UNITED STATES DISTRICT COURT

for the
Eastern District of Virginia

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* The premises known as 1560 Wilson Blvd., Suite 550, Arlington, Virginia 22209	)	Case No. 1:12 SW166

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Virginia
(identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before March 19, 2012
(not to exceed 14 days)

☑ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge Theresa C. Buchanan
(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)* ☐ for _____ days *(not to exceed 30)*.

☐ until, the facts justifying, the later specific date of /s/
Theresa Carroll Buchanan
United States Magistrate Judge

Date and time issued: March 5, 2012 3:30 pm
Judge's signature

City and state: Alexandria, Virginia The Honorable Theresa C. Buchanan, Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
1:12 SW166	3-6-2012 9:55 A.M.	On reception desk

Inventory made in the presence of : N/A

Inventory of the property taken and name of any person(s) seized:

See FD-597

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: 4-4-2012

Executing officer's signature

Michael L Wagner FBI SA

Printed name and title

ATTACHMENT A (Wilson Blvd)

DESCRIPTION OF LOCATION TO BE SEARCHED

The premises to be searched (1560 Wilson Boulevard, Suite 550, Arlington, Virginia), is located on the 5th floor of a 25 story office building. Suite 550 is directly across from the elevators on the fifth floor. The entrance is a single, wood frame door with a glass center and windows on both sides. A sign reading Suite 550 is on the wall outside the door. Through the door and windows, a reception area is clearly visible. The interior wall behind the reception desk is painted blue and the words "Symplicity Corporation" are on the wall. The door opens outward and has a proximity touchpad and magnetic lock.

ATTACHMENT B

Particular Things to be Seized

1. All information that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. §§ 2 (aiding and abetting), 371 (conspiracy), and 1030 (fraud and related activity in connection with computers), including a conspiracy to access protected computers without authorization in order to obtain information among Ariel Friedler, Matthew Kelley, Lori Davies, Deborah Sullivan, and other unknown persons, including other Symplicity employees, including information pertaining to the following matters:

   a. Records relating to computer intrusions;

   b. Records relating to the collection and use of confidential business material belonging to Symplicity's competitors;

   c. Records relating to the use of anonymizing systems, including Tor;

   d. Records relating to the design of competitor's systems;

   e. Records relating to the client lists of Symplicity's competitors;

   f. Records of any communications about the violations and conspiracy; and

   g. Any computers or electronic media that were or may have been used as a means to commit the offenses described on the warrant, including downloading confidential materials without authorization in violation of 18 U.S.C. § 1030(a)(2).

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

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

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

c. evidence of the lack of such malicious software;

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

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

f. evidence of the times the COMPUTER was used;

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

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

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

3. Records and things evidencing the use of the Internet Protocol addresses 77.247.181.164 , 173.168.135.160, 76.100.17.95, 71.49.239.7, 74.192.146.36, or Tor to communicate with Maxient, Pave Systems, or other Symplicity competitors including:

a. routers, modems, and network equipment used to connect computers to the Internet;

b. records of Internet Protocol addresses used;

c. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

ATTACHMENT C

TAINT TEAM PROCEDURE

Agents participating in the execution of the search warrants to which this document has been made apart shall use the following procedure to minimize the review of privileged document by the investigative team. A "taint team" comprised of two Agents, one of who is an Agent lawyer, will be present at 1560 Wilson Boulevard, Suite 550, Arlington, Virginia during the execution of the warrant. After the business location has been secured, the taint team will search the office of Ariel Friedler, CEO of Symplicity, first and remove any communications that they deem privileged and seal them so that the rest of the search team does not have access to them. As the search of the business continues, including any forensic review of computers that may occur off-premises, if a member of the search team comes across an item that is potentially a privileged communication, it will be brought to the attention of the taint team who will make a determination.

UNITED STATES DEPARTMENT OF JUSTICE FEDERAL BUREAU OF INVESTIGATION

Receipt for Property Received/Returned/Released/Seized

File # 288A-RH-54964

On (date) 3/6/2012

item(s) listed below were:
- ☐ Received From
- ☐ Returned To
- ☐ Released To
- ☒ Seized

(Name) Ariel Friedler - Symplicity

(Street Address) 1560 Wilson Boulevard, #550

(City) Arlington, Virginia 22209

Description of Item(s):

Black binder w/ CSM documents

Document titled "Questions about Explore"

Steno pad containing codes, instructions to internet sites

Apple Power Mac G4, S/N X81360L5KSK

4 pages encrypted - 2 with "Re: Advocate Web Services printed at top left; 1 page note from Thresa Pepper to Judette

One (1) Seagate Hard Drive, 250GB, S/N 5QE3H4VQ

Two (2) floppy disks

One (1) white 1GB Kingston thumbdrive

One (1) Seagate Hard Drive, 400GB, S/N 3RJ05BWK

Forty-three (43) CD's

Dell VOSTRO 1500, Service Tag H63CCG1, Symplicity # 0000000023

MacMini #0000000129 on desk locked by Matthew Kelly & powercord

1-Data Traveler 112 2GB USB Drive

1-CD-R Labeled Alchemy Database Volume 32

1 - Printout with handwritten note regarding Maxient

2 - 2GB USB Drives with Appsplace logon front

1 - 16GB flash disk

1 - Seagate Momentus 7200.3 Hard Drive S/N 5TH08J8E

Desktop Cooler Master NSN Symplicity Corp: 00140

Dell EV620 Laptop SN: 8TP9KC1 (Friedler) w/ powercord

UNITED STATES DEPARTMENT OF JUSTICE FEDERAL BUREAU OF INVESTIGATION

Receipt for Property Received/Returned/Released/Seized

File # 288A-RH-54964

Lancool desktop computer Model: PC-K1 (C to PC), Western Digital HDD Model WD7500AACS-00D6BY, S/N WCAU47585219, 750GB

One (1) black & silver EMC thumbdrive

DEWF1 is a 160GB HDD containing 80GB EO1 Image (S/N WCAV3E551802)

DEWF2, a 750GB HDD model WD7500AARS-0045B1, SN: WCAV5N572465 containing dd image of 500GB WD HDD from Lancool Desktop - CIO'S office

Dell Inspiron N7010 Laptop S/N 4ZL8SQ1, Symplicity: 00213 w/ powercord

DEWF4 - A WD ITB HD, S/N WMAV50849748, containing a full image of Wolfgang server and partial image of mysqldata server

DEWF3 - A WD ITB HD, Model WD10EADS, S/N WMAVU4052615, with a damaged EXT3 partition and partial images

Received By _____ Received From _____

(signature) _____ (signature) _____

AO 93 (Rev. 12/09) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
The Premises known as 21715 Filigree Court, Ashburn, Virginia aka DC2, cage 2320, racks numbered 0101 and 0103, and cage 2450, racks numbered 0101, 0102, 0103, 0104, 0105, 0106, 0107, 0108, 0109, and 0110.

Case No. 1:12 SW167

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Virginia
(identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before March 19, 2012
(not to exceed 14 days)

☑ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge Theresa C. Buchanan.
(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)* ☐ for _____ days *(not to exceed 30)*.
☐ until, the facts justifying, the later specific date of _____.

Date and time issued: March 5, 2012 3:30p

/s/
Theresa Carroll Buchanan
United States Magistrate Judge
Judge's signature

City and state: Alexandria, Virginia

The Honorable Theresa C. Buchanan, Magistrate Judge
Printed name and title

AO 93 (Rev. 12/09) Search and Seizure Warrant (Page 2)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
1:12 SW167 MJA	3-6-2012 10:30 A.M.	Antonio Lobato

Inventory made in the presence of : N/A

Inventory of the property taken and name of any person(s) seized:

See FD-597

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: 4-4-2012

Executing officer's signature

Michael L. Wagner FBI SA

Printed name and title

ATTACHMENT A (Filigree Court)

DESCRIPTION OF LOCATION TO BE SEARCHED

The premises to be searched (21715 Filigree Court, Ashburn, Virginia, aka DC2, cage 2320, racks numbered 0101 and 0103, and cage 2450, racks numbered 0101, 0102, 0103, 0104, 0105, 0106, 0107, 0108, 0109, and 0110), are 12 specified computer storage racks in a warehouse building approximately 147,600 square feet in size, constructed of tan concrete on a concrete slab foundation. The numbers "21715" are displayed at the top corner of the building exterior. The building interior consists of a series of metal-enclosed cages storing computer servers. The cages have key locks or biometric locks, and are generally numbered. Symplicity leases two cages within DC2, cage 2320 and cage 2450. Cage 2320 is a shared cage where multiple customers have racks stored within the same cage. Each rack has a lock on the front and back of the rack that only the customer who owns the rack can open. Symplicity has racks numbered 0101 and 0103 in cage 2320. Cage 2450 is a private cage that only Symplicity has servers stored in. There are 10 racks in cage 2450, numbered 0101, 0102, 0103, 0104, 0105, 0106, 0107, 0108, 0109, and 0110.

ATTACHMENT B

Particular Things to be Seized

1. All information that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. §§ 2 (aiding and abetting), 371 (conspiracy), and 1030 (fraud and related activity in connection with computers), including a conspiracy to access protected computers without authorization in order to obtain information among Ariel Friedler, Matthew Kelley, Lori Davies, Deborah Sullivan, and other unknown persons, including other Symplicity employees, including information pertaining to the following matters:

   a. Records relating to computer intrusions;

   b. Records relating to the collection and use of confidential business material belonging to Symplicity's competitors;

   c. Records relating to the use of anonymizing systems, including Tor;

   d. Records relating to the design of competitor's systems;

   e. Records relating to the client lists of Symplicity's competitors;

   f. Records of any communications about the violations and conspiracy; and

   g. Any computers or electronic media that were or may have been used as a means to commit the offenses described on the warrant, including downloading confidential materials without authorization in violation of 18 U.S.C. § 1030(a)(2).

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

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

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

c. evidence of the lack of such malicious software;

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

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

f. evidence of the times the COMPUTER was used;

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

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

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

3. Records and things evidencing the use of the Internet Protocol addresses 77.247.181.164 , 173.168.135.160, 76.100.17.95, 71.49.239.7, 74.192.146.36, or Tor to communicate with Maxient, Pave Systems, or other Symplicity competitors including:

a. routers, modems, and network equipment used to connect computers to the Internet;

b. records of Internet Protocol addresses used;

c. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

ATTACHMENT C

TAINT TEAM PROCEDURE

Agents participating in the execution of the search warrants to which this document has been made apart shall use the following procedure to minimize the review of privileged document by the investigative team. A "taint team" comprised of two Agents, one of who is an Agent lawyer, will be present at 1560 Wilson Boulevard, Suite 550, Arlington, Virginia during the execution of the warrant. After the business location has been secured, the taint team will search the office of Ariel Friedler, CEO of Symplicity, first and remove any communications that they deem privileged and seal them so that the rest of the search team does not have access to them. As the search of the business continues, including any forensic review of computers that may occur off-premises, if a member of the search team comes across an item that is potentially a privileged communication, it will be brought to the attention of the taint team who will make a determination.

FD-597 (Rev 8-11-94)

UNITED STATES DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
Receipt for Property Received/Returned/Released/Seized

File # 288A-RH-54964

On (date) 3/7/2012

item(s) listed below were:
- [x] Received From
- [ ] Returned To
- [ ] Released To
- [ ] Seized

(Name) Antonio Lobato

(Street Address) 21715 Filigree Court

(City) Ashburn VA 20147

Description of Item(s): One(1) Hitachi hard drive S/N: B9H3VBVS (FBI Property) containing 16 GB of Symplicity data files; One(1) Hitachi hard drive S/N: JK1101B9H3T56F (FBI Property) containing 159 GB of Symplicity Data files

Received By: _____ (Signature)

Received From: _____ (Signature)

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE SEARCH OF: The premises known as 1560 Wilson Blvd, Suite 550 Arlington, Virginia 22209	)	1:12SW166

And

IN THE MATTER OF THE SEARCH OF: The premises known as 21715 Filigree Court, Ashburn, Virginia, aka DC2, cage 2320, racks numbered 0101 and 0103, and cage 2450, racks numbered 0101, 0102, 0103, 0104, 0105, 0106, 0107, 0108, 0109, and 0110	)	1:12SW167

AFFIDAVIT IN SUPPORT OF SEARCH WARRANTS

I, Michael P. French, being duly sworn, depose and state the following:

INTRODUCTION

1. This affidavit is submitted in support of applications for search warrants for the premises known as 1560 Wilson Boulevard, Suite 550, Arlington, Virginia 22209 and 21715 Filigree Court, Ashburn, Virginia, aka DC2, cage 2320, racks numbered 0101 and 0103, and cage 2450, racks numbered 0101, 0102, 0103, 0104, 0105, 0106, 0107, 0108, 0109, and 0110 (hereafter together "SUBJECT PREMISES") for evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2 (aiding and abetting), 371 (conspiracy), and 1030(a)(2)(C) (intentionally accesses a protected computer without authorization, and as a result of such obtains information from any protected computer). The SUBJECT PREMISES is more fully described in Attachment A (Wilson Blvd) and Attachment A (Filigree Ct), herein incorporated

by reference. The items to be searched for and seized are described more particularly in Attachment B, herein incorporated by reference.

2. I am a Special Agent of the Federal Bureau of Investigation (FBI) assigned to the Richmond Division. I have been employed by the FBI for seven years. I am currently assigned to the Cyber Squad within the Richmond Division, where I am primarily responsible for the investigation of computer intrusions and cyber-crime matters. I have been the affiant for many complaint and search warrant affidavits, have made numerous arrests, and have executed many search warrants. Prior to transferring to the Richmond Field Office, I was assigned to the Washington Field Division for approximately five years where I was assigned to a Cyber squad that investigated internet fraud, intellectual property and child exploitation violations. In addition, I have received training in the investigation of cases involving computer crime and the use of the computers to advance criminal schemes. As a Special Agent of the FBI, I am authorized to investigate crimes involving computer intrusion, intellectual property rights, theft of trade secrets, wire fraud, and the use of public networks to facilitate such schemes.

3. I am familiar with the information contained in this affidavit based upon the investigation I have conducted to date and based on my conversations with other law enforcement officers who have engaged in numerous investigations involving computer intrusions.

4. Because this affidavit is being submitted for the limited purpose of applying for a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1030(a)(2)(C) is

presently located at the SUBJECT PREMISES, including within computers and related peripheral, and computer media found at the SUBJECT PREMISES.

PROBABLE CAUSE

5. The United States, including the FBI, is investigating a series of unauthorized access attempts, some of which were successful, into the computer systems of Maxient, LLC (Maxient) and Pave Systems, computer software companies that produce Student Conduct Records Management systems. As further described below, these attempts to access Maxient's and Pave's computer system appear to have originated with a competitor, Symplicity Corporation ("Symplicity"), a company headquartered in Arlington, Virginia within the Eastern District of Virginia.

Maxient Intrusions

6. Maxient has reported to the FBI that, since at least 2009, Maxient has experienced a series of attempted unauthorized accesses and at least one successful unauthorized access to its computers coming through its website, http://cm.maxient.com. According to Maxient, the unauthorized accesses to Maxient's computers allowed the target company to gain significant knowledge about Maxient's client lists, business model, and product design, which could be used to improve a competitor of Maxient's position in competitive bidding for future business.

7. On November 4, 2011, a cooperating witness ("CW") who formerly had been employed by Symplicity for approximately five years provided information to the FBI concerning the conduct of Ariel Friedler, the Chief Executive Officer ("CEO") of Symplicity.[1]

---

1 Ariel Friedler holds a Juris Doctorate and was admitted to the Florida bar in 2004, but, according to the Florida Bar Association, he became an inactive member in 2010 and so is not currently licensed to practice law. Nonetheless, to minimize any possibility that the investigative team will review privileged materials, in an abundance of caution, as further

According to the CW, Ariel Friedler showed the CW how to connect to Maxient's website and to look for specific customers by putting in Maxient's main URL, http://cm.maxient.com, followed by a question mark and a school abbreviation (ex: http://cm.maxient.com/?ulm) (the "?schoolcode" method).[2] Friedler told the CW that this was how Friedler checked for new customers on Maxient's website. The CW stated that every time Friedler found a new customer on Maxient's website, Friedler would send an instant message or email to the CW about it. The CW also stated that Friedler discussed using anonymizers and TOR[3] to hide Friedler's activity when Friedler was looking at competitors' networks, and that Friedler was very interested in using these technologies.

---

described in Attachment C, a filter agent will conduct an initial review of Friedler's office and will be available to review any other materials that an initial review determines may contain privileged materials.

2 As explained further below, Maxient operated a website that had individual areas for each of its customers that were protected by the use of individual usernames and passwords. Each Maxient customer could access the log-in page for its records on the Maxient site by navigating to a url specific to the customer that Maxient only gave to the customer and did not otherwise make publicly available. However, Maxient created individual log-in pages for its customers that followed a common naming convention, making it possible to hunt for client sites by inputting the standard convention and changing the client name. For example, http://cm.maxient.com/gmu would be the url to for the log in page for customer GMU. Because of the way that the Maxient website responded to slightly different urls, the "?schoolcode" method did in fact allow someone to navigate to a Maxient customer's log-in page, even though the ?schoolcode url was not the exact url given to customers.

3 The Onion Router Project ("TOR") is a system intended to enable online anonymity on the Internet. When a connection to the TOR network is first initiated, a random pathway through several Onion routers is chosen. At each Onion router, a layer of encryption is added. This method allows for a secure, anonymous connection between two computer systems because data passed along the anonymous connection appears different at each Onion router. The last IP address in the TOR route is known as the TOR exit node. When the connection is broken, all information about the connection is cleared at each Onion router.

8. As further discussed below, the information provided by the CW is consistent with Maxient's computer systems' records. Maxient's records further show attempts to access Maxient client pages without authorization.

Access from IP Address Associated with Symplicity

9. Beginning in May 2009, Maxient's log files show someone at the IP address 216.52.121.66 attempting to access client log-in pages on Maxient's web site. According to the American Registry for Internet Numbers ("ARIN"), IP address 216.52.121.66 is part of a network block (216.52.121.64-216.52.121.71) assigned to Symplicity Corporation, 1901 North Fort Myer Drive, Suite 503, Arlington, Virginia 22209 (hereinafter IP address 216.52.121.66 shall be referred to as the Symplicity IP Address).

10. In 2010, Maxient's server logs showed multiple attempts over a period of many months by the Symplicity IP Address to access Maxient customer log-in pages by trying many variations of a school's abbreviation to see if a log-in site existed for the university at that particular address. These urls were only given the customer and were not otherwise made public. There would be no reason for anyone other than a Maxient client to access the client's log-in page.

11. Significantly, the attempted accesses described above were formed in a way that did not exactly match the url actually given to clients, but, because of the coding of Maxient's website, would nonetheless redirect to the client log-in page if one existed. Specifically, clients were given a url in the form http://cm.maxient.com/clientname, where the client name was typically an abbreviation of a university's name. These accesses instead where submitted to http://cm.maxient.com, followed by a question mark and a school abbreviation (ex: http://cm.maxient.com/?ulm) (the "?schoolcode" method). Because of the way that the Maxient

website responded to slightly different urls, the "?schoolcode" method did in fact allow someone to navigate to a Maxient customer's log-in page, even though the ?schoolcode url was not the exact url given to customers. This is the same method described by the CW as having been used by Symplicity's CEO.

12. In August 2011, there were multiple attempts from Tor exit nodes to access Maxient's web sites using the same "?schoolcode" method used by the Symplicity IP address throughout 2010. As stated above, Symplicity's CEO had specifically discussed using TOR to hide his activity when looking at competitors' networks.

13. As early in February 2009, the Symplicity IP address also attempted to use what appeared to be SQL injection attacks. "Structured Query Language Injection" or "SQL Injection" is an attack often used to breach the security of a website by inputting SQL statements into a web form to get a poorly designed system to perform operations on the database other than the usual operations as intended by the site owner. Maxient's logs show numerous queries with odd characters and other malformed requests coming from the Symplicity IP address. Based on my training and experience, I know that attempting to repeatedly submit malformed queries like the ones submitted to Maxient's website from the Symplicity IP address is a method often used by hackers to attempt to gain unauthorized access to websites.

Access from IP Address Associated with Symplicity CEO

14. In the summer of 2010, Maxient's Intrusion Prevention System also showed repeated attempts to connect to both the public and management interface websites belonging to Maxient from another IP address 173.168.135.160. Maxient does not make public the url for these management interface sites as only a few Maxient employees are authorized to use these

sites in order to administer Maxient's systems. Someone using IP address 173.168.135.160 looked at the management interface sites and access non-public portions of Maxient's website where documentation regarding its products is stored.

15. On September 8, 2010, someone using IP address 173.168.135.160 also connected to the employee-only Maxient database management webpage. Logs also showed that the unauthorized user attempted to find customer sites by using the "?schoolcode" method.

16. According to Bright House Networks[4] records, the account assigned IP address 173.168.135.160 at 12:30 EDT and 13:42 EDT on September 8, 2010 was subscribed to in the name Moshe Friedler, service address 1011 South Clark Avenue, Tampa, Florida 33629. Moshe Friedler is the father of Ariel Friedler, the Chief Executive Officer ("CEO") of Symplicity.

Access from IP Address Associated with Symplicity Employee Matthew Kelley

17. Between November 13, 2010 and December 13, 2010, the IP address 98.218.225.32 attempted to connect to the client log-in page of several Maxient clients and made 45 connections to various Maxient customers' management web sites. The IP address 98.218.225.32 was using the "?schoolcode" method.

18. According to Comcast records, the account assigned IP address 98.218.225.32 during the relevant times was subscribed to in the name Rachel Miller, service address 1451 Belmont Street NW, Apartment 212, Washington, DC 20009. According to open source records, Matthew Kelley also resided at that address in July 2011.

---

4 Bright House Networks conducts business in Florida under the name of Time Warner/Road Runner Internet Services and is the owner of IP address **173.168.135.160**.

Accesses from IP Addresses Associated with Symplicity and Several of its Employees

19. According to Maxient logs, there were also multiple attempts to gain unauthorized access to its computer systems in 2010 and 2011 from IP addresses that were associated with other Symplicity employees, Matthew Kelley, Lori Davies, and Dr. Deborah Sullivan.

a. According to Maxient, Matthew Kelley is a Symplicity employee involved with their Conduct Records Management product. According to employment records checks, Kelley has worked for Symplicity since at least 2006.

b. According to the social networking career website Linkedin.com, Lori Davies lists her current employer as Symplicity where she has worked for over four years as a Product Support Specialist.

c. According to Symplicity's website, Dr. Deborah Sullivan is a Symplicity employee and her job title is Advocate Client Relationship Specialist.

20. During the summer of 2011, Maxient and Symplicity were competing with each other to win Vanderbilt University as a customer. Maxient log files show the Symplicity IP Address connecting to their server and searched for a customer website associated with Vanderbilt multiple times during this period. The attempts were always made using the "?schoolcode" method.

21. Maxient won the contract and built a functioning website for Vanderbilt that went live on Maxient's servers on July 12, 2011. Maxient did not provide a client url or other the access information for the Vanderbilt site to Vanderbilt officials until August 4, 2011.

22. Several weeks before Maxient even informed its customer about the creation of the log-in page, on July 12, 2011, at 11:18:49 EDT, the Symplicity IP Address issued the command "GET /?vanderbilt HTTP/1.1" which displayed the login page for the Vanderbilt site on Maxient's server. In the next ten minutes, the IP addresses 76.100.17.95, 71.49.239.7, and 74.192.146.36 issued the same command and accessed Vanderbilt login screen on Maxient's server. Within the next twenty minutes, the Symplicity IP Address again accessed the Vanderbilt log-in page on Maxient's server two more times. All of these IP addresses have been connected to Symplicity and/or its employees:

a. As described above, according to the American Registry for Internet Numbers ("ARIN"), the Symplicity IP address is IP address 216.52.121.66, part of a network block (216.52.121.64-216.52.121.71) assigned to Symplicity Corporation, 1901 North Fort Myer Drive, Suite 503, Arlington, Virginia 22209.

b. According to Comcast[5] records, the account assigned IP address 76.100.17.95 on July 12, 2011was subscribed to in the name Rachel Kelley, address 116 North Donelson Street, Alexandria, Virginia. According to open source records, Matthew Kelley also resided at that address in November 2010

c. According to CenturyTel[6] records, IP address 71.49.239.7 was assigned on July 12, 2011to the subscriber Lori Davies, 1722 Pebble Beach Lane, Lady Lake, Florida.

---

5 According to open source records, the IP address 76.100.17.95 is assigned to Comcast.

6 According to open source records, the IP address 71.49.239.7 is owned by CenturyTel who is now owned by CenturyLink.

d. According to Suddenlink[7] records, IP address 74.192.146.36 was assigned on July 12, 2011to the subscriber Harry Sullivan, 114 Brentwood Drive, Georgetown, Texas. According to open source records, also residing at this address is Deborah Sullivan.

Access to Log-in Pages of Former or Potential Symplicity Clients

23. Between August 14, 2011, and August 17, 2011, there were multiple failed login attempts to the Maxient customers' websites for former Symplicity clients. That is, someone reached the client log-in page and input invalid usernames and passwords in an attempt to gain access to the client's records on Maxient's computers.

24. For each of these failed log-ins, the person attempting to log-in to the client pages arrived at the login page using the "?schoolcode" method, a unique method the CW reports was used by Symplicity's CEO.

25. All of these login attempts came from known Tor exit nodes. As stated above, Symplicity's CEO had specifically discussed using Tor to hide his activity when looking at competitors' networks.

26. Each attempted log-in used a username that likely would have been known by Symplicity. The vast majority of these log-in attempts targeted specific usernames that can clearly be traced to known employees at these institutions who either have, or would be expected to have, accounts in the Maxient system and would have had accounts when they were clients of Symplicity.

---

7 According to open source records, the IP address 74.192.146.36 is owned by Suddenlink Communications.

27. In addition to the failed log-ins, on at least one occasion someone using the "?schoolcode" method did gain access to a Maxient client's records. On August 17, 2011, Maxient logs show that at 16:09:09 EDT, the IP address 77.247.181.164[8] accessed the login screen for the University of Louisiana at Monroe on Maxient's server after supplying the username "buckhaults" and the correct password. After logging in, this IP addressed accessed various portions of ULM's customer site including accessing Maxient's support documentation stored on another company's server. According to Maxient, visiting each part of Maxient's system would have provided a great deal of insight into the workings of the software, features, and common pitfalls simply from seeing the posting topics contained within. Maxient has informed the FBI that it did not authorize this access to its computer system through its website.

28. Between August 14, 2011 and August 17, 2011, there were also multiple failed login attempts to the Maxient customer websites for two potential clients that Symplicity was also competing to win. The person who provided the invalid logins arrived at Maxient's client pages using the "?schoolcode" method. Both companies set up demonstration sites for prospective companies, which sites required the potential clients to set up a username and password for the site.

Vulnerability Testing Tool Used Against Maxient's Server

29. On October 27, 2011 between 14:10:35 EDT and 14:11:10 EDT, over 10,000 connections were made to Maxient's Conduct Management server from the IP address 108.48.17.99. In each connection that was made to Maxient's server was the text "sfi9876."

---

8 According to open source records, the domain name associated with IP address 77.247.181.164 is rainbowwarrior.torservers.net and is a known TOR exit node.

30. An Internet search for the text "sfi9876" revealed that this is part of a tool called Skipfish. The website for the Skipfish describes the tool as follows:

> Skipfish is an active web application security reconnaissance tool. It prepares an interactive sitemap for the targeted site by carrying out a recursive crawl and dictionary-based probes. The resulting map is then annotated with the output from a number of active (but hopefully non-disruptive) security checks. The final report generated by the tool is meant to serve as a foundation for professional web application security assessments.

http://code.google.com/p/skipfish/wiki/SkipfishDoc. Some of the security checks that this tool perform including trying various SQL injection attacks, format string vulnerabilities, and integer overflow vulnerabilities. The documentation for the tool advises the tool user to "*First and foremost, please do not be evil. Use skipfish only against services you own, or have a permission to test.*" The tool can be programmed to use customized testing options to test specific sites. .

31. Multiple entries were found in Maxient's logs where the Skipfish tool attempted to access the customer site "ulm," where "ulm" is an abbreviation for the University of Louisiana at Monroe. These entries indicate that the individual using the Skipfish tool had knowledge of Maxient's customer.

32. Skipfish is a complex tool that requires the user to have knowledge of the Linux operating system, compiling source code manually, and using a command line to run the tool. The test results report that Skipfish would provide a detailed list of the various vulnerabilities of Maxient's server that exist. Maxient stated that they did not perform these tests and that they did not give authorization to anyone else to perform such testing

33. According to Verizon[9] records, IP address 108.48.17.99 was assigned at the relevant times to the subscriber Jillian Coyle, 5911 Jarvis Lane, Bethesda, Maryland, on October 27, 2011. Neither Coyle nor any other resident at this address currently appear to have any connection to Symplicity.

34. Symplicity uses website Github.[10] A Github user named "wcombs" has opened several support issues on the site for a Github project named "mxcl/homebrew" which utilizes Skipfish. "wcombs" stated that he was having issues compiling the "mxcl/homebrew" project with Skipfish. A member of the "mxcl/homebrew" project provided a solution to "wcombs'" problem and "wcombs" stated that the software then "installed perfectly". According to "wcombs'" profile on Github, he has been a member since December 12, 2010 and resides in West Virginia.

35. An Internet search for "wcombs Symplicity" reveals an email address for Will Combs, wcombs@symplicity.com. According to Virginia Employment Commission records, Combs has been an employee with Symplicity for several years. According to open source records, Will Combs resides in Martinsburg, West Virginia.

Pave Systems Intrusion

36. The CW stated that several years ago Friedler provided the CW with a customer list that he said was from another Symplicity competitor, Pave Systems. Friedler told the CW at

---

9 According to open source records, the IP address 108.48.17.99 is owned by Verizon Communications.

10 The website www.github.com describes itself as a "distributed version control system ideal for collaborative software development" Github is a free site that allows software projects to be hosted and many individuals can contribute to the project. Currently, there are over 2 million software repositories on the site with large companies such as Facebook, Microsoft, and Twitter providing sponsorship or contributing software code.

the time that Pave Systems had no security on their network which made it easy for Friedler to get the list.

37. On January 12, 2012, Ghassan Nino, owner of Pave Systems, told the FBI that approximately two years ago he was contacted by Friedler who was interested in buying Pave Systems' Student Conduct business. Nino stated that Friedler mentioned the names of several Pave Systems customers and Friedler stated that he found out the names of these clients from a "friend of mine." Nino stated that the names of Pave Systems customers is confidential information and is not publicly available. Nino was very surprised that Friedler knew who some of Pave Systems customers were.

The Premises

38. The CW stated that Symplicity has some of their computer servers at their office located **1560 Wilson Boulevard, Suite 550, Arlington, Virginia.** He stated that they are stored in a server room within the office space.The CW stated that the majority of Symplicity's servers are stored at a datacenter located at Ashburn, Virginia owned by Equinix.

39. The CW stated that there is a 50MB data line connecting the Symplicity office directly to their servers at the Equinix datacenter. Based on information provided by Equinix to your affiant on February 15, 2012, Symplicity is a customer in their DC2 datacenter located at **21715 Filigree Court, Ashburn, Virginia** and they have servers stored in racks in two different cages within the datacenter, cage 2320, racks numbered 0101 and 0103, and cage 2450, racks numbered 0101, 0102, 0103, 0104, 0105, 0106, 0107, 0108, 0109, and 0110.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

40. As previously stated, the investigation has determined that one or more computers are located at SUBJECT PREMISES, and there is probable cause to believe that such computers have been used as instrumentalities in the course of, and in furtherance of, fraud and related activity in connection with computers. Moreover, there is probable cause to believe that records and evidence are being stored in electronic form, including computer hard-drives, disks, CDs and other similar electronic storage devices. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

41. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe records described in Attachment B will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is 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.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In

addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

e. As described above, based on statements of the CW, I am aware that computer equipment was used to generate, store, and print documents used in the hacking scheme. There is reason to believe that there is a computer system currently located at each location that make of the SUBJECT PREMISES.

42. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described herein, but also for forensic electronic evidence that establishes how computers were

used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer in the SUBJECT PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

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, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

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

f. I know that when an individual uses a computer to obtain unauthorized access to a victim computer over the Internet, the individual's computer will generally

serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

43. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy or logical copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Generally speaking, logical copying only captures what the data that the operating system can see which does not include hidden sectors or deleted items. Either seizure, imaging, or logical copying is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing

evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

44. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), when persons executing the warrant conclude that it would be impractical to review

the media on-site, the warrant I am applying for would permit seizing, imaging, or logically copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, thus permitting its later examination consistent with the warrant. The examination may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

45. Symplicity is a functioning company that conducts legitimate business. The seizure of the Company's computers may limit the Company'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 to determine which computers and storage media must be seized or copied, and what computers and storage media need not be seized or copied. Where appropriate, Agents will copy data, rather than physically seize computers, to reduce the extent of disruption. If employees of the Company 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 Company's legitimate business. If, after inspecting the computers, it is determined that some or all of this equipment is no longer necessary to retrieve and preserve the evidence, the government will return it.

46. In light of the difficulties discussed above and if it is not feasible to image or logically copy the computer equipment onsite, as outlined in paragraph 44, I request permission for investigators to remove to a forensically-secure location the computers and computer-related equipment reasonably believed to be instrumentalities of the crimes, and to use whatever data

analysis techniques reasonably appear necessary to locate and retrieve digital evidence within the scope of this warrant. Such action will greatly diminish the intrusion of law enforcement into the premises and will ensure that evidence can be searched for without the risk of losing, destroying or missing the information/data for which there has been authorization to search.

CONCLUSION

47. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that violations of Title 18, United States Code, Sections 2 (aiding and abetting), 371 (conspiracy), and 1030(a)(2)(C) have occurred and fruits, evidence and instrumentalities of such criminal offenses described in Attachment B are presently located at the SUBJECT PREMISES. I, therefore, respectfully request that attached warrant be issued authorizing the search of the SUBJECT PREMISES in order to seize the items listed in Attachment B.

Michael P. French
Special Agent
Federal Bureau of Investigation

SUBSCRIBED and SWORN
before me this 5th of March, 2012

/s/
Theresa Carroll Buchanan
United States Magistrate Judge
Honorable Theresa C. Buchanan
UNITED STATES MAGISTRATE JUDGE