UNITED STATES DISTRICT COURT

for the

District of Alaska

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
INFORMATION ASSOCIATED WITH service@provendatarecovery.com and service@provendata.com THAT IS STORED AT PREMISES CONTROLLED BY Liquid Web, Inc.

Case No. 3:18-mj-00003-KFM

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):*

See Attachment A, incorporated here by reference.

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

See Attachment B, incorporated here by reference.

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 USC §§ 1030, 1343, and 2511.	Fraud and related activity in connection with computers, wire fraud, and illegal wiretapping.

The application is based on these facts:

See attached Affidavit in Support of Search Warrant.

- ☑ 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.

Signtaure Redacted
Applicant's signature

Jayanth Swamidass, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 1-5-2018

/s/ Kevin F. McCoy
United States Magistrate Judge
Signature Redacted
Judge's signature

City and state: Anchorage, Alaska

Magistrate Judge Kevin F. McCoy
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OFALASKA

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH service@provendatarecovery.com and service@provendata.com THAT IS STORED AT PREMISES CONTROLLED BY Liquid Web, Inc.	Case No. 3:18-mj-00003-KFM **Filed Under Seal**

AFFADAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Jayanth Swamidass, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that are stored at premises controlled by Liquid Web, Inc., an email provider headquartered at 2703 Ena Drive, East Lansing, Michigan 48917. The information to be searched is described in the following paragraphs and 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 Liquid Web, Inc. to disclose to the government copies of the 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 the items described in Section II of Attachment B.

2. I am a Special Agent ("SA") with the FBI, and have been since October 2015. I am currently assigned to the Anchorage, Alaska Division of the FBI, and to a squad responsible for investigating national security and criminal cyber threats and intrusions. Among other duties, my squad specializes in the investigation of computer and high-technology crimes, including

computer intrusions, denial of service attacks, and other types of malicious computer activity. Prior to joining the FBI, I was employed as a global trade consultant with a multinational professional services firm, where I advised large corporate clients on international trade regulatory matters. I hold a Juris Doctor degree and am a member of the California State Bar. As a federal agent, I am authorized to investigate violations of the laws of the United States and am a law enforcement officer with authority to execute federal search warrants. I have served several search warrants, and have seized evidence of criminal violations.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 1343 (wire fraud), and violations of 18 U.S.C. § 1030 (Computer Fraud and Abuse Act), and 18 U.S.C. § 1956 (money laundering) have been committed by unknown persons. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband or fruits of these crimes further described in Attachment B.

JURISDICTION

5. 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). 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).

KFM
JAN - 5 2018

LEGAL BACKGROUND

6. Title 18, United States Code § 371 states, "If two or more persons conspire either to commit any offense against the United States . . . and one or more of such persons do any act to effect the object of the conspiracy, each shall be … imprisoned not more than five years…."

7. Title 18, United States Code § 1343 states, "Whoever, 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 … imprisoned not more than 20 years….

8. Title 18, United States Code § 1030 states, "Whoever . . .

* * *

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains-- . . .

* * *

(C) information from any protected computer;

* * *

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;

(5)(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.

* * *

KFM
JAN - 5 2018

(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any--

(A) threat to cause damage to a protected computer;

(B) threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or

(C) demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion;

shall be punished as provided in subsection (c) of this section.

(b) Whoever conspires to commit or attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(c) The punishment for an offense under subsection (a) or (b) of this section is—

* * *

(2) . . . .

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if--

(i) the offense was committed for purposes of commercial advantage or private financial gain;

(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

(iii) the value of the information obtained exceeds $5,000; and

(3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4),3 or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph . . . ."

PROBABLE CAUSE

DMA Locker is used by the subject to encrypt data on a victim's computer system and require payment in exchange for restored access to that data

9. As of January 2, 2018, the FBI has received approximately 42 complaints from victims of a form of computer malware identified as DMA Locker. The characteristics of DMA

KFM
JAN - 5 2018

Locker categorize it as "ransomware." Generally, upon installation of ransomware on a victim's computer, the program will seek to encrypt all files on the system, rendering the computer unusable. When the owner or user of the computer attempts access, the ransomware will display a message – or ransom note – informing the user of the encryption and demanding payment in exchange for a key or password to decrypt the files.

10. In the case of DMA Locker, the FBI has identified that the subject responsible for such attacks is able to plant the ransomware on victim computers by exploiting weak passwords associated with Windows Remote Desktop Connection (RDC) accounts. Doing so gives the subject remote access to the computer. The ransomware requires administrator privilege to execute, but if the compromised account does not have administrator privileges, the subject will use additional software to gain access as an administrator.

11. FBI forensic analysis of victim computers suggests the subject uses additional software to scan the victim's local computer network and provide a map of additional computers connected to the victim's compromised computer. Doing so provides many benefits, one of which would provide the subject intelligence on how large of an infection they could possibly inflict on the victim network, and additionally, a list of additional services the victim's systems are using that might also be vulnerable to exploitation. When executed, the ransomware references a list of file extensions, which if located on the victim network, the ransomware will attempt to encrypt.

12. After the encryption is completed, the ransomware will display a message to the victim user, which informs the user of what has occurred, and that the encrypted information is only recoverable by paying the subject with Bitcoin – an online cryptocurrency with real value convertible to U.S. Dollars – who will then provide the victim with a decryption key to regain

KFM
JAN - 5 2018

access to the encrypted data. In the cases that the FBI has investigated, this ransom amount as ranged from approximately three Bitcoins to approximately 10 Bitcoins. While the conversion rate of Bitcoins to United States Dollars fluctuates daily, as of the date of this affidavit, 1 Bitcoin is valued at approximately $18,000.

13. According to the online website for the anti-malware company Malwarebytes, malware researchers first observed DMA Locker ransomware attacks beginning in or about February 2016.

FBI's first observed instance of DMA Locker attack and remediation by Proven Data Recovery

14. The FBI's investigation into DMA Locker began around April 3, 2016, when an attorney representative of the real-estate agency Herrington & Company contacted the FBI Anchorage Division to report that the company's computer system had been infected by malware. This ransomware had encrypted approximately all files on Herrington & Company's computer system and demanded payment of four Bitcoins made to Bitcoin address 15TNtDFq9ZKovLEk7s9zrZfRYAz6ZU4STe. After payment had been completed, the ransom note prompted the victim to send an email to address team4004@gmx.com referencing a code found in the note that would identify the victim to the subject. After this, the victim would be provided with an electronic key to decrypt the files.

15. On or about April 11, 2016, Simon Schroeder, an information technology (IT) services consultant hired by Herrington & Company to remediate the ransomware problem, sent an email to address team4004@gmx.com, attempting to confirm that the subject would provide a decryption key after payment. On April 11, 2016 at 19:51:09 +0200, the consultant received a one-word email from team4004@gmx.com, stating: "yes."

KFM
JAN - 5 2018

16. Also on or about April 11, 2016, the owner of Herrington & Company, Leif Herrington, informed the FBI that he had engaged a New York-based firm called Proven Data Recovery (PDR) to help recover Herrington's electronic data. PDR claimed the ability to decrypt files infected with ransomware for a fee. PDR quoted Herrington a price of approximately $6,000 in order to restore access to the encrypted files.

17. Following a consultation with a client manager from PDR, Schroeder provided PDR with a sample file for evaluation. PDR then scheduled an appointment a couple days later. During the appointment, Schroeder first moved the encrypted files to a backup computer system. Schroeder then granted remote access to PDR so it could access the infected computer system, which contained a subset of the encrypted files. Schroeder observed PDR work on Herrington & Company's computer system using the command prompt for approximately 45 minutes, after which the files were decrypted. Schroeder later provided PDR remote access to the computer workstation at Herrington & Company that contained the remainder of the encrypted files. PDR then decrypted those files using a similar process.

18. While Schroeder was unable to tell exactly what PDR had done to decrypt the data, based on the size of the encrypted files, and the speed at which PDR was able to decrypt them, Schroeder believed that PDR simply paid the original four Bitcoin ransom, after which the subject responsible provided the means to decrypt the files. PDR did not inform either Schroeder or Herrington that this would be their method to restore access to the files.

Proven Data Recovery's method to recover data encrypted by DMA Locker is to communicate with the subject responsible for the attack and pay the demanded ransom

19. Subsequent investigation by the FBI confirmed that PDR was only able to decrypt the victim's files by paying the subject the ransom amount via Bitcoin address 15TNtDFq9ZKovLEk7s9zrZfRYAz6ZU4STe, communicating with the subject at email address

KFM
JAN - 5 2018

team4004@gmx.com, and obtaining a decryption key from the subject via that same email address. Records associated with Bitcoin accounts owned by PDR, provided to the FBI pursuant to federal grand jury subpoena by Bitcoin exchanger Coinbase, Inc. showed a transaction of four bitcoins sent from PDR's account to Bitcoin address 15TNtDFq9ZKovLEk7s9zrZfRYAz6ZU4STe on April 11, 2016, at 11:37:41 AM.

20. On or about April 7, 2016, FBI Special Agents interviewed Mark Congionti, Lead Solutions Manager at, and one of the owners of, PDR, regarding his knowledge of DMA Locker and the DMA Locker attack on Herrington & Company. Congionti stated that he was very familiar with DMA Locker, as his company had helped numerous victims of the malware recover data. According to Congionti, there was currently no way to decrypt such data, apart from paying the subject and obtaining a decryption key. Congionti acknowledged that PDR did communicate with the subject responsible for DMA Locker attacks in the course of making payments to the subject on behalf of PDR's clients.

21. According to Congionti, all of PDR's communication with the DMA Locker subject was conducted using PDR's company email account, and retained by PDR. In fact, PDR maintained several hundred such email exchanges between PDR and email addresses associated with DMA Locker attacks. Congionti promised to provide the FBI with all requested records of communications associated with DMA Locker attacks, with the stipulation that producing them would likely be a time-intensive process.

Proven Data Recovery has provided the FBI with records of a limited number of email exchanges with DMA Locker email accounts; however, Proven Data Recovery maintains many more

22. On or about April 7, 2017, the FBI sent an email to Congionti requesting the following information: (1) any email communication with ransomer related to the April 2016

KFM
JAN - 5 2018

Herrington & Company DMA Locker attack, (2) Any email communication with the email accounts team4004@gmx.com, and team2002@gmx.com, (3) a list of all email aliases used by DMA Locker ransomer, (4) Bitcoin accounts used by DMA Locker ransomer, and (4) relevant forensic reports containing IP address identifiers. In an email sent to the FBI on or about May 12, 2017, Congionti provided copies of approximately 12 emails sent between the email account service@provendatarecovery.com and either the email address january0040@gmx.com or team4004@gmx.com. Both of these email addresses had been previously known to the FBI as ones utilized by the subject responsible for DMA Locker. In addition to these emails, Congionti also provided the FBI with a list of all email addresses that PDR had identified as associated with DMA Locker. These accounts were week4004@fastmail.com, january0040@gmx.com, january0060@gmx.com, team2002@gmx.com, team4004@gmx.com, team8008@gmx.com.

23. In the same email, Congionti stated that Proven Data Recovery had "200 or more cases and many more emails" related to DMA Locker attacks. At that time, given that it had already taken PDR over a month to produce any records, the FBI did not request that PDR provide records of all emails between PDR and the DMA Locker email accounts. However, the FBI did request the emails associated with the April 2016 DMA Locker attack on Herrington & Company.

24. On or about May 26, 2017, PDR provided the FBI with one email sent from the email account team4004@gmx.com to the account service@provdendatarecovery. This email was dated April 11, 2016 15:01:42 -0400, with subject line "Re: PAID DMALOCK 70:40:44:84:72:48:39:59." The content of the email said "Thank you for your payment. Password for attachment is your email: service@provendatarecovery.com Extract all files to C:\ProgramData and run svchosd.exe as administrator (it's important) then load dma_private.key

KFM
JAN - 5 2018

and click "UNLOCK FILES" button. The FBI understands this email to be the provision of a decryption key to PDR following payment of the four Bitcoin ransom.

25. Based on Mail Exchanger (MX) records for the domain provendatarecovery.com, the FBI believes email records are stored at the premises of Liquid Web, Inc. located at 2703 Ena Drive, Lansing, MI 48917. The MX is the server designated as responsible for receiving email for the associated domain. A domain's MX information is generally registered along with its Domain Name Servers (DNS) information which is publicly available through third party tools such as www.mxtoolbox.com. According to MX records returned by mxtoolbox.com for provendatarecovery.com, Liquid Web, Inc. IP address 72.52.140.22 is the designated MX server responsible for the domain.

26. On or about December 5, 2017, FBI Special Agents again interviewed PDR executives Mark Congionti and Victor Congionti. Both confirmed that PDR has used the email accounts service@provendata.com and service@provendatarecovery.com to communicate with the DMA Locker subject in the course of facilitating payment on behalf of victims of DMA Locker. Victor Congionti also confirmed that PDR utilized Liquid Web, Inc. to host these email accounts, and that all email content associated with these accounts is stored on a dedicated server in the control of Liquid Web. According to Victor Congionti, the host name of this server is serv.seribrum.com.

27. In general, an email that is sent to a Liquid Web subscriber is stored in the subscriber's "mail box" on Liquid Web servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Liquid Web servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Liquid Web's servers for a certain period of time.

KFM

JAN - 5 2018

28. Victor Congionti stated that PDR also maintains a database within their own computer systems that contains records of all PDR's clients that have been attacked by DMA Locker. PDR also maintains in its computer systems forensic reports PDR conducted of victim computer systems infected with DMA Locker.

BACKGROUND ON E-MAIL, IP ADDRESSES, AND BITCOIN

29. In my training and experience, I have learned that Liquid Web, Inc. provides a variety of on-line services, including electronic mail ("email") access, to the public. Liquid Web Inc. allows subscribers to obtain email accounts at customized domains like the email accounts listed in Attachment A. Subscribers obtain an account by registering with Liquid Web, Inc.. During the registration process, Liquid Web, Inc. asks subscribers to provide basic personal information. Therefore, the computers of Liquid Web, Inc. are likely to contain stored electronic communications (including retrieved and unretrieved email for Liquid Web, Inc. subscribers).

30. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

KFM
JAN - 5 2018

31. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

KFM

JAN - 5 2018

32. Bitcoin is a type of virtual currency, circulated over the Internet as a form of value. Bitcoin are not issued by any government, bank, or company, but rather are controlled through computer software operating via a decentralized, peer-to-peer network. Bitcoin is just one of many varieties of virtual currency.

33. Bitcoin are sent to and received from Bitcoin "addresses." A Bitcoin address is somewhat analogous to a bank account number and is represented as a 26-to-35-character-long case-sensitive string of letters and numbers. Each Bitcoin address is controlled through the use of a unique corresponding private key, a cryptographic equivalent of a password or pin needed to access the address. Only the holder of an address' private key can authorize any transfers of Bitcoin from that address to other Bitcoin addresses. Users can operate multiple Bitcoin addresses at any given time, with the possibility of using a unique Bitcoin address for each and every transaction.

34. To transfer Bitcoin to another address, the sender transmits a transaction announcement, cryptographically signed with the sender's private key, across the peer-to-peer Bitcoin network. The Bitcoin address of the receiving party and the sender's private key are the only pieces of information needed to complete the transaction. These two keys by themselves rarely reflect any identifying information. As a result, little-to-no personally identifiable information about the sender or recipient is transmitted in a Bitcoin transaction itself. Once the sender's transaction announcement is verified, the transaction is added to the blockchain, a decentralized public ledger that records all Bitcoin transactions. The blockchain logs every Bitcoin address that has ever received a bitcoin and maintains records of every transaction for each Bitcoin address.

KFM
JAN - 5 2018

35. While the identity of the Bitcoin address owner is generally anonymous (unless the owner opts to make the information publicly available), analysis of the blockchain can often identify the owner of a Bitcoin address. The analysis can also reveal additional addresses controlled by the same individual or entity. For example, a user or business may create many Bitcoin addresses to receive payments from different customers. When the business wants to move the bitcoin that it has received, it may group those addresses together to send a single transaction. Analysis of the blockchain information associated with such a transaction would indicate that each of those addresses was, in fact, part of a "cluster" of Bitcoin addresses controlled by a single entity. This analysis allows law enforcement and the private sector alike to gain insight into all of the addresses associated with a company. Several companies specializing in blockchain analysis create large databases for building these clusters and offer software products to facilitate this sort of analysis.

36. To acquire bitcoin, a typical user will purchase them from a virtual currency exchanger. A virtual currency exchange is a business that allows customers to trade virtual currencies for other forms of value, such as conventional fiat money (e.g., U.S. dollar, Russian ruble, €). When a user wishes to purchase bitcoin from an exchanger, the user will typically send payment in the form of fiat currency, often via bank wire, or other virtual currency to an exchanger, for the corresponding quantity of bitcoin, based on a fluctuating exchange rate. The exchanger, usually for a commission, will then either sell the user bitcoin from the exchange's reserves or will attempt to broker the purchase with another user who is trying to sell bitcoin. The purchased bitcoin are then transferred to the purchaser's Bitcoin address, allowing the user to conduct transactions with other Bitcoin users. Virtual currency exchanges doing business in

KFM
JAN - 5 2018

the United States are regulated under the Bank Secrecy Act and must collect identifying information of their customers and verify their clients' identities.

37. Since the blockchain serves as a searchable public ledger of every Bitcoin transaction, investigators may trace transactions to Bitcoin exchangers. Since those exchangers collect identifying information about their customers, subpoenas or other appropriate process submitted to these exchangers can reveal the true identity of the individual responsible for the transaction.

CONCLUSION

38. Based upon the above information, your affiant submits that there is probable cause to believe that within information on the premises controlled by Liquid Web, Inc., and on the premises controlled by Proven Data Recovery, as set forth in Attachment A (Property to be Searched), there exists evidence, fruits, and instrumentalities of violations of the Subject Offense, as set forth in Attachment B (Particular Things to be Seized).

39. Because the warrants will be served on Liquid Web and Proven Data Recovery, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

Signtaure Redacted

Jayanth Swamidass
Special Agent, Federal Bureau of Investigation

Subscribed and sworn to before me on the 5th day of January 2018.

/s/ Kevin F. McCoy
United States Magistrate Judge
Signature Redacted

United States Magistrate Judge

KFM

JAN - 5 2018

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with service@provendata.com and service@provendatarecovery.com that is stored at premises owned, maintained, controlled, or operated by Liquid Web, Inc., a company headquartered at 2703 Ena Drive, East Lansing, Michigan 48917.

KFM
JAN - 5 2018

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Liquid Web, Inc. (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on January 2, 2018, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the accounts, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the accounts, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

KFM

JAN - 5 2018

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code § 371, Title 18, United States Code § 1343, Title 18, United States Code § 1030, those violations involving the subject responsible for DMA Locker ransomware attacks and occurring after February 1, 2016, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) Any communication with any of the following email accounts: week4004@fastmail.com, january0040@gmx.com, january0060@gmx.com, team2002@gmx.com, team4004@gmx.com, team8008@gmx.com, or any other email address found to be used by a subject associated with the DMA Locker ransomware attacks.

(b) Information identifying, or that could lead to the identification of, any financial account owned or utilized by the subject responsible for DMA Locker attacks.

(c) Information identifying any victim of DMA Locker.

(d) Information related to any financial transaction between any party and an account identified as one owned or utilized by the subject responsible for DMA Locker attacks.

(e) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner.

(f) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation.

KFM
JAN - 5 2018

(g) The identity of the person(s) who created or used the user IDs, including records that help reveal the whereabouts of such person(s).

(h) The identity of the person(s) who communicated with the user IDs about matters relating to DMA Locker ransomware attacks, including records that help reveal their whereabouts.

KFM

JAN - 5 2018