attachment B.

5. The facts in this affidavit are based on my own personal involvement with this investigation, including documents I have reviewed and witnesses I have interviewed. This affidavit does not detail all of the facts known to me regarding this matter, but instead relates only those facts which I believe are necessary to establish the requisite probable cause for issuance of search and arrest warrants. Except as set forth below, I have not distinguished between facts as to which I have personal knowledge, and facts as to which I have hearsay knowledge. In addition, when I rely on statements made by others, such statements are set forth in part and in substance, unless otherwise indicated.

PROBABLE CAUSE TO BELIEVE THAT A FEDERAL CRIME WAS COMMITTED

Relevant Individuals and Entities

6. KELLERMAN is a 32-year-old naturalized U.S. Citizen originally from China. Up until November 2019 when he relocated to Georgia, KELLERMAN resided with [REDACTED], [REDACTED] and [REDACTED] at the SUBJECT LOCATION.

7. [REDACTED]
[REDACTED]. [REDACTED] resides, and receives mail, at the SUBJECT LOCATION.

8. [REDACTED]
[REDACTED]. [REDACTED] resides, and receives mail, at the SUBJECT LOCATION.

9. Ming Fei Zheng (“Ming Fei”) was KELLERMAN’s brother and [REDACTED] of [REDACTED] and [REDACTED]. Based on the investigation, Ming Fei died in April 2015 in China.

10. Sagicor Life Insurance Company (“Sagicor”) is an insurance company headquartered in Scottsdale, Arizona, which provides annuities, life and health insurance services.

Background and Scheme to Defraud

11. Since approximately January 2019, investigators have been investigating KELLERMAN, [REDACTED], and [REDACTED] for their roles in a scheme to defraud life insurance companies. As part of the scheme, KELLERMAN fraudulently applied for life insurance policies in the name of his brother, Ming Fei, who had already died. In doing so, KELLERMAN made numerous material misrepresentations to insurance companies leading some of these companies to issue policies listing KELLERMAN and his parents as beneficiaries. Later, KELLERMAN fraudulently obtained false documents that listed Ming Fei’s death as having occurred in 2018 and made claims on the policies.

12. As part of the scheme, KELLERMAN and others took steps to make it appear as if Ming Fei was alive at the time the policies were applied for. Among other things, they opened and used bank accounts in Ming Fei’s name, listed a commercial mail receiving agency as Ming Fei’s purported residence, and renewed Ming Fei Massachusetts driver’s license in 2017.

13. Between approximately December 20, 2016 and March 20, 2018, at least 24 life insurance policy applications in Ming Fei’s name totaling approximately \$11,650,000 in combined coverage limits, were submitted online or by telephone to at least 20 U.S.-based insurance companies. Some of the policy applications were withdrawn, or the policy coverage amounts reduced, due to the applicant refusing in-person interviews, medical exams, or failing to provide medical documentation.

14. Life insurance policies typically have a one or two year contestability period, which is a short window during which insurance companies can investigate and deny claims. The period

begins when the policy goes into effect. Some policies, such as for accidental death, do not have a contestability period. The State of Massachusetts carries a two-year contestability period and at least two of the policies, purportedly taken out by Ming Fei, were Accidental Death policies applied for in or about March 2018.

15. Since approximately September 24, 2018, KELLERMAN has filed at least 12 claims on the aforementioned life insurance policies. The total value of the claims on these policies is approximately \$5.3 million. In response to these claims and because some were made during the policies' two-year contestability period, several insurers hired private investigation companies to investigate and review the claims.

16. KELLERMAN, [REDACTED] and [REDACTED] were interviewed by insurance investigators regarding these claims. According to statements made to insurance investigators by KELLERMAN, [REDACTED], and [REDACTED], Ming Fei allegedly drowned while in China on or about August 4, 2018 while swimming in a canal beside a power station in his hometown of Dabeitou Village, Guangdong Province.

17. Based on my investigation, including interviews with witness, recorded undercover meetings with KELLERMAN, and other records I have reviewed, it appears that Ming Fei actually died more than three years earlier, on or about April 4, 2015. Accordingly, the applications for life insurance policies for Ming Fei, submitted after his death and subsequent claims made on several of those policies, were fraudulent.

Sagicor Life Insurance Policy Number S000086823

18. On or about April 5, 2017, an individual I believe to be KELLERMAN, and purporting to be Ming Fei, submitted a life insurance policy application online to Sagicor. The

application was for a \$500,000 life policy with an additional Accidental Death Benefit Rider of \$250,000. The beneficiaries listed on the policy application were KELLERMAN, [REDACTED], and [REDACTED]. The application was signed electronically from IP address 155.52.187.16, which resolves back to the Dana Farber Cancer Institute in Boston, Massachusetts.

19. The premiums for the Sagicor policy were paid via a Discover Cash Back Checking account in the name of Ming Fei. Review of Discover records obtained during the investigation revealed that the Ming Fei account was opened on or about December 19, 2016 and was funded by a cashier's check and electronic transfer from KELLERMAN. Discover records for an account in KELLERMAN's name also revealed that KELLERMAN accessed his own Discover account electronically the day before Ming Fei's Sagicor application was submitted, and he did so from IP address 155.52.187.30, which also resolves back to the Dana Farber Cancer Institute in Boston, Massachusetts.¹

20. Based on the application, Sagicor issued policy number S000086823 in the name of Ming Fei.

21. The mailing and residence address listed for Ming Fei on the Sagicor application was 478 E. Altamonte Drive, Unit 108-630, Altamonte Springs, FL 32701, which is a UPS Store. As part of my investigation, I interviewed Bipin Patel ("Patel"), the owner of the UPS Store in Altamonte Springs, Florida. Patel stated Box 630 had been rented by KELLERMAN since February 2015 and that KELLERMAN instructed him to forward all mail to him at the SUBJECT LOCATION. Patel also stated no other individuals were associated with Box 630 and that he had

¹ During a meeting with an undercover agent that is described in greater detail below, KELLERMAN reported that he had previously been treated for leukemia and was in remission.

never heard of Ming Fei.

22. On or about March 15, 2019, Sagicor mailed letters via the United States Postal Service (“USPS”) to the SUBJECT LOCATION addressed to KELLERMAN, [REDACTED], and [REDACTED]. The letters notified the beneficiaries that Sagicor had learned of the death of Ming Fei and needed to contact members of his family regarding any potential claim.²

23. On or about April 17, 2019, KELLERMAN called Sagicor from telephone number [REDACTED] to confirm the death. During the call, which was recorded by Sagicor, KELLERMAN told Sagicor that, among other things, Ming Fei accidentally drowned on August 4, 2018 while in China.

24. The following day, on or about April 18, 2019, Sagicor mailed a letter addressed to each of [REDACTED] and [REDACTED], via USPS. The letter contained instructions and attached forms required to file a claim. The same letter and forms were e-mailed on or about April 18, 2019 to e-mail address [REDACTED], which is KELLERMAN’s email account.

25. On or about June 13, 2019 and June 26, 2019, KELLERMAN emailed Sagicor from the [REDACTED] account. The communications attached documents related to the claims and included a fraudulent death certificate that listed Ming Fei’s death as August 4, 2018, and Foreign Death Questionnaires purportedly completed by KELLERMAN, [REDACTED], and [REDACTED] reflecting the same information.

² Sagicor was notified of Ming Fei’s death by another insurance company that had also issued a policy to Ming Fei.

Insurance Company Investigations of Death Claims

26. On or about March 4, 2019, Diligence International Group (“Diligence”), a private investigation company located in Carrollton, Texas, received a request from Sagicor to investigate the Ming Fei death claim.

27. Diligence investigators travelled to China, as part of their investigation, interviewed an individual in the town where Ming Fei purportedly died – Dabeitou Village, Guangdong Province, China. The individual told the investigator that Ming Fei died of a sudden heart attack two or three years prior during Tomb Sweeping Day.³ The investigator also interviewed a local doctor, Dr. Yunjin Liang, who signed the death certificate indicating a death date of August 4, 2018. Dr. Liang reported that he was told how Ming Fei died by one of Ming Fei’s relatives.⁴ Investigators also interviewed local police officers who stated they had no record of any death or drowning on August 4, 2018.

28. The Diligence Investigators also interviewed Ming Fei’s [REDACTED] [REDACTED] who was in China during their investigation. [REDACTED] told investigators Ming Fei died on August 4, 2018 and that his body was buried. [REDACTED] refused to provide the location of the burial and referred investigators to KELLERMAN for any further questions.

³ The Qingming Festival, or Tomb-Sweeping Day, is a traditional Chinese festival during which Chinese families visit the tombs of their ancestors to clean the gravesites, pray to their ancestors, and make ritual offerings. It typically falls on either April 4th or 5th of a given year.

⁴ Dr. Liang was previously interviewed by insurance investigators from another private investigation company, Broyles. According to that investigation, Dr. Liang reported Ming Fei’s brother asked him to sign a death certificate that had already been filled out. Dr. Liang also reported the “time of death” was not accurate and that he was told Ming Fei died years earlier. Dr. Liang told the Broyles investigator that he had no information or documentation on how Ming Fei died and no autopsy was performed. Dr. Liang stated he did not know Ming Fei died two or three years earlier, that he saw the body but did not know the cause of death. Dr. Liang was told by Ming Fei’s relative

29. Diligence investigators interviewed a staff member at the Qingyuan Funeral Home in Qingyuan City, Guangdong Province, China. A staff member stated that there was a record of an individual by the name of Ming Fei Zheng, 27 years of age, who was cremated on April 4, 2015. Investigators later returned to the funeral home and spoke to the funeral home director, who confirmed Ming Fei died on April 4, 2015.

Travel and Other Records

30. As part of the investigation, I reviewed international flight and border crossing records for KELLERMAN, [REDACTED], [REDACTED], and Ming Fei for travel during the 2015 through 2018 timeframe.

31. There is no record of any international travel for Ming Fei after March 9, 2015, when Ming Fei flew from Boston to Beijing. There is no record of any return flight, or any border crossing into or out of the United States after that date.

32. Flight records also indicate that on or about April 4, 2015, KELLERMAN and [REDACTED] purchased two tickets on the day of travel via Expedia.com for travel from Boston to Beijing. The date of this trip corresponds with the date that insurance company investigators were told Ming Fei actually died. According to travel records, [REDACTED] was already in China during this timeframe and accompanied [REDACTED] back to the U.S. on or about May 9, 2015.

33. As part of the Sagicor claim, KELLERMAN, [REDACTED], and [REDACTED] submitted Foreign Death Questionnaires to the insurance company. All three reported that Ming Fei last departed the United States on July 23, 2018 to visit family abroad.⁵ Records also indicated that KELLERMAN

that he had drowned.

⁵ Significantly, the same questionnaires also listed Ming Fei's last known address in the

and [REDACTED] flew from Chicago to Shanghai, China on or about July 25, 2018, shortly before the death date reported to the insurance companies. [REDACTED] appears to have been in the United States at that time, but did not travel to China until on or around October 23, 2018.

Undercover Operation

Initial Telephone Contact - September 9, 2019

34. On or about September 9, 2019, an undercover agent (the “UC”) posing as a claims manager for Sagicor, spoke with KELLERMAN via telephone. During the call, which was consensually recorded, the UC introduced himself to KELLERMAN, told him he would be travelling to the Boston area, and requested an in person meeting. KELLERMAN confirmed that he resided at the SUBJECT LOCATION and agreed to meet with the UC in the lobby of the Westin Hotel in Boston, Massachusetts on September 11, 2019.

September 11, 2019 Meeting

35. On or about September 11, 2019, KELLERMAN met with the UC in the lobby of the Westin Hotel in Boston, Massachusetts. During this recorded meeting, the UC told KELLERMAN that his company had conducted an investigation in China and discovered information suggesting that Ming Fei passed away before the policy went into effect. KELLERMAN told the UC that Chinese officials must have been bribed by the “third-party” insurance investigators to get information that suggested Ming Fei died years prior to the applications being submitted. KELLERMAN stated, “And we can do the same thing too. As long as we got money and connection. That’s why we could bury them, we could alter all this paperwork too.”

United States as 478 E. Altamonte Drive, Unit 108-630, Altamonte Springs, FL 32701, which as explained above, is a UPS store.

36. The UC continued, telling KELLERMAN that he had a lot of power in the company [Sagicor] and that, if he could get more documentation from KELLERMAN to push the claim through, they both could make some money. KELLERMAN agreed to locate additional documents and meet the UC in two weeks.

October 8, 2019 Meeting

37. On or about October 8, 2019, KELLERMAN met with the UC in a restaurant in South Boston, Massachusetts. During this meeting, which was consensually recorded, the UC explained to KELLERMAN that if KELLERMAN could furnish a document with the actual date of Ming Fei's death, the UC would be able to backdate the policy application and make it appear as if the policy was in effect before Ming Fei died. Specifically, the following exchange occurred:

UC: If you can give me a document with the actual date he died, and me and you can trust each other, I can backdate the application that it was initiated before your brother actually passed.

Kellerman: With no track?

UC: No track.

Kellerman: So that-

UC: I've done it, listen to me, I-I gave you this card before, I am in charge of all the claims for the Northwest region. I've done this four-five times. Everybody's gotten paid. Nobody cares the wiser. Everybody's happy.

Kellerman: So that means you can make the application backdated in 2014?

UC: Whatever works for the actual date.

Kellerman: But, I just need to provide the official verification --

UC: Yeah, I need to know from you that piece of paper is the actual document. As long as I know that's true – I'll backdate it to make sense, we'll make sure our stories are straight and everything should be fine.

Kellerman: So we could match the (UI) in China (UI). So that's the (UI).

UC: Exactly. Ok? It's a \$750 [thousand] policy. Are you comfortable with giving me \$150 [thousand]?

Kellerman: M-hum.

38. Later on in the meeting while discussing the specifics of how the scheme would work, KELLERMAN acknowledged that his brother Ming Fei died on April 4, 2015.

Kellerman: Ok, yeah. So all you need just one document. That's it.

UC: I just need to actual death certificate.

Kellerman: The death certificate.

UC: Yeah. When's the actual death?

Kellerman: Um, April 4, 2015.

UC: April 4, 2015?

Kellerman: Yeah.

39. The meeting continued and the UC asked KELLERMAN whether Ming Fei flew to China prior to his death in 2015, and if so, whether there was a record of his travel. KELLERMAN nodded affirmatively to both questions and explained that Ming Fei travelled "three weeks" before he died, which is consistent with the travel records described above.

40. KELLERMAN and the UC then agreed to meet the following night so that KELLERMAN can show that UC the document reflecting Ming Fei's actual date of death.

October 9, 2019 Meeting

41. On or about October 9, 2019, KELLERMAN picked up the UC at the Westin Hotel and drove the UC to a restaurant in the Chinatown section of Boston, Massachusetts. During this

meeting, which was consensually recorded, KELLERMAN produced a document that he said was a cremation certificate for his brother. KELLERMAN again confirmed that his brother actually died on April 4, 2015.

42. The document that KELLERMAN showed the UC was in Mandarin Chinese. KELLERMAN translated the text of the certificate along with receipts that were also attached to the document. The document listed Ming Fei's death as April 4, 2015 and stated that he was cremated on April 6, 2015.

43. As the meeting continued, KELLERMAN appeared to become nervous and began asserting that his brother had died in 2018, contradicting his own prior statements. KELLERMAN also presented inconsistent accounts about when he and [REDACTED] travelled to China after his brother's death. Then the following exchange occurred:

UC: Listen, I don't want to – I don't want to. Wait – wait you are not being straight with me now. You have to be straight with me Jason or I can't – I'm not going to take the risk. I have been doing this for a long time. Because if I go in a put in that's it's official in 2015 and it's really not I'm going to be the one who is in trouble.

Kellerman: You whatever I show you – you just (UI). I'm in trouble too.

UC: No you're not. Not here. I don't care what you did in China. I need to know when he really died. I need to know when he really actually died so we can make this right before I go back to Arizona.

Kellerman: Alright.

UC: As of last night and five minutes ago it was April 4, 2015.

Kellerman: Correct.

UC: Is that when he actually died?

Kellerman: Yes.

UC: Ok.

Kellerman: Alright.

UC: Alright. That's—I understand and I sympathize with the whole cremation thing. Like I'm sorry you had to go through that in China. That's not something we have to go through here ok. If he really died in April then that cremation certificate is the actual certificate.

Kellerman: Oh yeah absolutely. That's the officer in China give to me.

UC: Ok, so what are you talking about 2018?

Kellerman: What I give you that was all false document then.

UC: 2018?

Kellerman: Yeah.

44. Later, KELLERMAN, who still appeared nervous about his discussions with the UC, made statements about needing to make sure the UC was not an undercover FBI agent, not wanting to have federal agents “bust” his door, and not having to “hire a criminal attorney.”

45. KELLERMAN refused to give the UC the actual cremation certificate during the meeting, but agreed to email him a copy from an email address different from the one he previously used to communicate with Sagicor regarding the claim. On or about October 10, 2019, KELLERMAN e-mailed the UC from e-mail address [REDACTED] and attached a scanned copy of the cremation certificate.

46. Over the course of the next month, the UC and KELLERMAN communicated via email and text message on various occasions and agreed to meet again in Georgia to finalize the fraudulent insurance claim. As part of the ruse, the UC agreed to give KELLERMAN a hardcopy insurance application, which KELLERMAN could complete and which the UC would purportedly enter into the Sagicor system in place of the prior application.

November 12, 2019 Meeting

47. On or about November 12, 2019, the UC met KELLERMAN in the lobby of the Westin Hotel in Atlanta, Georgia. During this meeting, which was consensually recorded, the UC gave KELLERMAN a Sagicor application that KELLERMAN signed as Ming Fei. KELLERMAN dated the application March 18, 2013. During the meeting, KELLERMAN also completed several Sagicor claim documents, which he filled out using a death date of April 4, 2015. KELLERMAN thereafter provided the UC with the original cremation certificate and associated receipts in support of the claim.

**PROBABLE CAUSE TO BELIEVE THAT EVIDENCE, FRUITS, AND
INSTRUMENTALITIES OF THE CRIMES IDENTIFIED ABOVE
WILL BE FOUND AT THE SUBJECT LOCATION**

48. I have probable cause to believe that the SUBJECT LOCATION contains fruits, evidence, and instrumentalities of violations of the federal statutes listed above, as described in Attachment B.

49. The SUBJECT LOCATION is [REDACTED], Boston, Massachusetts 02115 within a housing development operating under the name [REDACTED]. [REDACTED] operates numerous buildings within the complex. As described more fully in Attachment A, the SUBJECT LOCATION is apartment number [REDACTED].

50. Massachusetts Registry of Motor Vehicle (“RMV”) records as well as public records from databases available to law enforcement indicate that [REDACTED] and [REDACTED] currently reside at the SUBJECT LOCATION. Records also list KELLERMAN as having resided at the SUBJECT LOCATION.

51. On December 9, 2019, investigators conducted surveillance and met with [REDACTED] representatives at the SUBJECT LOCATION. The [REDACTED] representatives confirmed that [REDACTED] and [REDACTED] reside at the SUBJECT LOCATION.

52. Since 2016, when the alleged fraud began, numerous insurance policy applications were submitted in Ming Fei's name listing KELLERMAN's mailbox in Altamonte Springs, Florida as Ming Fei's mailing and residential address. As noted above, any mail received at this commercial mail receiving facility was forwarded to KELLERMAN at the SUBJECT LOCATION.

53. In addition, during the course of the scheme, insurance policy claim documentation for KELLERMAN, [REDACTED], and [REDACTED] was sent to and from the SUBJECT LOCATION. For example, in connection with the Sagicor claim discussed above, Sagicor mailed claim forms and instructions to KELLERMAN, [REDACTED], and [REDACTED] at the SUBJECT LOCATION.

54. Mailing records obtained from several victim insurance companies during the course of the investigation indicated that in September and October 2018, [REDACTED] submitted claims to other life insurance companies (North American and Phoenix) from the SUBJECT LOCATION.

55. RMV records revealed that despite the fact that Ming Fei died in 2015, someone renewed his Massachusetts's driver's license online in 2017 and listed the SUBJECT LOCATION as Ming Fei's address.

56. Accordingly, there is probable cause to believe that records related to Ming Fei, insurance policies applied for in his name, and claims made in connection with those policies at the SUBJECT LOCATION.

SEIZURE OF COMPUTER EQUIPMENT AND DATA

57. From my training, experience, and information provided to me by other agents, I am aware that individuals frequently use computers to create and store records of their actions by communicating about them through e-mail, instant messages, and updates to online social networking websites; drafting letters; keeping their calendars; arranging for travel; storing pictures; researching topics of interest; buying and selling items online; and accessing their bank, financial, investment, utility, and other accounts online.

- a. Based on my training, experience, and information provided by other law enforcement officers, I know that many cell phones (which are included in Attachment B's definition of "hardware") can now function essentially as small computers. Phones have capabilities that include serving as a wireless telephone to make audio calls, digital camera, portable media player, GPS navigation device, sending and receiving text messages and emails, and storing a range and amount of electronic data. Examining data stored on devices of this type can uncover, among other things, evidence of communications and evidence that reveals or suggests who possessed or used the device.
- b. I am aware of a report from the United States Census Bureau that shows that in 2016, among all households nationally, 89 percent had a computer, which includes smartphones, and 81 percent had a broadband Internet subscription. Specifically, in 2016, when the use of smartphone ownership was measured separately for the first time, 76 percent of households had a smartphone and 58 percent of households had a tablet, and 77 percent of households had a desktop or laptop computer. Further, according to the Pew Research Center, as of 2019, 96 percent of adult Americans own a cellphone, and 81 percent own a cellphone with significant computing capability (a "smartphone"). The percentage of adults that own a smartphone is even higher among younger demographic groups: 96 percent of 18-29 year olds, 92 percent of 30-49 year olds, and 79 percent of 50-64 year olds owned smartphones in 2019.
- c. From my training and experience, I am aware that personal computer systems are generally capable of creating, receiving, and otherwise processing computer files, such as e-mail, word-processing documents, photographs, and spreadsheets.

58. Moreover, as set forth above, I am aware that KELLERMAN used computers in the course of the scheme, including during the time he was living at the SUBJECT LOCATION. For example, as noted above, in June 2019, while living at the SUBJECT LOCATION, KELLERMAN emailed Sagicor foreign death questionnaires and a fraudulent death certificate. In addition, numerous insurance policies and claims submitted by KELLERMAN, [REDACTED] and [REDACTED] were submitted electronically, which indicates the use of computers to fill out the forms.

59. Based on my knowledge, training, experience, and information provided to me by other agents, I know that computer files or remnants of such files can be recovered months or years after they have been written, downloaded, saved, deleted, or viewed locally or over the Internet. This is true because:

- a. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their computers, they can easily transfer the data from their old computer to their new computer.
- b. Even after 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, which might not occur for long periods of time. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how the computer has been used, what it has been used for, and who has used it. This 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. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is typically required for that task.

- d. Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.
- e. Data on a 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, email 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.
- f. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information

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

- g. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- h. 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.
- i. 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.

60. Based on my knowledge and training and the experience of other agents with whom I have spoken, I am aware that in order to completely and accurately retrieve data maintained in

computer hardware, computer software or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, and storage media ("computer equipment") be seized and subsequently processed by a computer specialist in a laboratory setting rather than in the location where it is seized. This is true because of:

- a. The volume of evidence — storage media such as hard disks, flash drives, CDs, and DVDs can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine which particular files are evidence, fruits, or instrumentalities of criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis on-site.
- b. Technical requirements — analyzing computer hardware, computer software or storage media for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even "hidden," deleted, compressed, or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a "booby trap."

Consequently, law enforcement agents may either copy the data at the premises to be searched or seize the computer equipment for subsequent processing elsewhere.

61. The premises may contain computer equipment whose use in the crimes or storage of the things described in this warrant is impractical to determine at the scene. Computer equipment and data can be disguised, mislabeled, or used without the owner's knowledge. In addition,

technical, time, safety, or other constraints can prevent definitive determination of their ownership at the premises during the execution of this warrant. If the things described in Attachment B are of the type that might be found on any of the computer equipment, this application seeks permission to search and seize it onsite or off-site in order to determine their true use or contents, regardless of how the contents or ownership appear or are described by people at the scene of the search.

62. The law enforcement agents will endeavor to search and seize only the computer equipment which, upon reasonable inspection and/or investigation conducted during the execution of the search, reasonably appear to contain the evidence in Attachment B because they are associated with (that is used by or belong to) the KELLERMAN, [REDACTED], or [REDACTED]. If however, the law enforcement agents cannot make a determination as to use or ownership regarding any particular device, the law enforcement agents will seize and search that device pursuant to the probable cause established herein.

..

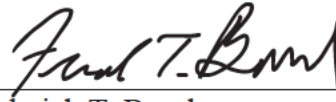
.

CONCLUSION

63. Based on the information described above, I have probable cause to believe that between April 5, 2017 and the present, KELLERMAN committed mail and wire fraud, in violation of 18 U.S.C. §§ 1341 and 1343, in connection with the fraudulent Sagicor life insurance policy in Ming Fei's name and the false claims he made on that that policy.


64. Based on the information described above, I also have probable cause to believe that located on the premises of [REDACTED], Boston, MA 02115, as more fully described in Attachment A, is evidence, fruits, or property designed for use, intended for use, or used in committing the described criminal offenses as more fully described in Attachment B.

Sworn to under the pains and penalties of perjury, this 11th day of December, 2019.



Frederick T. Busch
Postal Inspector
United States Postal Inspection Service

Subscribed and sworn to before me, this 11th day of December, 2019.



Hon. David H. Hennessy
Chief United States Magistrate Judge

