AFFIDAVIT OF SPECIAL AGENT KRISTIN D. KOCH IN SUPPORT OF AN APPLICATION FOR AN ARREST AND SEARCH WARRANTS

I, Kristin D. Koch, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), and have been since June of 2003. I was assigned to the Boston Division of the FBI in October of 2003. I am currently assigned to the Organized Crime Task Force, Squad C-3, where I work on investigations relating to organized crime, labor racketeering and major theft.

2. As an FBI Special Agent, I have participated in investigations involving organized crime, labor racketeering, violent crime (including extortion), illegal distribution of controlled substances, firearms offenses, interstate gambling offenses, loan sharking, white collar crime, art theft, and fugitives. In the course of these investigations, I have been the affiant on and participated in the execution of numerous arrest and search warrants. Through my training, education, and experience, including the debriefing of witnesses, I have become familiar with, among other criminal activities, the manner in which individuals carry out art theft and fraud.

3. I am currently investigating Brian R. Walshe ("Walshe") for wire fraud, in violation of Title 18, United States Code § 1343, sale or receipt of stolen goods in violation of Title 18, United States Code § 2315, and transportation of stolen goods in violation of Title 18, United States Code § 2314 (collectively, the "Target Offenses").

4. I submit this affidavit in support of an application for a criminal complaint charging Walshe with wire fraud in violation of 18 U.S.C. § 1343.

5. I also submit this affidavit in support of applications for the issuance of search warrants pursuant to Fed. R. Crim. P. 41, authorizing a search of the following premises, all more fully described below:

a. A condominium located at Lynn, Massachusetts, (hereinafter, the "Residence"), more fully described in Attachment A;

b. An email account: brianwalshe71916@gmail.com, more fully described in Attachment B;

c. An email account: brw@tensailconsulting.com, more fully described in Attachment C.

6. I also submit this affidavit in support of an application for the issuance of search warrants for the persons of Walshe and Ana Knipp, who are described more fully below in Attachment D.

7. I submit that there is probable cause to believe that the Residence, the Email Accounts, and the persons of Walshe and Knipp contain evidence, fruits and instrumentalities of violations of the Target Offenses, as described in Attachments E, F, G, and H, respectively.

8. The statements contained in this affidavit are based on my own investigation, including interviews with the victims discussed below, review of documents and other records, and on information provided to me by other Special Agents of the FBI, other law enforcement officers and witnesses. This affidavit is submitted for the limited purpose of establishing the requisite probable cause for the requested warrants and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE TO BELIEVE FEDERAL CRIMES WERE COMMITTED

Walshe Defrauded Victim 1 Through Sale of Fake Warhol Paintings

9. In early November 2016, a person known to the FBI, whom I will call "Victim 1,"[1]

[1] Victim 1 owns a gallery in Los Angeles, California, that buys and sells works of art by Andy Warhol. I have met and spoken to Victim 1 several times.

found two Andy Warhol "Shadow" paintings (the "Paintings") for sale on eBay.[2] Victim 1 provided copies of the listing to the FBI. The original listing price for the Paintings was $100,000 for the pair. The listing included photographs of the Paintings and indicated that each painting had a Warhol Foundation authentication stamp on them. The eBay seller was listed as: ancili2012. The item description was as follows:

> "We are selling 2 Andy Warhol paintings from our private collection. We are parting with these pieces only because we need the money for renovations to our house. Our loss is your gain. Pieces bought from a former Martin Lawrence art dealer in California. We over paid terribly in 2007 for the art. Price paid $240,000. We have enclosed the Christie's estimates as of 2011 for the art as well. Auction range $120,000 to $180,000. We are trying to sell on Ebay (sic) because it is much cheaper and because Christie's won't be able to auction our pieces till May 2017. The pieces are numbered and registered with the Warhol Foundation. Pieces are from 1979. Size 14 inches by 11 inches. Synthetic Polymer Paint and Silkscreen ink on canvas. *Warhol Foundation # PA65.049 & PA65.032.*"[3] (emphasis added)

10. The eBay seller included a photograph of an invoice from Fleishman Fine Art for the two Warhol Shadow paintings, with the same Warhol Foundation numbers, and a purchase price of $240,000. However, the "Bill To" and "Ship To" were listed as: [Name Redacted]/

Gangnam-gu, Seoul, Korea, not Walshe. In addition, the eBay seller also included photographs of a label on the back of the painting from the Jablonka Gallery with the number PA65.049; and a photograph of a document from Christie's document listing the Paintings and two works by Keith Haring ("Haring").[4]

---

[2] Andy Warhol (1928-1987) was an American visual artist and among the leading figures of "pop art." His works include some of the most expensive pieces ever sold. Warhol's "Shadows" are a series of untitled, abstract, acrylic on canvas paintings from 1978. Photographs of the Paintings are included in the Appendix to this Affidavit.

[3] The Warhol Foundation number referred the unique identifier given to the painting by the Andy Warhol Art Authentication Board, Inc., a private corporation associated with the Andy Warhol Foundation for the Visual Arts (now defunct), which certified the authenticity of the work. The number was on a stamp affixed to the back of the painting.

[4] Keith Haring (1958-1990) was an American artist known for pop art which had a graffiti-like appearance.

11. Victim 1 believed that the Paintings were authentic because of the Warhol Foundation numbers and, as a result, was interested in purchasing them. Victim 1 communicated through eBay messenger with the seller, who identified herself in some communications as "Ana," who I believe was Ana Knipp ("Knipp"), Walshe's wife. Victim 1 provided his phone number and asked the seller to contact him directly. Victim 1 received a phone call from -4735 and the individual at the other end of the line identified himself as Walshe.[5] Between November 3 and 5, 2016, Walshe and Victim 1 exchanged a number of communications, with each person initiating contact.

12. On November 3, 2016, Walshe and Victim 1 reached agreement: Victim 1 would purchase the Paintings for a total of $80,000 outside of eBay.[6] Walshe told Victim 1 that he (Walshe) wanted to make the exchange private, to which Victim 1 agreed, because eBay would charge a fee for the transaction. Victim 1 then drew up a contract through DocuSign,[7] which was executed by both parties on November 3, 2016. The contract specified that the buyer had three days to terminate the contract and get a full refund if the buyer did not accept the artwork. Walshe also sent a copy of his Massachusetts driver's license to Victim 1.[8] Victim 1 stated that he would not have purchased the Paintings if they had not had the Warhol Foundation authentication stamps on them.

13. Walshe communicated with Victim 1's assistant, whom I will call Witness 1, using the

---

[5] According to telephone records through April 2017, -4735 is a Verizon Wireless number subscribed to by Walshe and assigned to a Blackberry, which is a kind of smartphone. The first telephone contact between this phone number and the numbers used by Victim 1 was on November 3, 2016.

[6] eBay also owns PayPal, which provides an escrow service for transactions conducted over the site for a fee.

[7] DocuSign is an online contracting service.

[8] I have seen this copy and confirmed that it was for Walshe, with an address of 225 Beacon Street, Boston, Massachusetts.

email address: brw@tensailconsulting.com. They agreed that Witness 1 would fly to Boston on November 7, 2016 to meet Walshe, pick up the Paintings, and present Walshe with a cashier's check for $80,000. On November 3, 2016 at 6:05 p.m. PDT, Walshe wrote in response to an email from Witness 1 telling him that she sent over the purchase agreement: "Hello, Looks good. Let me know if you have received the signed document. I have a carry on for the pieces. Will you have insurance to travel with the art? I will bring my insurance documents when we meet on Monday. If you like I can send them to you later today?[9] Best Brian". On the same date at 6:34 p.m. PDT, Walshe also sent Victim 1 and Witness 1 an email from the address brainwalshe71916@gmail.com that contained a photograph of each painting.

14. On November 6, 2016 at 6:03 a.m. PDT, Walshe sent an email to Victim 1 from the email address: brianwalshe71916@gmail.com. In this email Walshe asked Victim 1 if he was interested in purchasing three more Warhol abstract paintings. Victim 1 declined.

15. On November 7, 2016, Witness 1 flew to Boston to meet with Walshe. The meeting was supposed to take place at 225 Beacon Street in Boston (the address on Walshe's license) but at the last minute Walshe changed the location. He asked Witness 1 if she could meet him at the Four Seasons Hotel in Boston instead. Witness 1 agreed and they met in the hotel's Bristol Lounge.

16. I have reviewed video surveillance from the Four Seasons Hotel for November 7, 2016 for the entrance to the Bristol Lounge. At approximately 10:23 a.m. EDT, an individual carrying a small suitcase and a brown shopping bag, whose face was not fully visible, entered the Bristol Lounge. At approximately 11:05 a.m. EDT, this same individual – whom I could at this point

[9] Victim 1 did receive an insurance document from Walshe. However, I believe that it was a quote, not a contract, and that Walshe never actually insured the Paintings.

identify as Walshe – left the Bristol Lounge only carrying the small suitcase.

17. Walshe brought what he represented were the Paintings. Upon inspection, Witness 1 could not see the Warhol Foundation authentication stamps because the frames were covering the backs of the paintings. Witness 1 used her cellphone to take photographs of the Paintings and sent them via text message to Victim 1, who was in his car and did not have the original photographs with him to make the comparison. He thought the photographs sent by Witness 1 looked like the photographs he had seen on the eBay listing, so he authorized her to make the purchase. Witness 1 gave the cashier's check for $80,000 to Walshe and he gave her the Paintings. Witness 1 flew back to Los Angeles with the Paintings that day, and brought them to Victim 1 the next day, which was November 8, 2016.

18. According to bank records, on November 7, 2016, the $80,000 cashier's check was deposited into the business account for Ten Sail Consulting LLC, for which Walshe was the only signatory. On November 8, 2016, there was an ATM cash withdrawal of $500. On November 9, 2016 there were four transactions titled "Chase Credit Card Bill Payment" totaling $24,900 going out of the account. On November 21, 2016, there were two cash withdrawals totaling $8,000.

19. On November 8, 2016, Victim 1 removed the frames and found no Warhol Foundation authentication stamps. He also noticed that the canvasses and staples looked new. When he compared the Paintings to the photographs from the eBay listing, they did not look identical. Victim 1 concluded that the Paintings that he purchased from Walshe were not what had been described in the eBay listing.

20. Starting on November 8, 2016, Victim 1 attempted to contact Walshe via telephone, text

message and email.[10] Walshe did not respond to Victim 1's attempts to reach him.

21. Victim 1 was able to find a contact number for Walshe's mother. On November 8, 2016, Victim 1 contacted her and asked her to have Walshe call him back. Instead, Victim 1 got a call from her attorney who said that she (Walshe's mother) was not responsible for her son but that Walshe would contact Victim 1 in the next few days to resolve the situation.

22. Victim 1 also was able to find a work contact number for Knipp, Walshe's wife. Victim 1 spoke to her. On November 16, 2016 at 9:10 a.m.,[11] Victim 1 received an email from the address brw@tensailconsulting.com, which read:

> "Hello [Victim 1], Thank you for calling my wife. She said you were very kind and respectful, which is how I remembered you from our first interaction. I was going to call on Tuesday (election day) to ask about the 'shadows', but because of the time difference I was unable. I was in meetings and buildings all that day which did not allow me to have my phone. Once I saw your messages, things had already escalated to an uncomfortable level. Mr. Hardcastle is our family lawyer. He was trying to resolve the matter without unnecessary litigation. He was not going to represent me formally in any civil or criminal proceedings, but was hoping to satisfy you as a client. On Friday he did offer a full refund to your lawyer, but from your Saturday email it seemed it was too late to resolve this matter without a drawn-out court case. The information you explained to my wife is very troubling. If the photos I sent you are clearly different then the 'Shadows' you have now, then that is a serious problem. However, regardless of the problems with the 'shadows', you have a right to a full refund according to our written agreement in section 9.3. I have no reason to believe that you would mis-represent any information. When I spoke to you last I had the impression that you were a fair and honest businessman. My wife has the same impression since your conversation yesterday. I was just surprised with how quickly things escalated. I am traveling this week, but I would like to return your $80,000 ASAP. Please send me your Bank of America information and I will send you the money. Once you receive your money please send me the 'shadows'. I need to investigate what happened on my side of this transaction. Once I have the 'shadows' and can confirm your information, I will also refund the cost of sending [Witness 1] to Boston. I don't want you to suffer financially from this transaction. Especially, if the fault is on my side. Thank you again for reaching out to my wife. I will be in touch directly with you later this week. Best Brian".

---

[10] According to records for Walshe's number (-4735), Walshe's phone received sixteen incoming calls and text messages from Victim 1 between November 8 and 12, 2016, which were not answered or responded to.

[11] Where a time zone is not listed, the records do not indicate whether it was EDT or PDT.

23. Over the next several days and then weeks Walshe continued to tell Victim 1 that he was trying to refund his money. Eventually, Walshe stated that the money would be returned in several transactions. However, every time Victim 1 asked Walshe where the money was, Walshe gave him an excuse. For example, on November 23, 2016 at 12:06 p.m., Walshe responded to an email from Victim 1 by stating in part, "…Sorry for the delay. They set the wires up yesterday when the teller systems were down. I am waiting to get confirmation the $15,000 went out today. I am still waiting for some off-shore checks and wires to clear. Once that occurs the other $50,000 will be sent in 2 wires. Sorry for the delay…" All of these communications occurred over email from the email address: brw@tensailconsulting.com.

24. In the end, Walshe refunded Victim 1 $30,000. A wire transfer for $15,000 from the Ten Sail Consulting LLC account to an account controlled by Victim 1 was completed on November 22, 2016. A second direct account transfer for $15,000 from the Ten Sail Consulting LLC account to Victim 1's account was completed on November 28, 2016. There were no additional deposits or incoming wires into that account before those wires went sent to Victim 1.

25. Walshe continued to make excuses to Victim 1 as to why he could not return the remaining funds. On December 8, 2016, Victim 1 sent Walshe an email stating that he had spoken with the FBI and would leave the matter to the authorities. Victim 1 has had no contact with Walshe since then and received no further funds from Walshe.

Walshe Stole The Paintings and Additional Art Work From Victim 2

26. Another witness, whom I will call "Witness 2", who worked at Fleischman Fine Art, provided additional information regarding the Paintings. In 2007, Witness 2 stated that he purchased the Paintings from the Jablonka Gallery in Germany after he had identified a buyer for them. Witness 2 sold them to that buyer, listed on the Fleischman Fine Art invoice as "[name

redacted]/ ." Witness 2 thought that actual buyer was "Sam Chang," whom Witness 2 had met in the company of Walshe a few years earlier when Witness 2 was working at the Martin Lawrence Gallery in Los Angeles. After this meeting, Walshe occasionally called Witness 2 to ask about Warhol or Haring artwork.

27. The true owner of the Paintings is the family of a person, whom I will call "Victim 2."[12] Victim 2 met Walshe in 1994 at Carnegie Melon University when they were both students there. Walshe did not graduate and was only there for a year; Victim 2 did graduate and eventually returned to South Korea, where Victim 2 lived and worked. Walshe often visited Victim 2 in Korea and stayed for several weeks or longer at a time. Victim 2 last saw Walshe in 2012, when Walshe attended Victim 2's wedding in Korea.

28. Victim 2 purchased a number of pieces of art from Witness 2, who once worked at the Martin Lawrence Gallery.[13] Victim 2 thought that he met Witness 2 in 2004 or 2005. Walshe was present with Victim 2 and Victim 2's parents when he first purchased a Warhol painting from Witness 2. Sometime after this purchase, Witness 2, who had left the Martin Lawrence Gallery but was still dealing in fine art, called Victim 2 and asked him if he was interested in purchasing two Shadow paintings by Warhol: the Paintings at issue here. Victim 2 was interested and Witness 2 purchased the art for Victim 2. The invoice was in the name of Victim 2's sister's and father's company. Victim 2's father paid for the paintings. In total, Victim 2 thought that he did six or seven transactions with Witness 2, including two Haring pieces.

29. In addition, in Las Vegas, Victim 2 purchased a Warhol Dollar Sign, which is a silk screen print of a dollar sign on a handkerchief, for approximately $15,000 to $18,000. Victim 2's

---

[12] Victim 2 is a South Korean national. I have met and spoken to Victim 2.

[13] The Martin Lawrence Gallery is a well-established art gallery operating in Los Angeles and Las Vegas, among other places.

parents, but not Walshe, were with him during that purchase.

30. At some time in Korea, Walshe told Victim 2 that he (Walshe) could sell some of the art belonging to Victim 2 and his family. Victim 2 had not thought about selling any paintings but Walshe said that he could get a good price. Victim 2 trusted Walshe and let Walshe take some of his art from Victim 2's family home: the Paintings, plus two prints by Haring, the Warhol Dollar Sign print, and a porcelain statue from the Tang Dynasty.

31. After some time passed and Victim 2 had not heard from Walshe, Victim 2 tried to reach Walshe by telephone and email, without success. Eventually Victim 2 reached out to a mutual friend from their college days, whom I will call "Friend 1."[14] Victim 2 asked Friend 1 to call Walshe and find out what he had done with the art. Friend 1 called Walshe and Walshe answered the phone. In response to Friend 1's request, Walshe said that he would return the art he had taken from Victim 2. However, every time they were supposed to meet up Walshe came up with an excuse about why he did not show up or had to cancel.

32. Eventually Friend 1 called a friend of his from the Massachusetts Institute of Technology, whom Friend 1 knew from graduate school and whom I will call "Friend 2." Friend 1 asked Friend 2, who still lived in Boston and had met Walshe, to go to Walshe's house and retrieve Victim 2's art. Friend 2 saw Walshe at 225 Beacon Street and demanded the art. Walshe gave Friend 2 two prints by Haring and the Tang Dynasty porcelain statue but not the Warhols. Friend 2 in turn gave these items to Friend 1 for Victim 2.

33. According to a document labelled an "invoice" from the Gagosian Gallery in New York City,[15] on May 3, 2011, Walshe attempted to consign the Paintings. An employee of the

[14] I know Friend 1's name and address.
[15] The Gagosian Gallery is another well-known art gallery with locations around the world.

Gagosian Gallery who met with Walshe told the FBI that the Gallery declined to accept the paintings because Walshe did not have a bill of sale. Walshe also had the Dollar Sign and two Keith Haring prints with him.

34. According to records of Christie's, the auction house, on September 21, 2011, an Andy Warhol Dollar Sign was sold on consignment for a hammer price[16] of $40,000 for Brian Walshe of 225 Beacon Street, Boston, Massachusetts. The provenance was the Bellagio Gallery of Fine Art in Las Vegas. I believe that the Dollar Sign was the piece that Walshe obtained from Victim 2.

35. I believe that, as demonstrated by the information from Fleischman, the photographs, and the Warhol Foundation numbers, Victim 2 purchased authentic Paintings that Walshe took from him. I also believe that Walshe falsely offered the authentic Paintings for sale in his eBay listing but that he delivered fake paintings to Victim 1. I also believe that Walshe may have used the authentic Paintings to create the fake paintings and that the authentic Paintings are likely still in Walshe's possession.

PROBABLE CAUSE TO BELIEVE THAT THE PERSONS TO BE SEARCHED CONTAINS EVIDENCE, FRUITS, AND INSTRUMENTALITIES

36. From my training and experience, I am aware that when a person handles an object, he or she can leave behind fingerprints and/or trace amounts of deoxyribonucleic acid ("DNA"). A report from an Examiner at the FBI Laboratory advised that fingerprints and a partial palm print of unknown origin were located on the black frames that contained the Paintings. Although DNA testing has not been conducted on the black frames to date, it is well established in the scientific community that a person who handles an object may leave behind traces of their DNA.

[16] The "hammer price" is the auction price. The auction house typically adds a percentage from 25% to 20%, which is the "buyer's premium."

Based on the aforementioned information provided by Victim 1 and Witness 1, and my review of the video surveillance from the Four Seasons Hotel, I have probable cause to believe that Walshe's fingerprints and/or palm prints and/or DNA may be on the black frames.

37. In addition, I am aware that Knipp is the wife of Walshe. I have seen a copy of a marriage certificate dated December 21, 2015 and recorded January 7, 2016, for Walshe and Knipp. In addition, Walshe referred to Knipp as his wife in an email to Victim 1, discussed above. And, as discussed below, I believe that Walshe and Knipp live together at the Premises.

38. According to the marriage license, Knipp was going to change her last name to Walshe. However, her RMV listing, bank records, and the deed for the Residence, continue to list her as Knipp. Accordingly, I have referred to her as Knipp, although she may also go by the married name of Walshe.

39. Knipp participated in the sale of the Paintings as discussed above. Walshe (or Knipp) used her eBay listing and she spoke to Victim 1. In addition, they were married and, I believe, living together, at the time of the sale. As a result, I believe that it is possible that Knipp and Walshe may have handled the fake paintings given to Victim 1 or the real Paintings, which I hope to recover in the search of the Premises, and may have left prints or DNA on evidence as a result.

40. In addition to the Paintings, I also believe that Walshe (or Knipp or both) likely handled other evidence, as described in Attachments E below, and it is likely that the FBI will recover DNA from such evidence. I request the DNA samples in Attachment H, which will be useful for comparing to the samples which I believe that the FBI will likely recover in the search of the Premises.

PROBABLE CAUSE TO BELIEVE THAT THE RESIDENCE TO BE SEARCHED CONTAINS EVIDENCE, FRUITS, AND INSTRUMENTALITIES

41. A search of the Essex County Registry of Deeds revealed several records for the Residence. One of these records indicated that on April 15, 2016, Knipp purchased the property from a seemingly unrelated individual. She has owned the property since. I am also aware that most married people live together.

42. On February 9, 2018, I traveled to Lynn, Massachusetts. There is a call box located on the exterior of the building. When I entered the number for , the name "Walshe" was displayed on the screen. is located on the second floor of the building. It is a corner unit facing both Essex Street and Washington Street. I personally observed Walshe enter this unit.

43. A request was made to eBay for the records relating to the seller: ancili2012. This seller was identified as Knipp. As of September 10, 2016, Knipp listed her shipping address with eBay as the Residence.

44. A search of the Suffolk County Registry of Deeds revealed several records for 225 Beacon Street, Boston, Massachusetts. One of these records indicated that this residence was owned by Walshe's mother until March 21, 2017, at which time she sold it to a seemingly unrelated individual. Even though Walshe has used this address previously, such as on his RMV listing or as the original location for his meeting with Witness 1, because his mother no longer owns this property, I believe that Walshe could not be living there or storing anything there.

45. Based on the above, I have probable cause to believe that Walshe is currently residing at the Residence and evidence, fruits and instrumentalities of the Target Offenses may be located in the Residence. In particular, I believe that Walshe may be storing the actual Paintings, additional copies of the Paintings, or copies or originals of the Keith Haring prints there, as well as the

computer equipment and records described in Attachment E.

SEIZURE OF COMPUTER EQUIPMENT AND DATA

46. 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 email, 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. I am also aware that the Consumer Electronics Association estimated that in 2010, 86 percent of all U.S. households owned at least one computer.

a. From my training and experience, I am aware that personal computer systems are generally capable of creating, receiving, and otherwise processing computer files generated at or to be used at a business, such as e-mail, word-processing documents, photographs, and spreadsheets.

b. From my training, experience, and information provided to me by other agents, I am aware that individuals commonly store records of the type described in Attachment E in computer hardware, computer software, smartphones, and storage media.

c. Based on my training, experience, and information provided by other law enforcement officers, I know that many smartphones, including Walshe's Blackberry (which is included in the definition of "computer hardware" in Attachment E) can now function essentially as small computers. Smartphones have capabilities that include serving as a wireless telephone, digital camera, portable media player, GPS navigation device, sending and receiving text messages and e-mails, and storing a vast range and amount of electronic data. Examining data

stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

d. As described above, Walshe sent and received numerous emails with Victim 1. In addition, Walshe advertised the Paintings for sale on eBay, and those advertisements would have required the use of computer equipment, including cell phones. In addition, Walshe exchanged text messages and communicated by cell phone with Victim 1. I believe that Walshe likely stores such equipment in the Residence, especially because he does not have a job, as far as I am aware.

47. 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.

48. 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.

49. 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 E 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.

PROBABLE CAUSE TO BELIEVE THAT THE EMAIL ACCOUNTS TO BE SEARCHED CONTAIN EVIDENCE, FRUITS, AND INSTRUMENTALITIES

50. As detailed above, I have reviewed emails which demonstrate that Walshe communicated

with Victim 1 and Witness 1 using the accounts brianwalshe71916@gmail.com and brw@tensailconsulting.com (hereinafter, the "Accounts"). I therefore have probable cause to believe that the Accounts may contain the emails described above and other evidence, fruits and instrumentalities of the Target Offenses.

51. According to whois.com, e-mail addresses listing the domains gmail.com (i.e., xxx@gmail.com) are hosted by Google, Inc. "Google," an Internet Service Provider and electronic communications service located in the Northern District of California. Accordingly, I have probable cause to believe that the account brianwalshe71916@gmail.com and relevant data are maintained by Google, which, government databases indicate, accepts service of process at:

1600 Amphitheatre Parkway, Mountain View, California (CA) 94043, or through their Law Enforcement Request System, as described in Attachment B.

52. According to whois.com, e-mail addresses listing the domain tensailconsulting.com (i.e., xxx@tensailconsulting.com) are hosted by GoDaddy.com, LLC "GoDaddy," an Internet Service Provider and electronic communications service located in the District of Arizona. Accordingly, I have probable cause to believe that the account brw@tensailconsulting.com and relevant data are maintained by GoDaddy, which, government databases indicate, accepts service of process at:

14455 N. Hayden Road, Suite 219 Scottsdale, Arizona 85260 and by facsimile at (480) 624-2546, as described in Attachment C.

53. On March 30, 2018, I sent Google a letter requesting that the company preserve records associates with the Accounts for ninety days pursuant to 18 United States Code § 2703(f).

TECHNICAL BACKGROUND REGARDING THE EMAIL ACCOUNTS

54. In my training and experience and through discussions with other agents, I have learned

that e-mail hosting companies, such as Google and GoDaddy, maintain computer servers connected to the Internet. Their customers use those computers to send e-mail on the Internet.

55. Customers can access their accounts on the company's e-mail servers from any computer connected to the Internet.

56. An e-mail sent to a Google subscriber is stored in the subscriber's "mail box" on the company's servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Google's servers indefinitely. In addition, Google has storage capacity that allows customers to store opened incoming mail and sent mail indefinitely if they choose, subject to a maximum size limit.

57. E-mail providers also typically maintain electronic records relating to their customers. These records include account application information, account access information, and e-mail transaction information.

58. Google can also provide the following additional information associated with a subscriber's account: address books; "buddy" or friend lists; photos, files, data, documents or other information; and World-Wide Web profiles or homepages. I believe that GoDaddy likely maintains similar information.

LEGAL AUTHORITY

59. The government may obtain both electronic communications and subscriber information from an e-mail provider by obtaining a search warrant. 18 U.S.C. §§ 2703(a), 2703(c)(1)(A).

60. Any court with jurisdiction over the offense under investigation may issue a search warrant under 18 U.S.C. § 2703(a), regardless of the location of the website hosting company or e-mail provider whose information will be searched. 18 U.S.C. § 2703(b)(1)(A). Furthermore, unlike other search warrants, § 2703 warrants do not require an officer to be present for service

or execution of the search warrant. 18 U.S.C. § 2703(g).

61. If the government obtains a search warrant, there is no requirement that either the government or the provider give notice to the subscriber. 18 U.S.C. §§ 2703(b)(1)(A), 2703(c)(3).

62. This application seeks a warrant to search all responsive records and information under the control of Google and GoDaddy, providers subject to the jurisdiction of this court, regardless of where they have chosen to store such information. Pursuant to 18 U.S.C. § 2713, the government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Google or GoDaddy's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.

FOURTEEN-DAY RULE FOR EXECUTION OF EMAIL SEARCH WARRANTS

63. Federal Rules of Criminal Procedure 41(e)(2)(A) & (B) direct the United States to execute a search warrant for electronic evidence within 14 days of the warrant's issuance. If the Court issues these warrants, the United States will execute it not by entering the premises of Google or GoDaddy, as with a conventional warrant, but rather by serving a copy of the warrant on the company and awaiting its production of the requested data. This practice is approved in 18 U.S.C. § 2703(g), and it is generally a prudent one because it minimizes the government's intrusion onto Internet companies' physical premises and the resulting disruption of their business practices.

64. Based on my training and experience and that of other law enforcement, I understand that e-mail providers sometimes produce data in response to a search warrant outside the 14-day

period set forth in Rule 41 for execution of a warrant. I also understand that e-mail providers sometimes produce data that was created or received after this 14-day deadline ("late-created data").

65. The United States does not ask for this extra data or participate in its production.

66. Should Google or GoDaddy produce late-created data in response to this warrant, that was created by the account holder, such as email or other content, the government will avoid reviewing such content and will seek a follow-up search warrant from this court. However, with respect to late-created data that was created by Google or GoDaddy, including subscriber, IP address, logging, and other transactional data, which could also be obtained by grand jury subpoena or an order under 18 U.S.C. § 2703(d) (neither of which contains a 14-day time limit), I seek permission to review such data.

67. For these reasons, I request that the Court approve the procedures in Attachments F and G, which set forth these limitations.

CONCLUSION

68. Based on the information described above, I probably cause to believe that Brian Walshe has violated 18 United States Code §§ 1343, 2314, and 2315.

69. Based on the information described above, I also have probable cause to believe that the Premises, Accounts, and Persons of Walshe and Knipp, as described in Attachments A, B, C, and D, contain evidence, fruits, and instrumentalities of those crimes, as described in Attachments E, F, G, and H.

70. The procedures for executing those warrants are set out in Attachments E, F, G, and H to the search warrants.

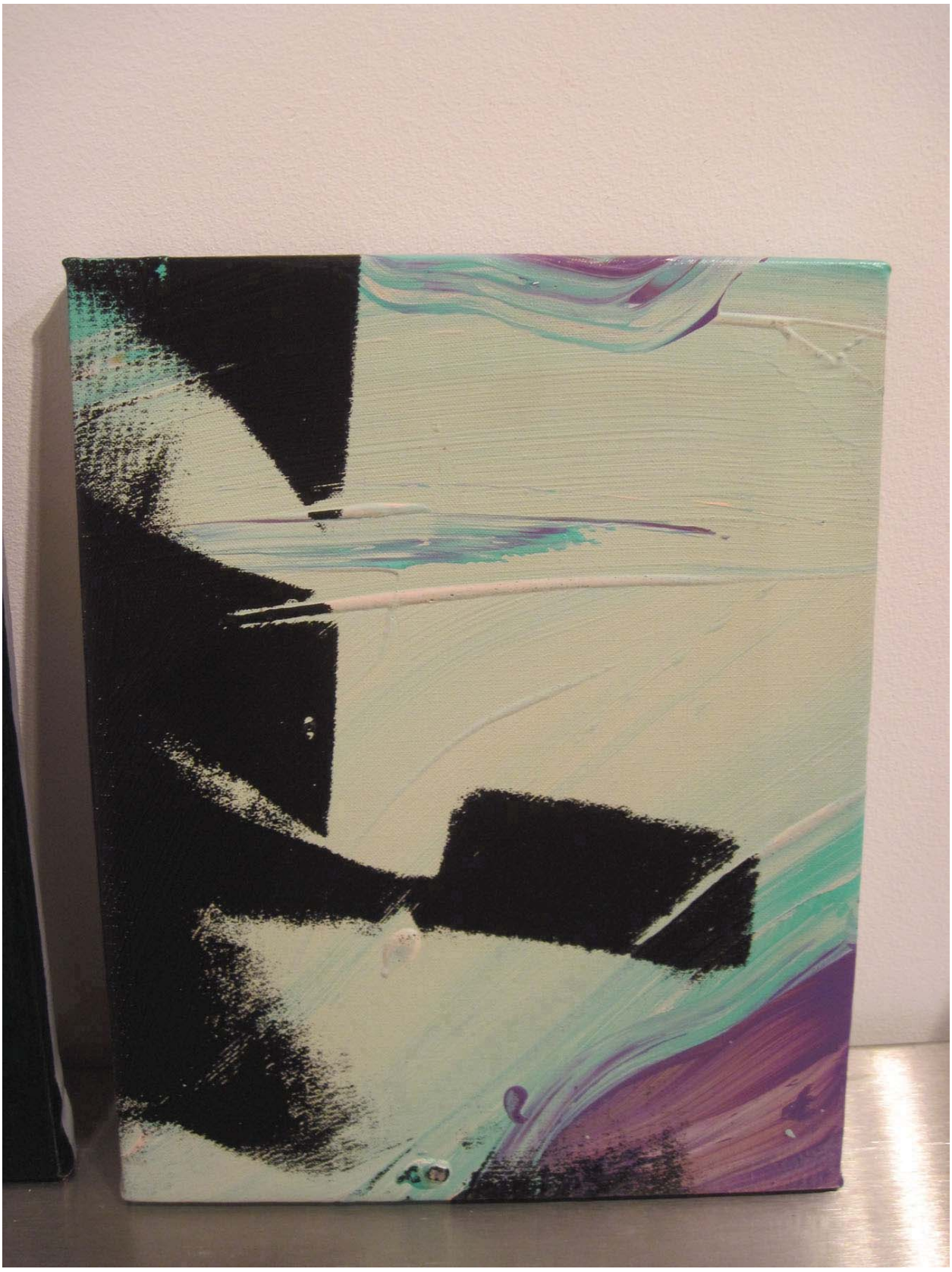
Respectfully submitted,

Kristin D. Koch
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on May 8, 2018.

JENNIFER C. BOAL
UNITED STATES MAGISTRATE JUDGE

APPENDIX



ATTACHMENT A

DESCRIPTION OF THE RESIDENCE TO BE SEARCHED

The premises to be searched are located at , Lynn, Massachusetts. The building at Lynn, Massachusetts is a four story red brick multi-unit condominium building. One the front of the building are the words and above the front door is the number . is located on the second floor of the building adjacent to the door for the stairwell. It is a corner unit facing both

According to publicly available real estate websites is a two bedroom, one bathroom condominium that is approximately 1191 square feet. The number is on a placard outside of the unit.

ATTACHMENT B

DESCRIPTION OF THE GOOGLE ACCOUNT TO BE SEARCHED

The premises to be searched and seized are (1) the e-mail account identified as brianwalshe71916@gmail.com (2) other user-generated data stored with those accounts, and (3) associated subscriber, transactional, user connection information associated with the accounts, as described further in Attachment F. This information is maintained by Google, which accepts service of process at:

1600 Amphitheatre Parkway, Mountain View, California (CA) 94043 or through their Law Enforcement Request System at https://lers.google.com.

ATTACHMENT C

DESCRIPTION OF THE GODADDY ACCOUNT TO BE SEARCHED

The premises to be searched and seized are (1) the e-mail account identified as brw@tensailconsulting.com (2) other user-generated data stored with those accounts, and (3) associated subscriber, transactional, user connection information associated with the accounts, as described further in Attachment G. This information is maintained by GoDaddy, which accepts service of process at:

14455 N. Hayden Road, Suite 219 Scottsdale, Arizona 85260 or by facsimile at (480) 624-2546.

ATTACHMENT D

DESCRIPTION OF THE PERSONS TO BE SEARCHED

Brian R. Walshe, born 1975, social security number -6970, is a 6'2" tall white male with a medium build, medium length brown hair and brown eyes and is depicted below.

Ana Knipp a/k/a Ana Walshe is a 5'2" tall white female and is depicted below.

ATTACHMENT E

ITEMS TO BE SEIZED FROM THE RESIDENCE

I. All records, in whatever form, from January 1, 2011 to the present, and tangible objects that constitute evidence, fruits, or instrumentalities of violations of 18 U.S.C. §§ 1343, 2314, 2315, including:

A. Records and tangible objects pertaining to the following people, entities, physical addresses, telephone numbers, bank accounts, websites, e-mail addresses, IP addresses: Brian Walshe, Ana Walshe, aka Ana Knipp,

Gogosian Gallery Martin Lawrence Gallery,

Christie's, Sotheby's, Gallery Valentine,

and Bellagio Gallery of Fine Art;

B. Records and tangible objects, including the art work itself (and any transparencies and duplicates thereof) and any photographs thereof, where applicable, pertaining to the following topics:

1. Brian Walshe,
2. Ana Walshe, aka Ana Knipp,
3.
4.
5.
6. Christie's, Sotheby's, and art auctions,
7. Gogosian Gallery, Martin Lawrence Gallery, Gallery Valentine, and art galleries,

8. Andy Warhol, including Andy Warhol Shadow Paintings and Dollar Sign,

9. Keith Haring, including any Keith Haring prints

10. Chinese porcelain,

11. Art sales,

12. eBay,

13. DocuSign

14. international travel and the purchase of airline tickets;

C. Records and tangible objects pertaining to the payment, receipt, transfer, or storage of money or other things of value by Walshe, Knipp, or any one of the names listed above, including, without limitation:

1. Bank, credit union, investment, money transfer, and other financial accounts;

2. Credit and debit card accounts;

3. Tax statements and returns;

4. Business or personal expenses;

5. Income, whether from wages or investments;

6. Loans;

D. Records and tangible objects, including the passport or other travel documents, pertaining to the travel or whereabouts of Walshe between January 2011 and December 2016;

E. Records and tangible objects pertaining to the existence, identity, and travel of any co-conspirators, as well as any co-conspirators' acts taken in

furtherance of the crimes listed above;

F. Records and tangible objects, including paint, paintbrushes, canvasses, frames, and other painting supplies, pertaining to the production of art work;

G. Records and tangible objects pertaining to safes, safe deposit boxes, storage units, including keys;

H. Records and tangible objects pertaining to the transportation, receipt, or shipping of art work;

I. For any computer hardware, computer software, mobile phones, or storage media called for by this warrant or that might contain things otherwise called for by this warrant ("the computer equipment"):

1. evidence of who used, owned, or controlled the computer equipment;

2. evidence of the presence or absence of malicious software that would allow others to control the items, and evidence of the presence or absence of security software designed to detect malicious software;

3. evidence of the attachment of other computer hardware or storage media;

4. evidence of counter-forensic programs and associated data that are designed to eliminate data;

5. evidence of when the computer equipment was used;

6. passwords, encryption keys, and other access devices that may be

necessary to access the computer equipment;

7. records and tangible objects pertaining to accounts held with companies providing Internet access or remote; and

J. Records and tangible objects relating to the ownership, occupancy, or use of the premises to be searched (such as utility bills, phone bills, rent payments, mortgage payments, photographs, insurance documentation, receipts and check registers).

II. All computer hardware, computer software, and storage media. Off-site searching of these items shall be limited to searching for the items described in paragraph I.

DEFINITIONS

For the purpose of this warrant:

A. “Computer equipment” means any computer hardware, computer software, mobile phone, storage media, and data.

B. “Computer hardware" means any electronic device capable of data processing (such as a computer, smartphone, mobile phone, or wireless communication device); any device capable of capturing digital images, including a digital camera or cell phone camera; any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).

C. "Computer software" means any program, program code, information or

data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.

D. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, or memory card).

E. "Data" means all information stored on storage media of any form in any storage format and for any purpose.

F. "A record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.

RETURN OF SEIZED COMPUTER EQUIPMENT

If the owner of the seized computer equipment requests that it be returned, the government will attempt to do so, under the terms set forth below. If, after inspecting the seized computer equipment, the government determines that some or all of this equipment does not contain contraband or the passwords, account information, or personally-identifying information of victims, and the original is no longer necessary to retrieve and preserve as evidence, fruits or instrumentalities of a crime, the equipment will be returned within a reasonable time, if the party seeking return will stipulate to a forensic copy's authenticity (but not necessarily relevancy or admissibility) for evidentiary purposes.

If computer equipment cannot be returned, agents will make available to the computer system's owner, within a reasonable time period after the execution of the warrant, copies of files

that do not contain or constitute contraband; passwords, account information, or personally-identifying information of victims; or the fruits or instrumentalities of crime.

For purposes of authentication at trial, the Government is authorized to retain a digital copy of all computer equipment seized pursuant to this warrant for as long as is necessary for authentication purposes.

ATTACHMENT F

ITEMS TO BE SEIZED FROM THE GOOGLE ACCOUNT

I. Search Procedure

A. Within fourteen days of the search warrant's issue, the warrant will be served on Google personnel, who will identify the accounts and files to be searched, as described in Section II below.

B. Google will then create an exact electronic duplicate of these accounts and files ("the account duplicate").

C. Google will provide the account duplicate to law enforcement personnel.

D. Law enforcement personnel will then search the account duplicate for the records and data to be seized, which are described in Section III below.

E. Law enforcement personnel will avoid reviewing any late-created data that was created by or received by the account-holder(s), such as e-mail, absent a follow-up warrant. If Google provided data that it created after fourteen days from the warrant's issue ("late-created data"), law enforcement personnel may view all late-created data that was created by Google, including subscriber, IP address, logging, and other transactional data, without a further order of the Court

II. Accounts and Files to Be Copied by Google Personnel

A. All data files associated with brianwalshe71916@gmail.com, for the time period January 1, 2011 to present, including:

1. The contents of all e-mail, whether draft, deleted, sent, or received;

2. The contents of all text or instant messages;

3. The contents of all electronic data files, whether word-processing, spreadsheet, image, video, or any other content;

4. The contents of all calendar data;

5. Lists of friends, buddies, contacts, or other subscribers;

6. Records pertaining to communications between Google and any person regarding these accounts and any e-mail accounts associated with those addresses, including, without limitation, contacts with support services and records of actions taken.

B. All subscriber and transactional records for brianwalshe71916@gmail.com e-mail accounts and any associated e-mail accounts, for the time period January 2011 to present, including:

1. Subscriber information for these and any associated e-mail accounts:

a. Name(s) and account identifiers;

b. Address(es);

c. Records of session times and durations;

d. Length of service (including start date) and types of service utilized;

e. Telephone instrument number of other subscriber number or identity, including any temporary assigned network address;

f. The means and source of payment for such service (including any credit card or bank account number); and

g. The Internet Protocol address used by the subscriber to register the account or otherwise initiate service.

2. User connection logs for any connections to or from these and any associated e-mail accounts, for the time period January 1, 2011 to present, including:

a. Connection time and date;

b. Disconnect time and date;

c. The IP address that was used when the user connected to the service;

d. Source and destination of any e-mail messages sent from or received by the account, and the date, time, and length of the message; and

e. Any address to which e-mail was or is to be forwarded from the account or e-mail address.

III. Records and Data to be Searched and Seized by Law Enforcement Personnel

A. For the period January 1, 2011 to present, evidence, fruits, or instrumentalities of violations of Title 18, U.S.C. §§ 1343 (Wire fraud), 2314 (transportation of stolen goods), and 2315 (sale or receipt of stolen goods), including records relating to:

1. All communications between or among Brian Walshe, Ana Walshe, aka Ana Knipp, Gogosian Gallery, Martin Lawrence Gallery, Bellagio Gallery of Fine Art, Christie's, Sotheby's, Gallery Valentine,

2. All communications pertaining to Brian Walshe, Ana Walshe, aka Ana Knipp Christie's, Sotheby's, Gogosian Galley, Martin Lawrence Gallery, Bellagio Gallery of Fine Art, Gallery Valentine, Andy Warhol, Keith Haring, art auctions, art sales, eBay, international travel, purchase of airline tickets;

3. The identity of the person or persons who have owned or operated the brianwalshe71916@gmail.com e-mail accounts or any associated e-mail accounts;

4. The contents of all electronic data files, whether word-processing, spreadsheet, image, video, or any other content, pertaining Brian Walshe, Ana Walshe, aka Ana Knipp Christie's, Sotheby's, Gogosian Galley, Martin Lawrence Gallery, Bellagio Gallery of Fine Art, Gallery Valentine Andy Warhol, Keith Haring, art auctions, art sales, eBay, international travel, purchase of airline tickets;

5. The contents of all calendar data regarding Walshe;

6. The existence and identity of any co-conspirators;

7. The travel or whereabouts of the person or persons who have owned or operated the brianwalshe71916@gmail.com e-mail accounts or any associated e-mail accounts;

8. The identity, location, and ownership of any computers used to access these e-mail accounts;

9. Other e-mail or Internet accounts providing Internet access or remote data storage;

10. The existence or location of physical media storing electronic data, such as hard drives, CD- or DVD-ROMs, or thumb drives; and

11. The existence or location of paper print-outs of any data from any of the above.

B. All of the subscriber, transactional, and logging records described in Section II(B).

ATTACHMENT G

ITEMS TO BE SEIZED FROM THE GODADDY ACCOUNT

I. Search Procedure

A. Within fourteen days of the search warrant's issue, the warrant will be served on GoDaddy personnel, who will identify the accounts and files to be searched, as described in Section II below.

B. GoDaddy will then create an exact electronic duplicate of these accounts and files ("the account duplicate").

C. GoDaddy will provide the account duplicate to law enforcement personnel.

D. Law enforcement personnel will then search the account duplicate for the records and data to be seized, which are described in Section III below.

E. Law enforcement personnel will avoid reviewing any late-created data that was created by or received by the account-holder(s), such as e-mail, absent a follow-up warrant. If GoDaddy provided data that it created after fourteen days from the warrant's issue ("late-created data"), law enforcement personnel may view all late-created data that was created by GoDaddy, including subscriber, IP address, logging, and other transactional data, without a further order of the Court.

II. Accounts and Files to Be Copied by GoDaddy Personnel

A. All data files associated with brw@tensailconsulting.com, for the time period January 1, 2011 to present, including:

1. The contents of all e-mail, whether draft, deleted, sent, or received;

2. The contents of all text or instant messages;

3. The contents of all electronic data files, whether word-processing, spreadsheet, image, video, or any other content;

4. The contents of all calendar data;

5. Lists of friends, buddies, contacts, or other subscribers;

6. Records pertaining to communications between GoDaddy and any person regarding these accounts and any e-mail accounts associated with those addresses, including, without limitation, contacts with support services and records of actions taken.

B. All subscriber and transactional records for brw@tensailconsulting.com e-mail accounts and any associated e-mail accounts, for the time period January 2011 to present, including:

1. Subscriber information for these and any associated e-mail accounts:

a. Name(s) and account identifiers;

b. Address(es);

c. Records of session times and durations;

d. Length of service (including start date) and types of service utilized;

e. Telephone instrument number of other subscriber number or identity, including any temporary assigned network address;

f. The means and source of payment for such service (including any credit card or bank account number); and

g. The Internet Protocol address used by the subscriber to register the account or otherwise initiate service.

2. User connection logs for any connections to or from these and any associated e-mail accounts, for the time period January 1, 2011 to present, including:

a. Connection time and date;

b. Disconnect time and date;

c. The IP address that was used when the user connected to the service;

d. Source and destination of any e-mail messages sent from or received by the account, and the date, time, and length of the message; and

e. Any address to which e-mail was or is to be forwarded from the account or e-mail address.

III. Records and Data to be Searched and Seized by Law Enforcement Personnel

A. For the period January 1, 2011 to present, evidence, fruits, or instrumentalities of violations of Title 18, U.S.C. §§ 1343 (Wire fraud), 2314 (transportation of stolen goods), and 2315 (sale or receipt of stolen goods), including records relating to:

1. All communications between or among Brian Walshe, Ana Walshe, aka Ana Knipp Gogosian Gallery, Martin Lawrence Gallery, Bellagio Gallery of Fine Art, Christie's, Sotheby's, Gallery Valentine

2. All communications pertaining to Brian Walshe, Ana Walshe, aka Ana Knipp Christie's, Sotheby's, Gogosian Galley, Martin Lawrence Gallery, Bellagio Gallery of Fine Art, Gallery Valentine, Andy Warhol, Keith Haring, art auctions, art sales, eBay, international travel, purchase of airline tickets;

3. The identity of the person or persons who have owned or operated the brw@tensailconsulting.com e-mail accounts or any associated e-mail accounts;

4. The contents of all electronic data files, whether word-processing, spreadsheet, image, video, or any other content, pertaining to Brian Walshe, Ana Walshe, aka Ana Knipp, Christie's, Sotheby's, Gogosian Galley, Martin Lawrence Gallery, Bellagio Gallery of Fine Art, Gallery Valentine, Andy Warhol, Keith Haring, art auctions, art sales, eBay, international travel, purchase of airline tickets;

5. The contents of all calendar data regarding Walshe;

6. The existence and identity of any co-conspirators;

7. The travel or whereabouts of the person or persons who have owned or operated the brw@tensailconsulting.com e-mail accounts or any associated e-mail accounts;

8. The identity, location, and ownership of any computers used to access these e-mail accounts;

9. Other e-mail or Internet accounts providing Internet access or remote data storage;

10. The existence or location of physical media storing electronic data, such as hard drives, CD- or DVD-ROMs, or thumb drives; and

11. The existence or location of paper print-outs of any data from any of the above.

B. All of the subscriber, transactional, and logging records described in Section II(B).

ATTACHMENT H

ITEMS TO BE SEIZED FROM THE PERSONS OF WALSHE AND KNIPP

Major case fingerprints which record all of the friction ridge surfaces of the hand and palm; and a DNA sample in the form of a mouth swab.