# UNITED STATES DISTRICT COURT

for the

District of Columbia

In the Matter of the Search of
*(Briefly describe the property to be searched or identify the person by name and address)*
DELL OPTIPLEX 990 DESKTOP, SERVICE # 1B83KQ1, EXPRESS SERVICE CODE 2855514025, STORED AT PREMISES CONTROLLED BY THE ARMED FORCES FOUNDATION LOCATED AT 16 NORTH CAROLINA AVE, SE, WASHINGTON, DC 20003

Case No.

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Dell Optiplex 990 Desktop, Service # 1B83KQ1, Express Service Code 2855514025, located at 16 North Carolina Ave, SE, Washington, DC (as further described in the attached affidavit, incorporated fully herein, including Attachment A).

located in the _____ District of Columbia, there is now concealed *(identify the person or describe the property to be seized)*:

all records contained in Dell Optiplex 990 Desktop, Service # 1B83KQ1, Express Service Code 2855514025, relating to violations of 18 U.S.C. § 1343 (as further described in the attached affidavit in suport of search warrant, incorporated fully herein, including Attachment B).

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

| *Code Section* | *Offense Description* |
|---|---|
| 18 U.S.C. § 1343 | Wire Fraud |

The application is based on these facts:

SEE ATTACHED AFFIDAVIT HEREIN INCORPORATED BY REFERENCE AS IF FULLY RESTATED HEREIN.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

*Applicant's signature*

Timothy D. Lynch, Special Agent, FBI
*Printed name and title*

Sworn to before me and signed in my presence.

Date: 09/18/2015

*Judge's signature*

City and state: Washington, D.C.

G. Michael Harvey, U.S. Magistrate Judge
*Printed name and title*

# ATTACHMENT A

## Property to Be Searched

This warrant applies to the following four (4) computers:

1. Dell Optiplex 990 Desktop, Service # 1B83KQ1,
   Express Service Code 2855514025
2. Dell Optiplex 990 Desktop, Service # 1B82KQ1,
   Express Service Code 2855467369
3. Dell Latitude E6500 Laptop, Service # BCZ2VK1,
   Express Service Code 24729120577
4. Dell Inspiron N5010 Laptop, Service # DJT61N1,
   Express Service Code 29496018637

stored at premises controlled by the **Armed Forces Foundation.**, a non-profit organization that accepts service of legal process at 16 North Carolina Avenue SE, Washington, DC 20003.

**ATTACHMENT B**

All records relating to violations of Title 18, United States Code, 1343 (wire fraud), pertaining to the following matters:

a. Records or information relating to a scheme to defraud or theft from AFF;

b. Records related to any AFF's bank or investment accounts;

c. Records related to FDS's bank or investment accounts;

d. Records relating to the AFF and FDS QuickBooks accounting program;

e. Records relating to the AFF and FDS American Express and any other revolving credit accounts;

f. Any emails or records relating to a memo dated April 30, 2008, purporting to authorize "compensation" payments to Patricia Driscoll;

g. Any other emails, word documents, or spreadsheets providing justification for payments made from the AFF to Patricia Driscoll or concealment of such payments;

h. Any billing records relating to services provided to the AFF or Patricia Driscoll by the law firms of:

1. Parkowski, Guerke, and Swayze;
2. Warfield, Darrah, and Erdmann;
3. Dycio and Biggs;

i. Files related to Driscoll's filing of a theft report with the Washington, D.C., Metropolitan Police Department on June 7, 2015.

j. Files related to any purchases from FLIR Systems;

k. Any Deleted files relating to the above list.

# ATTACHMENT C

## FILTER TEAM PRACTICES AND PROCEDURES

**Filter team membership**

- An AUSA from the United States Attorney's Office for the District of Columbia who is not part of the case prosecution/investigation team, and will never be so in the future.
- A federal agent(s) who is not part of, or connected in any way to, the case investigation/prosecution team.

**Items to be reviewed by filter team:**

- Emails and email attachments
- Material on the subject computers (two desktop computers and two laptop computers)

**Filter team review procedures**

1. The Filter Team will run search terms against the seized data, designed to identify potentially privileged communications with counsel among the relevant files, and the results of these searches – i.e., the potentially privileged communications with counsel – will be segregated from the remaining data.
2. Only the Filter Team will have access to this information on the government's databases, and the databases will be programmed to deny access to anyone other than a Filter Team member who seeks to view such files.
3. The filter team AUSA will divide all relevant materials into four categories:
    a. Privileged information ("category a");
    b. Potentially privileged information ("category b");
    c. Privileged or potentially privileged information that may fall into the crime-fraud exception of the attorney-client privilege ("category c"); and

d. Non-privileged information ("category d").

4. The filter team AUSA will determine whether any information in category (b) and category (c) falls outside the attorney-client privilege due to waiver, an exception to the privilege, or the like.
5. The filter team AUSA will submit to the Court, under seal, a copy of all items from categories (b), and (c), and seek the Court's final determination concerning whether the submitted materials are protected by attorney-client privilege.
6. The filter team AUSA will forward to the investigation/prosecution team the materials determined to fall in category (d) (non-privileged information).
7. The filter team AUSA will forward to the investigation/prosecution team all materials the Court determines are not protected by attorney-client privilege, or fall into an exception to the privilege.
8. At the conclusion of this process, the Filter Team will return all privileged materials to counsel for the subscriber of the Target Account.
9. At the conclusion of this process, the Filter Team will permanently delete all privileged materials from any databases, and will destroy any copies.

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

| | |
|---|---|
| IN THE MATTER OF THE SEARCH OF DELL OPTIPLEX 990 DESKTOP, SERVICE # 1B83KQ1, EXPRESS SERVICE CODE 2855514025, STORED AT PREMISES CONTROLLED BY THE ARMED FORCES FOUNDATION LOCATED AT 16 NORTH CAROLINA AVE, SE, WASHINGTON, DC 20003 | Case No. _____<br><br>**Filed Under Seal** |

AFFIDAVIT IN SUPPORT OF
**AN APPLICATION FOR A SEARCH WARRANT**

I, Timothy D. Lynch, being first duly sworn, state:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for two desktop computers and two laptop computers ("subject computers"), known to have been utilized by investigative subject Patricia P. Driscoll while she was employed as the President of the Armed Forces Foundation ("AFF"), a non-profit organization located at 16 North Carolina Avenue SE, Washington, DC 20003. The subject computers are currently in the possession of the AFF. The items to be searched are described in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require the AFF to disclose to the government copies of information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate items described in Section II of Attachment B.

2. I have been employed as a Special Agent (SA) with the Federal Bureau of Investigation (FBI) for 11 years, conducting numerous white collar investigations

involving financial institutions fraud, wire fraud, mail fraud, and money laundering. I am currently assigned to a squad at the FBI's Washington Field Office (WFO) focused on fraud occurring at nonprofit organizations.

3. The information contained in this affidavit has been provided to me by witnesses, other agents and law enforcement officers, records received via grand jury subpoena, and public source information. This affidavit is intended to demonstrate there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this investigation.

## JURISDICTION

4. This Court has jurisdiction to issue the requested warrant because it is a "court of competent jurisdiction" as defined by 18 U.S.C. §§ 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A) and (c)(1)(A). Specifically the Court is a "district court of the United States that has jurisdiction over the offense being investigated." 18 U.S.C.§2711(3)(A)(i).

## RELEVANT STATUTE

5. *Wire Fraud*. Title 18, United States Code, Section 1343 provides in relevant part that, "[w]hoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice" shall be guilty of a federal offense.

## SUMMARY

6. I make this affidavit in support of a joint investigation by the FBI and IRS, for four (4) computers currently in the possession of the Armed Forces Foundation. I seek authority to search the computers listed in Attachment A for items which constitute evidence, fruits, and instrumentalities of violations of transmitting in interstate commerce any communication containing any information regarding a conspiracy to commit criminal violations of Title 18 U.S.C. Section 1343.

7. Based on my training, experience, and the facts set forth in this affidavit, I submit there is probable cause to believe that Patricia P. Driscoll has used the subject computers in furtherance of her theft of funds legally belonging to the Armed Forces Foundation ("AFF"), an IRS tax-exempt 501(c)(3) charitable institution. As set forth herein, I submit there is probable cause to believe that a violation of Title 18, United States Code, 1343 (Fraud by Wire), has occurred and that there is probable cause to search the items described in Attachment A for evidence of these crimes further described in Attachment B.

## BACKGROUND OF ENTITIES

8. The Armed Forces Foundation ("AFF") is a 501(c)(3) non-profit organization, Employer Identification Number (EIN) 75-3070368, located at 16 North Carolina Avenue SE, Washington, DC 20003, office telephone number 202-547-4713. The AFF was incorporated in the District of Columbia on May 16, 2002, but its status was revoked on or about October 9, 2003. The AFF was incorporated in Oklahoma on August 8, 2005, and in North Dakota on August 19, 2005, and appears to remain in good standing in those states.

9. The AFF website, www.armedforcesfoundation.org, identifies its mission as, *"To protect and promote the physical, mental, and emotional wellness of military service members, veterans, and their families."* Through its website and other fundraising events, the AFF actively solicits for donations stating, *"Your donation helps to protect and promote the physical, mental, and emotional wellness of military service members, veterans, and their families."* The website has a "Financial Information" disclaimer stating: *"The Armed Forces Foundation recognize the importance of honoring the trust each donor and sponsor places with us with each contribution. By insuring the financial transparency and accountability through Board of Director oversight, regular audits, and maintaining good standing with nonprofit watchdogs."*
10. The AFF's 2013 IRS Form 990, Return of Organization Exempt from Income (the most recent available), identified Patricia Driscoll as the AFF President and listed her 2013 salary as $171,027. The AFF website previously stated: *"Ms. Driscoll is also the Chief Executive Officer of Frontline Defense Systems LLC (FDS), a company that provides solutions relating to advance technologies and surveillance systems for the intelligence community and the Department of Defense."* On July 15, 2015, the AFF announced Driscoll's resignation as President after 12 years of service.
11. The AFF website, www.armedforcesfoundation.org, contains the following solicitation for donations: *"Your donation helps to protect and promote the physical, mental, and emotional wellness of military service members, veterans, and their families. Through direct assistance programs and awareness and advocacy campaigns, we seek to honor this population for its service, improve military-to-civilian reintegration efforts, and preserve our fighting forces for the future. Please consider a monthly, recurring gift,*

*by joining the Armed Forces Foundation's Honor Guard, so that we can offer predictable and reliable support to the service members and families that we serve year-round."*

12. The AFF solicits for credit card donations through their official website, providing a page for potential donors to submit their name, email address, donation amount, and credit card information. The AFF website also solicits for donations via check, stating: *"Please make checks payable to the Armed Forces Foundation. Letters can be mailed to - Armed Forces Foundation 16 North Carolina Avenue, SE Washington, DC 20003."* A review of bank records showed that numerous check and electronic donations were deposited into an account in the name of the AFF at SunTrust Bank.

13. During this investigation, I recovered documents showing that Patricia Driscoll was directly involved in fundraising on behalf of the AFF. I recovered a document discarded by the AFF with the title, *"Reply to Patricia Driscoll, President, Armed Forces Foundation,"* containing the following text:

*"Dear Patricia,*

*I am thankful for the sacrifices our military families make year round and recognize that the holidays can be especially hard.*

*Thank you for stepping in to help make things just a little easier for these deserving military families around the holiday season.*

*I want to support your mission of financially supporting our heroes and their families, and that's why I've enclosed my tax-deductible contribution to your direct Financial Assistance Program."*

The document offers selections of donations in the amount of $100, $50, $25, $10, or another amount, and contains a space for the donor to write in their credit card information.

14. A second document recovered from the AFF had the title, "*Support Our Troops! Reply Form,"* containing the following text:

*"Dear Patricia,*

*I find our governments negligence toward the brave men and women who have served our great country so valiantly appalling. They deserve much, much better. 120 day wait times and simply ignoring the problems our Veterans come back with, does not make those issues go away.*

*I am a good American and I pay my taxes. But I understand that the VA is not using that money well. And our service members are suffering because of that. I will not let them go without the care they need."*

The document then has the statement, *"And I have included a tax-deductible donation to the AFF for"* a variety of donation options from $24.98 to $1,083. The donation options describe how each amount could be used to help a veteran.

15. Frontline Defense Systems LLC ("FDS"), EIN 32-0036399, is also located at 16 North Carolina Avenue SE, Washington, D.C. 2003, office telephone number 202-547-4225, fax number 202-547-4293. FDS was incorporated in Nevada on October 11, 2002, and the listed officer was Patricia Driscoll.

16. The FDS website, frontlinedefensesystems.com, posts an "Executive Summary" stating: *"Frontline Defense Systems LLC, is a customized services company specifically designed to support the U.S. Govt. and commercial companies engaged in the Global War on Terror. We specialize in customizing "best of breed" off the shelf, hardware and software components to solve specific problems in the intelligence collection and operational support arenas."* The FDS website also identifies 16 North Carolina Avenue SE, Washington, DC 20003, as its mailing address.

17. Frontline Defense Holdings ("FDH") was incorporated in Nevada on August 11, 2005, by Driscoll and a business partner. On November 7, 2005, Driscoll and the partner purchased 16 North Carolina Ave SE, Washington, D.C. 20003, a residential row home serving as the headquarters for both the AFF and FDS. FDH acts as manager for this property. On May 5, 2015, Driscoll's FDH partner sold his half -share of this building to the AFF.

## INITIATION OF INVESTIGATION

18. In May 2015, ESPN published an "Outside the Lines" report on its website, www.espn.go.com, titled: *"Documents: Kurt Busch's ex-girlfriend used veterans charity as bank."* The article alleged that, as President of the AFF, Driscoll used AFF funds for various personal expenses such as:

    a. Over $130,000 used to pay credit card bills for Frontline Defense Systems;

    b. Driscoll's personal federal and state taxes;

    c. $6,315.22 for an infrared camera shipped to Driscoll's residence;

    d. Airfare for Driscoll's then 7 year-old son, identified in this affidavit as "HH";

    e. $15,000 in legal fees relating to a child custody case involving HH;

19. The ESPN article stated that, "*a representative of a former foundation employee contacted the FBI in Washington, alleging that Driscoll broke laws while running the foundation. In addition to providing the FBI documents in support of the claims, the former employee plans to file a federal whistleblower complaint against Driscoll with the Internal Revenue Service, said an attorney with knowledge of the matter. The attorney said the documents, many of which Outside the Lines reviewed, could lead to charges of embezzlement and tax fraud.*"

PROBABLE CAUSE

20. On June 9, 2015, I interviewed the "former foundation employee" discussed in the ESPN article, furthered identified as Cooperative Witness 1 ("CW1"). CW1 worked as an FDS employee from 2005 to the beginning of 2014, performing general clerical work. Driscoll originally hired CW1 strictly as an FDS employee responsible for general clerical matters. As the FDS Chief Executive Officer (CEO), Driscoll interacted with CW1 on a daily basis while also serving as the President of the AFF. CW1 worked upstairs at 16 North Carolina Avenue SE, while AFF operations were run out of the basement.

21. CW1 provided me with a copy of a form that Driscoll allegedly required all AFF employees to sign, stating:

"*You are fully aware that the President of the Armed Forces Foundation, Patricia Driscoll runs and owns Frontline Defense Systems, LLC (FDS). You also have knowledge that AFF pays rent to Frontline Defense Holdings (FDS is half owner of this company). At no time are you allowed to be involved in any Frontline Defense Systems activities. From time to time, you may hear or see things that pertain to the*

*business of FDS because FDS shares office space with the AFF. You are in no way allowed to divulge any information to anyone, including family members. By signing this contract you are recognizing the separation between the two entities and are legally bound to keep yourself from being involved or divulging information about Patricia Driscoll or Frontline Defense Systems, LLC."* The form's salutation was from, *"Patricia Driscoll, President, Armed Forces Foundation,"* and contained a blank line for the AFF employee to sign and date.

22. I have learned from interviews with both CW1 and other former AFF employees that FDS employees regularly performed both AFF and FDS work. For example, Driscoll routinely instructed CW1 to write checks out of the AFF's checking account to cover Driscoll's personal or FDS expenses. CW1 stated that, by 2011, FDS did not have enough funds to cover the FDS payroll. Records obtained from Automated Data Processing ("ADP"), the AFF's payroll company, showed that CW1 began receiving salary payments from the AFF checking account in November 2011. CW1 was aware salary payments were coming from the AFF, despite the fact that CW1 was an FDS employee and their duties had not changed.

23. In addition to the change in income from FDS to AFF, I identified Check #5526 from the AFF SunTrust Checking Account which was made payable to "Frontline Defense Systems" in the amount of $17,500. This check was then deposited into FDS' Wells Fargo checking account. The memo line of the check states "(CW1) June-Oct". CW1 stated that this check was to cover the payroll that FDS paid to CW1 from June through October of 2011. Driscoll told CW1 that, since CW1 did work for AFF during this time, the AFF was responsible for paying CW1's salary.

24. I reviewed the individual grants reported by the AFF on their publicly available IRS Form 990. Individual grants are the monies issued by a nonprofit organization in a calendar year to benefit individuals in need. I then compared the AFF's reported individual grants to Driscoll's reported AFF salary for the same year. From 2009 to 2013, the AFF's grants dropped significantly, while Driscoll's salary steadily increased:

| Year | Individual Grants | Driscoll Salary |
|---|---|---|
| 2009 | $2,187,453 | $104,715 |
| 2010 | $4,556,364 | $141,379 |
| 2011 | $4,470,826 | $144,675 |
| 2012 | $284,602 | $194,010 |
| 2013 | $276,215 | $171,027 |

25. In addition to the salary listed in the above paragraph, it appears that Driscoll paid her personal and FDS bills with AFF funds. I, along with my partner from the IRS – Criminal Investigation ("IRS-CI"), reviewed the FDS monthly American Express credit card statement dated June 13, 2012, and identified the following charges from May 18, 2012:

| *"Description* | *Amount* |
|---|---|
| *US Treasury Tax PA 5LANHAM MD* | *$14,300* |
| *TAX PAYMENTS* | |
| *VALUETTTAXPAYMENT C 5NASHVILLE TN* | *$327.47* |
| *TAX PAYMENTS* | |
| *MARYLAND STATE OF PCANNAPOLIS MD* | *$4,170* |

*OPAYFEE MARYLANDSTTXANNAPOLIS MD $103.83*

*Total: $18,901.30"*

26. In my experience, and in the experience of my IRS-CI partner on this investigation, the above-listed entries on the FDS monthly credit card statement appear to be payments for Driscoll's individual tax liability, quite possibly as a result of an audit on her personal income tax return. The FDS monthly statement dated June 13, 2012, identified the balance at the end of the reporting period as $20,884.73. On July 2, 2012, the AFF SunTrust checking account made a matching electronic Automated Clearing House ("ACH") electronic payment to American Express in the amount of $20,884.73. This appears to be one example of AFF funds paying FDS credit card payments for non-AFF expenses at the direction of Driscoll.

27. Based on other examples of matching amounts from FDS American Express credit card monthly statements and withdrawals from the AFF's checking account, it appears that Driscoll caused the AFF to pay for her personal or FDS expenses with AFF funds on numerous occasions. I and my IRS-CI partner reviewed monthly statements for both the AFF's SunTrust checking account and the FDS's American Express business platinum credit card from January 29, 2012, to July 29, 2013. The following 17 transactions occurred when payments to the FDS credit card matched the exact amount and approximate date of an electronic ACH withdrawal from the AFF checking account. The AFF bank records show all these transactions as payments to American Express:

| FDS Statement Date | AFF ACH Date | Amount |
|---|---|---|
| 01/29/2012 | 02/13/2013 | $4,763.75 |
| 02/27/2012 | 03/05/2012 | $4,630.07 |
| 03/29/2012 | 04/09/2012 | $4,514.77 |
| 05/29/2012 | 05/30/2012 | $2,992.08 |
| 06/28/2012 | 07/02/2012 | $20,884.73 |
| 07/29/2012 | 07/26/2012 | $9,157.64 |
| 08/29/2012 | 09/04/2012 | $5,062.55 |
| 09/28/2012 | 09/26/2012 | $2,829.49 |
| 10/29/2012 | 11/15/2012 | $5,439.05 |
| 12/29/2012 | 01/07/2013 | $11,077.75 |
| 01/29/2013 | 02/01/2013 | $5,721.70 |
| 02/26/2013 | 02/25/2013 | $5,565.01 |
| 03/29/2013 | 03/22/2013 | $3,762.45 |
| 04/28/2013 | 04/30/2013 | $26,476.05 |
| 05/29/2013 | 05/22/2013 | $9,427.46 |
| 06/28/2013 | 06/24/2013 | $4,000.00 |
| 07/29/2013 | 07/23/2013 | $4,602.02 |
| | Total: | $130,906.57 |

28. I reviewed the monthly FDS American Express credit card statements. The individual charges appear overwhelmingly personal in nature, and not connected to either FDS or AFF business. The following is a representative sample of some of the entities charged to the FDS card: Target, Michaels (arts and crafts), iTunes Music Store, Santoro Psychological, Massage Envy, Tiffany and Co., Bed Bath and Beyond, Columbia Dermatology, Candy Et La Chocolat Saint Barthelemy, Black Swan Family Clothing, Bebe Store (women's clothing), BCBG (women's clothing), Little Passports ("A Global Online Adventure for Children"), Golden Haven Hot Springs Resort, Giant Food, Toys 'R Us, Starbucks, and St. Supery Winery.

29. I interviewed the current AFF President, who previously served as the AFF's Chief of Staff under Driscoll. The current AFF President stated definitively that the AFF had no reason to make any of the above purchases. He further advised that the AFF occasionally purchases small gift baskets to thank particular donors. Outside of gift baskets, the AFF does not purchase gifts or luxury items for any reason.

30. From a review of the AFF SunTrust bank statements available to law enforcement for the years 2011 to 2014, it does not appear that either Driscoll or FDS repaid the money that was taken from AFF to pay the FDS credit card bills, in that there are no recorded deposits matching these amounts from either Driscoll or FDS.

31. I have investigated allegations that Driscoll used AFF funds to purchase a piece of technical equipment not related to any AFF business and sold it to a third party for personal profit. I have obtained a SunTrust Bank statement showing a $6,315.22 debit card charge to "1029 Ost-Star-Tron Freeport, PA" on November 1, 2012. Open source research revealed this company to be Optical Systems Technology – Star-Tron, doing business as FLIR Systems. According to their website, FLIR Systems sells Forward Looking Infrared Radiometer (FLIR) cameras and Night Vision Goggles (NVGs).

32. CW1 provided copies of emails in which Driscoll directed CW1 to make the above purchase and have the item shipped to Driscoll's house at 3899 College Avenue, Ellicott City, Maryland. I obtained records from FLIR Systems confirming this purchase and the request that the item be shipped to Driscoll's personal residence. I obtained records from FLIR Systems which contain e-mails between Driscoll, CW1 and a FLIR Systems employee pertaining to this purchase and matching those previously provided to me by CW1.

33. On October 25, 2012, from e-mail address patricia@frontlinedefensesystems.com, Driscoll wrote to CW1, "*Please complete ASAP. Needs to be shipped to my house.*" The e-mail included the signature, "*Patricia Driscoll, CEO, Frontline Defense Systems,*" and "*President & Exec Board Member, Armed Forces Foundation.*" The same day, at Driscoll's direction, CW1 purchased a Recon M24 (640x480) for $6,315.22 using a debit from the AFF SunTrust account. Internet research further identified this item as a Thermal Monocular Night Vision Scope.

34. FLIR Systems records identified the purchaser as Patricia Driscoll, Frontline Defense Systems. The shipping address was identified as Driscoll's residence, 3899 College Avenue Ellicott City, Maryland, while the billing address was listed as 16 North Carolina Avenue SE, Washington, DC.

35. I have learned that Driscoll sold the item, purchased with AFF funds, to a third party who then paid Driscoll personally for the item. A representative for the third party confirmed this transaction took place and then emailed me: a copy of a $10,000 check made out from the third party to Driscoll, a copy of the third party's corporate check ledger stating the check was to "repay Driscoll," and a photograph of the purchased item with a model number matching that provided by CW1 and FLIR Systems.

36. I have discovered that Driscoll used AFF funds to pay for attorneys representing her in non-AFF legal matters. I discovered through Delaware court records that Driscoll was represented by Carolyn N. McNiece of the law firm Parkowski, Guerke, & Swayze P.A., in a legal case against an ex-boyfriend. The case was adjudicated in Delaware Family Court where Driscoll sought and obtained a protective order against the ex-boyfriend. Based on its website, Parkowski, Guerke, & Swayze P.A is based solely in the state of Delaware.

37. In a letter dated September 10, 2015, a representative of the law firm Parkowski, Guerke, & Swayze P.A. notified the U.S. Attorney's Office for the District of Columbia stating, "*Our firm has never represented Armed Forces Foundation and has no billing records related to Armed Forces Foundation.*"

38. I and my IRS partner interviewed the current AFF President and questioned him regarding AFF fees being used to make payments to lawyers. The current AFF President was completely unaware of Carolyn McNiece or her law firm, Parkowski, Guerke, & Swayze P.A., and had never heard of them performing any work for the AFF. A review of bank records revealed the following thirteen (13) debits totaling $65,220 made from the AFF's SunTrust checking account to Parkowski, Guerke, & Swayze, P.A.:

| Date | Amount |
|---|---|
| 11/14/2014 | $2,000 |
| 01/15/2015 | $7,000 |
| 01/16/2015 | $6,000 |
| 02/23/2015 | $6,000 |
| 02/23/2015 | $6,000 |
| 02/24/2015 | $6,000 |
| 02/26/2015 | $4,900 |
| 03/26/2015 | $6,000 |
| 03/27/2015 | $6,000 |
| 03/30/2015 | $1,600 |
| 03/30/2015 | $6,000 |
| 04/14/2015 | $6,000 |
| 05/21/2015 | $1,720 |
| Total: | $65,220 |

39. CW1 provided me with a photograph of two checks from the AFF checkbook. The first is of a partially filled out, voided check number 6233 written to "Warfield Darrah." Voided check number 6233 has the number "15" written as an amount, and the memo section has the hand-written note "Trademark." Check number 6234 is written to "Warfield Darrah" in the amount of $15,000 and the memo section is blank. In the check ledger, a handwritten note on the check stub for check number 6234, reads, "*Trademark for AFF programs Legal advise on BU Run."*

40. Warfield, Darrah, and Erdmann is a law firm based in Severna Park, Maryland. According to its website, Warfield, Darrah, and Erdmann does not practice trademark law. CW1 believes that Driscoll intentionally left out the name "Erdmann" on the above check in order to conceal that this was a payment to her personal attorney.

41. I and my IRS partner interviewed attorney Robert Erdmann. Mr. Erdmann stated that he represents Driscoll in a custody dispute between Driscoll and her ex-husband over their son, HH. Erdmann provided the following two e-mails pertaining to legal fees owed by Driscoll for Erdmann's representation in her child custody matter.

42. On September 18, 2012, Erdmann received an e-mail from his firm's account manager regarding Driscoll. The subject line of the e-mail stated, "*Driscoll – total dues is $17,390.20 - $2,253.43 is interest. Balance w/o interest is $15,136.77."* Erdmann stated that this bill was related solely to his representation of Driscoll for her private child custody matter.

43. On October 2, 2012, Erdmann e-mailed the following to Driscoll's e-mail address, patricia@frontlinedefensesystems.com : *"As to the bill with my firm, with interest it is $17,390.20. Without interest it is $15,136.77. I am willing to accept $15,000.00 even and be square with you."* Erdmann has never billed the AFF for any legal work and any money he received would have been for his personal representation of Driscoll regarding her child custody matter. Erdmann stated that Driscoll would have provided her payment information to his law firm's account manager, and that he was unaware she had used AFF funds to pay his firm.

44. I asked the current AFF President if the firm of Warfield, Darrah, and Erdmann, P.C., had ever performed any work for the AFF. The current AFF President stated, "*not that I know of,"* and *"I did not see them do any work for us in that time."* A review of bank records identified the following five (5) debits totaling $22,293.89 charged from the AFF SunTrust checking account to "Warfield and Darrah PC:"

| Date | Amount |
|---|---|
| 03/06/2015 | $5,000 |
| 03/09/2015 | $5,000 |
| 03/12/2015 | $5,000 |
| 03/13/2015 | $5,000 |
| 03/16/2015 | $2,293.89 |
| Total: | $22,293.89 |

45. On one occasion, the current AFF President received an envelope at the AFF office from the law firm of Dycio and Biggs. From interviews and public records, I discovered that attorney Mark Dycio represented Driscoll in a defamation suit she filed against another individual. The lawsuit was personal in nature and not connected to AFF business. The current AFF President opened the envelope and saw that it was a bill for services. The current AFF President told an AFF administrative employee, *"Do not pay this until you ask Patricia (Driscoll) about it."*

46. The current AFF President later became aware that the AFF had made payments to Dycio and said, *"We (the AFF) didn't hire him."* A review of the AFF's SunTrust checking account shows that the AFF paid the following three (3) checks totaling $42, 362.42 to "Dycio and Biggs, Attorneys at Law:"

| Date | Check Number | Amount |
|---|---|---|
| 12/18/2014 | 7852 | $14,893.97 |
| 03/03/2015 | 7982 | $20,005.49 |
| 04/13/2015 | 8062 | $7,462.96 |
| | Total: | $42,362.42 |

47. I combined the total amount of payments made from the AFF SunTrust checking account to each of the above three identified law firms, identifying what appear to be 21 payments totaling $129,876.31 to three law firms who had no apparent business relationship with the AFF:

| Law Firm | Payments | Total Amount |
|---|---|---|
| Parkowski, Guerke, & Swayze, P.A | 13 | $65,220 |
| Dycio and Biggs, Attorneys at Law | 3 | $42,362.42 |
| Warfield, Darrah, & Erdmann, P.C. | 5 | $22,293.89 |
| Total: | 21 | $129,876.31 |

48. CW1 provided me with the following memo printed on AFF letterhead and dated April 30, 2008:

*"Dear Patricia Driscoll,*

*As part of your executive compensation package, the Armed Forces Foundation will be providing you with the following benefits exclusive of your monthly payroll check: fully paid health insurance (provided by United Health Care), fully paid dental insurance (provided by Delta Dental)*

*Due to the fact that half of your time at Frontline Defense Systems is spent running the Armed Forces Foundation, the following monthly reimbursements will be paid to Frontline Defense Systems:*

*$1,350 for building rent,*

*$742.50 for car payment,*

*$200 for cell phone,*

*$160 for gasoline costs,*

*$125 for office telephone bill,*

*$75 for Frontline Defense Systems' employee cell phone bill*

*$164.50 for Frontline Defense Systems' employee health insurance,*

*$183.00 for utilities"*

49. In 2010, Driscoll told CW1 to create the above memo, but directed CW1 to back-date the memo to 2008. CW1 advised the rent payments in the memo were in addition to the monthly rent Driscoll was already receiving from the AFF and which had been reported on the IRS Form 990. CW1 stated the car and cell phone reimbursements were for Driscoll's personal Land Rover and cell phone. The total of the above amounts is $3,000.

50. The AFF provided me with an email chain dated September 1, 2010, between CW1 and Driscoll. In the email, CW1 provided text from the above memo and asked Driscoll, "*Is this format ok or do you want paragraph form?"* Driscoll replied, "*Perfect! Sign it : ) your name. send it to the mortgage people."*

51. Driscoll instructed CW1 to make all checks payable to FDS in order to further conceal the fact they were for Driscoll's personal expenses. A review of the AFF's SunTrust checking account identified the following ten (10) checks made payable to Frontline Defense Systems in the amount of $3,000, which CW1 identified as being payments directly connected to the above memo:

| Check Date | Check # | Payable To | Amount |
|---|---|---|---|
| 01/28/2011 | 5056 | Frontline Defense Systems | $3,000 |
| 02/24/2011 | 5109 | Frontline Defense Systems | $3,000 |
| 03/30/2011 | 5152 | Frontline Defense Systems | $3,000 |
| 04/29/2011 | 5211 | Frontline Defense Systems | $3,000 |
| 05/26/2011 | 5269 | Frontline Defense Systems | $3,000 |
| 06/28/2011 | 5314 | Frontline Defense Systems | $3,000 |

| | | | |
|---|---|---|---|
| 07/28/2011 | 5385 | Frontline Defense Systems | $3,000 |
| 08/29/2011 | 5420 | Frontline Defense Systems | $3,000 |
| 09/27/2011 | 5469 | Frontline Defense Systems | $3,000 |
| 10/28/2011 | 5520 | Frontline Defense Systems | $3,000 |
| | | Total: | $30,000 |

52. CW1 provided an email chain between Driscoll, an AFF Board Member, and a former AFF accountant. The emails were cut and pasted so only the text and names of the senders were visible. Dates, subjects, and an e-mail address for Driscoll were not visible.

53. The accountant wrote to the AFF Board Member: *"I noticed that the receivable on AFF's books of money owed to it from Frontline which was $9k at 12/31/2010 is still around $9 for 12/31/2011. But the receivable grows quickly to $29,000 by July 2012 due mostly to the payment of FDS' American express credit card bills by AFF. What is that about? AFF should definitely not be paying any of FDS' bills for any reason. What am I missing here?"*

54. In another e-mail, the accountant questioned Driscoll's use of AFF funds to purchase airfare for her son, HH. The accountant wrote: *"Patricia – In looking over the latest version of Quickbooks, I noticed that airfare expenses for (HH) are being written off for 2011 and 2012 as program expenses. This is absolutely forbidden by IRS tax law. I have done extensive research on this topic and the only way to allow the deductions is if the dependent (or spouse) was actually on payroll, actually worked for the company, and actually had bona fide reason for being on the trip. None is the case here with (HH). I have changed all his airfare expenses to the "Due to Board Member PD"*

*account which now shows that you owe AFF money instead of AFF owing you money. Please discontinue having AFF pay (HH's) airfare. If you must use the company credit card, then please reimburse AFF as soon as possible. There are no exceptions to this rule for single parents who travel. There are no court cases or private letter rulings that have allowed this."*

55. Driscoll responded, *"My child care is part of my benefits. It was authorized by the board to allow (HH) to travel with me at the foundations expense after the divorce, so I could continue to do my job. I understand that this may not be a program expense any longer, but it should be."*

56. The accountant then replied: *"The IRS does not care what the board said about you continuing to do your job. The tax law is the tax law. And it must be retroactive back. The Board can give you a raise to cover his travel but the deductions are disallowed for tax purposes. It is not administrative. The only way to fix it is to reclass it to payroll, amend 4th quarter payroll filings and issue you a new W-2. Then it can be deducted for 2011. The same is true for 2012."*

57. Driscoll replied: *"Hugh* (AFF Board Member) *and I discussed this – at what point can (HH) be classified as a volunteer for activities? We have given him little jobs to do when he's been with me. I'm trying to gain a clear understanding."*

58. The accountant then responded: *"Patricia – I was gone on Monday when you wrote and I was tied up all day yesterday until about 4:30. I would not like to discuss tax issues on the phone as I need a paper trail for my files with a non-profit. Non-profits are open to public inspection and I need to be able to substantiate what I have said and done and why so as not to be sued. Given that, there is no hard and fast rule on how*

*much a volunteer has to "volunteer" in order for travel expenses to be taken. If you took an adult with you and paid the airfare and could substantiate a full days worth of volunteering for each day at the event, then there is probably no issue with deducting travel expenses for that volunteer if the IRS or the public comes looking. But the appearance of a 7 year old who is your son, is sometimes flying first class and then saying he is volunteering would not sit with anyone. You have the issue of his being your dependent that causes the disallowance first and foremost. The IRS rule is clear on deducting travel for spouses and dependents. You will not be able to convince anyone he volunteers for 8 hours a day at these events. And I have counted about 10 or more trips for him from Sept 2011 through July 2012. Child labor laws alone would get you for that if he actually volunteered that many hours for that many trips. This is not a case you want to take to Tax Court and attempt to win."*

59. I interviewed the former AFF accountant, who reviewed copies of the above emails and acknowledged they were authentic. The accountant resigned from the AFF in November 2012 in large part because of the above described disputes over QuickBooks irregularities and the recording of travel reimbursements and volunteer hours for Driscoll's son.

60. CW1 identified Driscoll's email accounts as patricia@frontlinedefensesystems.com and pdriscoll@armedforcesfoundation.org. CW1 had numerous email conversations with Driscoll on these accounts in which Driscoll directed CW1 on how to record various AFF expenditures. CW1 advised that a search of the subject email addresses would produce evidence of criminal activity by Driscoll relating to her misuse of AFF funds.

61. CW1 stated that Driscoll is known for bullying and intimidating people who oppose her. Driscoll threatened to accuse CW1 of embezzlement if CW1 ever reported Driscoll's misuse of AFF funds.

62. CW1 testified on behalf of Driscoll's ex-husband during Driscoll's child custody trial in June 2015. Outside the courtroom, CW1 heard Driscoll speaking loudly into her cell phone, apparently so CW1 could hear what Driscoll was saying. CW1 heard Driscoll talking to an unidentified party about getting a warrant and telling them to "come get her." CW1 expressed to me their concern that Driscoll had threatened to falsely accuse CW1 of embezzlement in retaliation for CW1 reporting Driscoll's misuse of AFF funds.

63. I contacted a Detective in the Washington, D.C. Metropolitan Police Department ("MPD") who advised that on June 7, 2015, Driscoll filed a report accusing CW1 of theft of FDS funds and property. Driscoll accused CW1 of check fraud and embezzlement occurring in approximately 2005 through 2007, and of stealing an FDS laptop purchased for CW1's use in 2011. Your affiant notes that Driscoll's MPD report was filed approximately two weeks after the ESPN article was published on May 21, 2015. CW1 has stated that, based on the contents of the article, Driscoll would be fully aware that CW1 was the whistleblower mentioned in the ESPN article.

64. In the MPD report, Driscoll accused CW1 of stealing a Dell Inspiron laptop, service number DJT61N1. Driscoll provided MPD with a receipt for this laptop showing that it was purchased on April 7, 2015, for $787.49. Driscoll included the note, "*Computer owned by FDS, not returned.*" The MPD Detective noted that Driscoll called him repeatedly to ask when MPD planned to arrest and search the home of CW1.

65. On August 26, 2015, an AFF representative identified the following four (4) computers that had been located at 16 North Carolina Avenue SE, Washington, DC 20003:

    a. Dell Optiplex 990 desktop computer, Service # 1B82KQ1, Express Service Code 2855467369, previously used by CW1 and currently used by an AFF clerical employee ("Subject Computer 1")

    b. Dell Optiplex 990 desktop computer, Service #1B83KQ1, Express Service Code 2855514025, located in an office used by Driscoll ("Subject Computer 2")

    c. Dell Latitude E6500 laptop computer, Service # BCZ2VK1, Express Service Code 24729120577, believed to have been previously used by Driscoll ("Subject Computer 3")

    d. Dell Inspiron N5010 laptop computer, Service # DJT61N1, Express Service Code 29496018637, believed to have been previously used by CW1 ("Subject Computer 4")

66. The AFF representative noted that the two laptops above had been found in an office cabinet on the second floor of 16 North Carolina Avenue SE, Washington, DC 20003. The Dell Inspiron N5010 laptop, Service # DJT61N1, is the same laptop that Driscoll reported to MPD as stolen and for which she was attempting to have MPD Detectives obtain search and arrest warrants for CW1.

67. On September 9, 2015, I and my IRS-CI partner met with representatives of AFF. I reviewed records for several AFF payments to FDS that had been recorded in the AFF's QuickBooks general ledger. The representatives stated that these records clearly showed that QuickBooks records reflecting payments to FDS had been back-dated and gave the following three (3) examples. The "claim date" is the date the reported expense was actually incurred. The "date entered" is the date the entry was actually made in QuickBooks. Your affiant notes that the $82,000 payment above was entered the day after the ESPN article was published:

| Description | Amount | Claim Date | Date Entered |
|---|---|---|---|
| Due to FDS | $82,000 | 12/31/2010 | 05/22/2015 |
| Due to FDS | $48,194.59 | 01/01/2013 | 06/09/2013 |
| Due to FDS | $2,000 | 01/01/2014 | 06/10/2015 |

68. The AFF representatives advised that the information relating to the AFF QuickBooks general ledger was recovered from the Dell Optiplex 990 desktop computer, Service # 1B82KQ1, Express Service Code 2855467369 ("Subject Computer 1"). The AFF representatives advised that Subject Computer 1 was previously used by CW1, and was currently being used by an AFF clerical employee. I also obtained the following e-mail showing that Driscoll used AFF computers and suggesting that she logged into these computers under both her account profile and that of CW1.

69. On October 28, 2012, from patricia@frontlinedefensesystems.com, Driscoll e-mailed CW1 about having remote access to QuickBooks in order to prepare information for the former AFF accountant. Driscoll wrote to CW1, *"Let's talk tomorrow so I can log in and look at what we need for (*the AFF accountant). *Make sure I've got remote access for quickbooks."* CW1 replied to Driscoll, *"The only way you can have remote access to QuickBooks is through my laptop :-/ or if you log in as me which means I can't be logged in."* When Driscoll asked why she wouldn't have remote access to QuickBooks, CW1 replied, *"Because QuickBooks is only on my computer."* Driscoll replied, *"Ok, I always need to have access. I have no issue logging in as you. Send me the login name and password. I'll let you know when I log in."* Based on the preceding e-mail, interviews with CW1, and information provided in this affidavit, Driscoll was known to use office computers to send and receive e-mails and to manage the day-to-day affairs of the AFF and FDS.

70. Based on my training and experience, and information acquired from other law enforcement officials with technical expertise, I know the terms described below have the following meanings or characteristics:

    a. "Computer" means "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." See 18 U.S.C. § 1030(e)(1).

b. "Computer hardware" means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

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

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

e. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

f. The Internet is a global network of computers and other electronic devices that communicate with each other using numerous specified protocols. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

g. "Internet Service Providers," or "ISPs," are entities that provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

ISPs can offer a range of options in providing access to the Internet, including via telephone-based dial-up and broadband access via digital subscriber line ("DSL"), cable, dedicated circuits, or satellite. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name - a user name or screen name, an e-mail address, an e-mail mailbox, and a personal password selected by the subscriber. By using a modem, the subscriber can establish communication with an ISP and access the Internet by using his or her account name and password.

h. "Internet Connection" means a connection required for access to the Internet. The connection would be provided by cable, DSL (Digital Subscriber Line), wireless, or satellite systems.

i. A "modem" translates signals for physical transmission to and from the Internet Service Provider, which then sends and receives the information to and from other computers connected to the Internet.

j. A "router" often serves as a wireless access point and directs traffic between computers connected to a network (whether by wire or wirelessly). A router connected to the Internet collects traffic bound for the Internet from its client machines and sends out requests on their behalf. The router also distributes to the relevant client inbound traffic arriving from the Internet. The router is in turn typically connected to a modem.

k. "Domain Name" means the common, easy-to-remember names associated with an Internet Protocol address. For example, a domain name of

"www.usdoj.gov" refers to the Internet Protocol address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first-level, or top-level domains are typically .com for commercial organizations, .gov for the governmental organizations, .org for organizations, and, .edu for educational organizations. Second-level names will further identify the organization, for example usdoj.gov further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government.

l. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

m. "Cache" means the text, image, and graphic files sent to and temporarily stored by a user's computer from a website accessed by the user in order to allow the user speedier access to and interaction with that website.

n. "Secure Hash Algorithm Version 1 hash value" (SHA 1 hash value) is an algorithm that processes digital files, resulting in a 160-bit value that is unique to that file. It is computationally infeasible for two files with different content to have the same SHA 1 hash value. By comparing the hash values of files, it

can be concluded that two files that share the same hash value are identical with a precision that exceeds 99.9999 percent certainty. There is, for example, no known instance of two different child pornographic images or videos having the same SHA1 hash value.

o. "Peer to Peer file sharing" (P2P) is a method of communication available to Internet users through the use of special software, which may be downloaded from the Internet. In general, P2P software allows a user to set up files on a computer to be shared with other computer users running compatible P2P software. A user may obtain files by opening the P2P software on the user's computer and searching for files that are currently being shared on the network. A P2P file transfer is assisted by reference to the IP addresses of computers on the network: an IP address identifies the location of each P2P computer and makes it possible for data to be transferred between computers. One aspect of P2P file sharing is that multiple files may be downloaded at the same time. Another aspect of P2P file sharing is that, when downloading a file, portions of that file may come from multiple other users on the network. However, a tool used by law enforcement restricts the download so that the file is downloaded, in whole or in part, from a single user on the network.

   i. When a user wishes to share a file, the user adds the file to his a shared library files (either by downloading a file from another user or by copying any file into the shared directory), and the file's SHA 1 has value is recorded by the P2P software. The hash value is independent of the file

name; that is, any change in the name of the file will not change the hash value.

ii. Third party software is available to identify the IP address of a P2P computer that is sending a file. Such software monitors and logs Internet and local network traffic.

p. "VPN" means a virtual private network. A VPN extends a private network across public networks like the Internet. It enables a host computer to send and receive data across shared or public networks as if they were an integral part of a private network with all the functionality, security, and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two. The VPN connection across the Internet is technically a wide area network (WAN) link between the sites. From a user perspective, the extended network resources are accessed in the same way as resources available from a private network-hence the name "virtual private network." The communication between two VPN endpoints is encrypted and usually cannot be intercepted by law enforcement.

q. "Encryption" is the process of encoding messages or information in such a way that eavesdroppers or hackers cannot read it but authorized parties can. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, turning it into an unreadable ciphertext. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any adversary that can see the

ciphertext should not be able to determine anything about the original message. An authorized party, however, is able to decode the ciphertext using a decryption algorithm that usually requires a secret decryption key, to which adversaries do not have access.

r. "Malware," short for malicious (or malevolent) software, is software used or programmed by attackers to disrupt computer operations, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. Malware is a general term used to refer to a variety of forms of hostile or intrusive software.

s. A "botnet" is a collection of compromised computers, known as "bots," that autonomously respond to and execute commands issued by the botnet's owner, often for nefarious purposes. Computers become part of a botnet by being infected with malware, which may install itself on a user's computer without the user's knowledge, often by taking advantage of web browser vulnerabilities or by tricking the user into running a Trojan horse program. Once the computer is infected and becomes a bot in the botnet, the malware can listen for, respond to, and execute commands issued by the botnet's owner, for example, to send out spam e-mail or to make connections to a particular server as part of a distributed denial of service, or "DDoS," attack, defined below.

t. "Carding" is an activity in which a perpetrator steals or traffics in stolen credit card information or uses stolen credit card data to buy goods and services.

u. A Distributed Denial of Service, or "DDoS," attack on a server refers to the process of making massive requests to a particular server or domain. The

number of requests to a domain, server, or IP address eventually overwhelms the target, and causes it to stop functioning.

v. Twitter is an online social networking service and microblogging service that enables its users to send and read text-based messages of up to 140 characters, known as "tweets." Tweets are publicly visible by default, but senders can restrict message delivery to just their followers. Users can tweet via the Twitter website, compatible external applications (such as for smartphones), or by Short Message Service (SMS), a text messaging service component of phone, web, or mobile communication systems.

**COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS**

71. As described above and in Attachment B, this application seeks permission to search for records that might be found on the computers, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or on other electronic storage media or digital devices. As used herein, the terms "electronic storage media" and "digital devices" include any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop computers, laptop computers, notebooks, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, USB flash drives, memory cards, optical disks, and magnetic

tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Thus, the warrant applied for would authorize the seizure of electronic storage media and digital devices or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

72. *Probable Cause.* Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit that if electronic storage media or digital devices are found on the computers, there is probable cause to believe that the records and information described in Attachment B will be stored in the electronic storage media and digital devices for at least the following reasons:

    a. Individuals who engage in criminal activity, including wire fraud, use computers to communicate with others and to create document to aid in the execution and concealment of the theft.

    b. Individuals who engage in the foregoing criminal activity, in the event that they change computers, will often "back up" or transfer files from their old computers' hard drives to that of their new computers, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity.

    c. Computer, smart phone, and other digital device files, or remnants of such files, can be recovered months or even years after they have been downloaded onto an electronic storage medium, deleted, or viewed via the Internet. Electronic files downloaded to an electronic storage medium can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered

months or years later using readily-available forensics tools. When a person "deletes" a file on a digital device such as a home computer or a smart phone, the data contained in the file does not actually disappear; rather, that data remains on the electronic storage medium until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the electronic storage medium that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a digital device's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve "residue" of an electronic file from an electronic storage medium depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer, smart phone, or other digital device habits.

73. *Forensic Evidence.* As further described in Attachment B, this application seeks permission to locate not only electronic evidence or information that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence or information that establishes how electronic storage media or digital devices were used, the purpose of their use, who used them, and when. Based on my

knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit there is probable cause to believe that this forensic electronic evidence and information will be on electronic storage media and digital devices in the computers because:

a. Although some of the records called for by this warrant might be found in the form of user-generated documents or records (such as word processing, picture, movie, or texting files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive, flash drive, memory card, or other electronic storage media image as a whole. Digital data on the electronic storage media not currently associated with any file 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 digital data on a hard drive that show what tasks and processes on a computer were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on a hard drive, flash drive, memory card, or memory chip that can reveal information such as online nicknames and

passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times a computer, smart phone, or other digital device was in use. Computer, smart phone, and other digital device file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. 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.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an

accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, electronic storage media and digital device evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on electronic storage media or digital devices is evidence may depend on other information stored on the devices and the application of knowledge about how the devices behave. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how electronic storage media or a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on the device. For example, the presence or absence of counter-forensic programs, anti-virus programs (and associated data), and malware may be relevant to establishing the user's intent and the identity of the user.

74. *Methods To Be Used To Search Digital Devices.* Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I know that:

a. Searching digital devices can be an extremely technical process, often requiring specific expertise, specialized equipment, and substantial amounts of time. There are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical manuals, specialized equipment, and software programs necessary to conduct a thorough search. Digital devices – whether, for example, desktop computers,

mobile devices, or portable storage devices – may be customized with a vast array of software applications, each generating a particular form of information or records and each often requiring unique forensic tools, techniques, and expertise. As a result, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched, and to obtain specialized hardware and software solutions to meet the needs of a particular forensic analysis.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. Recovery of "residue" of electronic files from electronic storage media also requires specialized tools and often substantial time. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. The volume of data stored on many digital devices will typically be so large that it will be extremely impractical to search for data during the physical search of the premises. Smart phones capable of storing 64 gigabytes, flash drives capable of storing 128 gigabytes, and desktop computers capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might contain enormous amounts of data.

d. Further, as discussed above, evidence of how a digital device has been used, the purposes for which it has been used, and who has used it, may be reflected in the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data or software on a digital device is not segregable from the digital device itself. Analysis of the digital device as a whole to demonstrate the absence of particular data or software requires specialized tools and a controlled laboratory environment, and can require substantial time.

e. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. Digital device users may encode communications or files, including substituting innocuous terms for incriminating terms or deliberately misspelling words, thereby thwarting "keyword" search techniques and necessitating continuous modification of keyword terms. Moreover, certain file

formats, like portable document format ("PDF"), do not lend themselves to keyword searches. Some applications for computers, smart phones, and other digital devices, do not store data as searchable text; rather, the data is saved in a proprietary non-text format. Documents printed by a computer, even if the document was never saved to the hard drive, are recoverable by forensic examiners but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband or instrumentalities of a crime.

f. Analyzing the contents of mobile devices can be very labor intensive and also requires special technical skills, equipment, and software.

g. Based on all of the foregoing, I respectfully submit that searching any electronic storage media or digital device for the information, records, or evidence subject to seizure pursuant to this warrant may require a wide array of electronic data analysis techniques and may take weeks or months to complete. Any pre-defined search protocol would only inevitably result in over- or under-inclusive searches, and misdirected time and effort, as forensic examiners

encounter technological and user-created challenges, content, and software applications that cannot be anticipated in advance of the forensic examination of the media or devices. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques reasonably appear to be necessary to locate and retrieve digital information, records, or evidence within the scope of this warrant.

h. In searching for information, records, or evidence, further described in Attachment B, law enforcement personnel executing this search warrant will employ the following procedures: Upon securing the computers, law enforcement personnel will, consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, seize any electronic storage media or digital devices, as defined above, deemed capable of containing the information, records, or evidence described in Attachment B and transport these items to an appropriate law enforcement laboratory or similar facility for review. For all the reasons described above, it would not be feasible to conduct a complete, safe, and appropriate search of any such electronic storage media or digital devices at the PREMISES. The electronic storage media and digital devices, and/or any digital images thereof created by law enforcement in aid of the examination and review, will be examined and reviewed by law enforcement personnel in order to extract and seize the information, records, or evidence described in Attachment B.

1. The analysis of the contents of any seized electronic storage media or digital devices may entail any or all of various forensic techniques as

circumstances warrant. Such techniques may include, but shall not be limited to, surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); conducting a file-by-file review by "opening," reviewing, or reading the images or first few "pages" of such files in order to determine their precise contents; "scanning" storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic "keyword" searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

2. In searching the seized electronic storage media or digital devices, the forensic examiners may examine as much of the contents of the electronic storage media or digital devices as deemed necessary to make a determination as to whether the contents fall within the items to be seized as set forth in Attachment B. In addition, the forensic examiners may search for and attempt to recover "deleted," "hidden," or encrypted data to determine whether the contents fall within the items to be seized as described in Attachment B. Any search techniques or protocols used in searching the contents of the seized electronic storage media or digital devices will be specifically chosen to identify only the specific items to be seized under this warrant.

3. AFF is a functioning entity that conducts legitimate business. The seizure of one of AFF's computers may limit AFF's ability to conduct its legitimate business. As with any search warrant, I expect that this warrant will be executed reasonably. Reasonable execution will likely involve conducting an investigation on the scene of what electronic storage media and digital devices must be seized or copied, and what electronic storage media and digital devices need not be seized or copied. Where appropriate, law enforcement personnel executing the warrant will copy data, rather than physically seize computers, to reduce the extent of disruption. If employees of AFF so request, the agents will, to the extent practicable, attempt to provide the employees with copies of data that may be necessary or important to the continuing function of the AFF's legitimate business. If, after inspecting seized computers, it is determined that some or all of this equipment is no longer necessary to retrieve and preserve evidence, the government will return it.

POTENTIAL PRIVILEGED DOCUMENTS

75. During the time of the scheme, Driscoll was represented by attorneys in connection with her child support matter and her allegations against a former boyfriend. As such, potentially privileged communications and documents may be present among the data described above. As described further in Attachment C, to safeguard any privileges in this investigation, a filter team consisting of an Assistant United States Attorney ("AUSA"), a supervising AUSA and agents ("Filter Team"), all of whom are not involved in the investigation, will be used.

## CONCLUSION

Based on the forgoing, I submit that this affidavit supports probable cause for a warrant to search items described in Attachment A to seize the items described in Attachment B.

Respectfully submitted,

_____
Timothy D. Lynch, Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on September ____, 2015

_____
The Honorable G. Michael Harvey
UNITED STATES MAGISTRATE JUDGE