AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Central District of Illinois

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 the LastPass account associate with stephan4096@gmail.com that is stored at premises controlled by LogMeIn, Inc.

Case No. 19-MJ- 7019

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, attached hereto and incorporated by reference.

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

See Attachment B, attached hereto and incorporated 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*
21 United States Code §841(a)(1); 18 United States Code §1956(a)(1)(B)(i)	Distribution of a Controlled Substance; Money Laundering

The application is based on these facts:
See Special Agent Todd Emery's attached affidavit.

- ☐ 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.

s/Todd Emery
Applicant's signature

Special Agent Todd Emery, DEA
Printed name and title

Sworn to before me and signed in my presence.

Date: 1/31/2019

s/Eric I. Long
Judge's signature

City and state: Urbana, Illinois

Eric I. Long, United States Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF ILLINOIS

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH the LastPass account associated with **stephan4096@gmail.com** THAT IS STORED AT PREMISES CONTROLLED BY **LogMeIn, Inc.**	Case No. 19 mj 7019 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Todd M. Emery, 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 a certain account that is stored at premises controlled by LogMeIn, Inc., an electronic storage company headquartered at 323 Summer Street, Boston, Massachusetts. 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 LogMeIn, Inc. to disclose to the government records and copies of the information (including the content of communications) pertaining to the subscriber or customer associated with the accounts described above and 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 with the Drug Enforcement Administration and have

been so employed for more than seven years. I have had extensive training in the investigation of drug related crimes and the enforcement of federal laws concerning controlled substances as found in Title 21 of the United States Code. Currently, I am assigned to the DEA's Springfield, Illinois, Resident Office (SRO). I have investigated illicit controlled substance trafficking, to include the importation, distribution, manufacture and cultivation of illegal substances. I have personally conducted or assisted in numerous investigations of state and federal criminal violations involving the illegal trafficking of narcotics and related crimes. I have received specialized training in various aspects of narcotics investigations, which includes but is not limited to interviewing defendants and witnesses, surveillance techniques, and money laundering. Prior to my assignment at SRO, I served as Technical Operations Agent to the DEA Imperial, California, District Office for approximately five years where I assisted agents in conducting cyber investigations, authored several search warrants to technical enterprises such as Microsoft and Facebook, and handled operations for that office's wire room to include assisting in routing data packets such as email content to approved systems for agent investigations. I also served two years at DEA's Office of Special Intelligence, where I learned skillsets involving Virtual Private Networking (VPN), IP configuration, and basic programming in a few computer coding languages. I have helped prepare numerous complaint and search warrant affidavits, participated in the execution of search warrants, and testified at criminal trials during my participation in drug investigations.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. 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 21 U.S.C. § 841(a)(1), Distribution of a Controlled Substance, and 18 U.S.C. § 1956(a)(1)(B)(i), Money Laundering, have been committed by Stephan Caamano, utilizing information stored within LastPass and LogMeIn accounts attached to email stephan4096@gmail.com controlled, maintained, or operated by LogMeIn, Inc. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/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).

PROBABLE CAUSE

6. In December 2017, law enforcement agents began investigating Stephan Caamano for manufacturing controlled substances following the discovery of purchases of tablet press machines from China. Through the investigation, it was discovered that

Caamano maintained a LastPass account with LogMeIn, Inc. which was linked to the email account stephan4096@gmail.com.

7. Throughout 2017, Customs and Border Protection agents seized several suspicious packages intended for delivery to Caamano. These included: (1) a package containing one turbine wheel box pill press machine from Shanghai, China, addressed to Stephan Caamano at 510 South Fair Street, Champaign, Illinois, seized on April 18, 2017; (2) a package containing 109 grams of Fentanyl and 210 grams of Alprazolam from an unknown shipper to Caamano at 1717 West Kirby Avenue, #108, Champaign, Illinois, a mailbox rented by Caamano on June 13, 2017; and (3) seven packages that contained drilling machine bolts for a tablet press machine from Shanghai, China, inbound to Caamano at an address of 202 South Broadway Avenue, #142, Urbana, Illinois, a mailbox rented by Caamano, on July 13, 2017.

8. In addition to suspicious deliveries being made to Caamano, law enforcement officers linked several suspicious packages containing counterfeit Xanax pills as having originated with Caamano. On March 8, 2018, agents conducted surveillance of Caamano at his residence, 1510 Glenshire Drive, Champaign, Illinois.[1] At approximately 10:00 a.m., agents observed Caamano depart his residence and travel to a

---

[1] Agents previously had performed an open source records search and learned utilities in Stephan CAAMANO's name had been established at 1510 Glenshire Drive, Champaign, Illinois. Agents also had discovered via subpoenaed bank records that CAAMANO had purchased the property in full with a wire transaction to the seller's bank under the business name Longevity Realty Management LLC.

United States Postal Service drop box located near 2012 Round Barn Road, Champaign, Illinois. Agents then observed and video recorded Caamano as he removed yellow manila envelopes from the rear passenger area of his vehicle multiple times and deposited said manila envelopes into the USPS drop box.

9. That same morning, while maintaining surveillance of the drop box, agents contacted the United States Postal Inspection Service to open the drop box near 2012 Round Barn Road, Champaign, Illinois, and collect all mail from inside the drop box.

10. Later that morning, agents met with the USPS mail carrier sent to retrieve the packages at the Round Barn Road location. Prior to the mail carrier's arrival, agents confirmed via surveillance that no other individuals had gained access to the USPS drop box or tampered with its contents. With assistance from the USPS mail carrier, agents were able to visually inspect the contents of the drop box and observed 33 yellow manila envelopes matching in appearance the yellow manila envelopes agents previously saw Caamano depositing into the drop box. These 33 packages were brought to the United States Post Office, located at 600 North Neil Street, Champaign, Illinois.

11. Agents visually inspected each of the 33 manila envelopes and observed that the return sender on each was listed as a "Colin H. Taylor". Agents also observed a shipping company, EasyPost, had created the shipping label on each envelope, and all envelopes had the same EasyPost account number: C26321. Inside one of the packages, officers discovered approximately 1,000 pills which were determined following analysis

to contain alprazolam, a Schedule IV controlled substance. The pills were nearly identical in appearance to the medication Xanax, manufactured by Pfizer.

12. Agents interviewed the USPS mail carrier who advised similar manila envelopes had been deposited into four USPS drop boxes in the vicinity of Mattis Avenue and Kirby Avenue in Champaign, Illinois, each day for several months. The mail carrier estimated the number of manila envelopes to be between 50 and 100 among the four drop boxes each day.

13. Multiple similar packages were obtained by law enforcement sent utilizing the same EasyPost account previously linked to Caamano, account C26321. On February 21, 2018, the Sheriff's Office took a report at 3206 Halifax Drive, Apartment B, Champaign, Illinois, in which a female subject, identified as T.A., received four boxes delivered to her by USPS, each identifying her as the "return sender." T.A. told the Sheriff's Office that she did not send any boxes and opened one to check its contents. Upon inspection, T.A. observed three gray packages, wrapped in bubble wrap, inside the box. T.A. then opened one gray package and discovered numerous pills, all marked with "Xanax" on each pill. T.A. relinquished custody of the four boxes and their contents to the Sheriff's Office. Agents reviewed photographs taken of the shipping labels on the four boxes and observed a shipping label created by the same EasyPost previously linked to Caamano.

14. On March 12, 2018, DEA agents took custody of the four boxes delivered to T.A. and their contents from the Sheriff's Office. Agents inspected the contents and

confirmed the four boxes were each filled with three packages. Each of the three packages contained numerous white elongated pills. Agents observed that each pill bore the marking "Xanax" on one side and the marking "2" on the other side, markings consistent with pills made by the pharmaceutical manufacturer Pfizer. Agents noted upon inspecting the pills through the plastic packaging that several of the pills had lighter markings, indicating possible counterfeit production. On March 27, 2018, laboratory results returned indicating the pills were all alprazolam (the main active chemical in Pfizer's Xanax) with a 95% level of confidence. In total, the four packages contained 83,538 dosage units (pills).

15. Meanwhile, on March 8, 2018, Cleveland Police Department Detective John Dlugalinski reported USPS Parcel 9405536897846313514706, also sent by the same EasyPost account, to United States Postal Inspection Services Investigator Bryon Green. The parcel was addressed to 3740 Euclid Ave, Cleveland, Ohio, 44115, and was turned over by a resident who had no knowledge of the parcel. The parcel contained more than 1,000 Xanax-labeled alprazolam pills; the presence of alprazolam was confirmed by the Cuyahoga County Laboratory.

16. On March 22, 2018, Investigator Green identified additional associated mailings from this same EasyPost account delivered to Nicholas Armstrong at 1443 E. 25th St. in Cleveland, Ohio 44114. These parcels, like those deposited by Caamano into the mail drop box in Champaign, Illinois, had a return address of Colin H. Taylor, 2105 S. Zuppke Dr., Urbana, Illinois, and were associated with EasyPost account C26321.

17. On March 26, 2018, Investigator Green, along with Homeland Security Investigations and the Drug Enforcement Administration, conducted a controlled delivery of the parcels destined for Armstrong. Agents detained Armstrong after he took custody of the parcels and returned to his residence. Armstrong signed a consent form permitting law enforcement agents to search his residence, which resulted in the recovery of the two parcels associated with EasyPost account C26321, along with various narcotics.

18. Armstrong provided a statement to agents and advised he purchased the "Xanax" that was recovered from the parcels from a darkweb vendor that Armstrong identified as Reddit user "Googleplex". Armstrong stated that "Googleplex" sells "Xanax" on the Dream Market, but advised that Armstrong purchased directly from "Googleplex" by sending Monero[2] cryptocurrency to a wallet[3] provided by "Googleplex." Armstrong stated he communicates with "Googleplex" via email.

---

[2] An open-source cryptocurrency that focuses on privacy and decentralization. Monero uses a public ledger to record transactions while new units are created through a process called mining. Monero aims to improve on existing cryptocurrency design by obscuring sender, recipient, and amount of every transaction made, as well as making the mining process more egalitarian.

[3] A "wallet" or cryptocurrency wallet stores the public and private keys, which can be used to receive or spend the cryptocurrency. A wallet can contain multiple public and private key pairs. The cryptocurrency itself is not in the wallet. The cryptocurrency is decentrally stored and maintained in a publically available ledger. With a private key, it is possible to write in the public ledger in order to spend the cryptocurrency.

19. Based on the foregoing investigation, on May 27, 2018, residential search warrants were executed at 1510 Glenshire Drive and 510 South Fair Street in Champaign, Illinois. Stephan Caamano's rental residence, 510 South Fair Street, was largely empty, although law enforcement agents proof of residency for Caamano, as well as one zp9 rotary tablet press with a Xanax pilil stamp, two 20-liter mixing machines, three commercial grade scales, three heavy duty vacuum sealing machines, multiple large plastic bins and containers used to sort and mix powders, a container filled with binding agent Firmapress, pressed counterfeit Xanax bars, non-prescribed steroids, doping masking agents, non-FDA approved tramadol and domperidone medicines, tryptamine (psychedelic), and multiple materials used for packaging and shipping items via registered mail. The pill press had been partially taken apart.

20. Based on the statements gathered from Armstrong, agents also collected several electronics from Caamano's residence at 1510 Glenshire Drive in Champaign, Illinois. These included: multiple cellular devices, a Toshiba laptop, amd several computers and computer-related components containing memory/hard drive space, including a CyberPowerPC computer tower.

21. Through use of a prior search warrant acquired in this investigation, information was obtained from a cellular device, taken at the time of Caamano's arrest, showed numerous accounts and applications activated on the device. One of those accounts was a LastPass account associated with email stephan4096@gmail.com. This

email address had been used by Caamano to purchase several items relating to his illicit drug activities, including pill presses.

22. Also found on the same cellular device as the LastPass account was evidence of cryptocurrency and TOR applications, which confirm use of the device for illicit dark web activities, as described by Armstrong.

23. On October 15, 2018, Champaign Police Department Digital Forensics Examiners were able to bypass Caamano's encryption on his CyberPowerPC. On this computer was an extension app for LastPass, associated with email account stephan4096@gmail.com. Agents were unable to access Caamano's LastPass account as no master password could be located on the device to unlock the account. Agents were also unable to access several websites and programs on the computer due to lack of password access; these websites and programs included cryptocurrency wallets maintained by Caamano. Based on statements from customers associated with Caamano's illicit drug sales, it is believed Caamano received payment for the counterfeit Xanax pills via cryptocurrency and maintained these moneys through darkweb wallets.

24. The moneys maintained in cryptocurrency wallets was used to purchase gold bullion, which was shipped to Caamano at his 1510 Glenshire residence. Caamano then sold the gold bullion in exchange for US currency through various gold companies, thereby masking the origin of the money as cryptocurrency.

LOGMEIN, INC. AND LASTPASS

25. I have learned in my training and experience, as well as the investigation conducted in this case, that LogMeIn, Inc. owns and operates a password manager, vault, and digital wallet app of the name "LastPass" that can be accessed at www.lastpass.com, as well as from mobile apps. This program allows users to maintain log-in information, including usernames and passwords, for other programs and websites on LastPass. LastPass then enters the log-in information into these other websites and programs for the LastPass user.

26. To create a LastPass account, an individual must choose a unique username and password and complete basic profile information regarding the user. This information can include the user's full name, physical address, location, email addresses, interests, and other personal information. Once these steps are complete, the profile for the new account is created.

27. Once a username/profile is established and a new account is created, the new user then chooses a strong master password for his/her LastPass account, which allows the user to then add log-in information for other accounts. The other account information is aggregated in the LastPass Vault, which stores usernames and passwords for other websites or programs. The LastPass Vault is accessible by internet or browser extension, enabling the account holder to sign in to one program—LastPass—and then easily access all other password-protected sites or programs without typing in each website's passwords. Because LastPass is an internet or browser extention, use of the

program does not require a local copy of LastPass be maintained on each user's individual computer terminal. In addition to storing passwords, LastPass can also generate new, randomized passwords or audit old and vulnerable passwords stored within the Vault.

28. LogMeIn, Inc. retains Internet Protocol ("IP") logs for each user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on LastPass, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views his/her LastPass account, that user's IP log may reflect the fact that the user viewed the account, and would show when and from what IP address the user did so.

29. Database providers like LogMeIn, Inc. typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, LogMeIn, Inc. users may communicate directly with LogMeIn/LastPass about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Database providers like LogMeIn, Inc. typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

30. LogMeIn, Inc. maintains the following information regarding user accounts, along with other information:

a. **Basic subscriber information**: a LastPass subscriber's name, address, IP logs, username or other subscriber identity, and billing information (if any).

b. **Other non-content records or information**: a user or the user's conduct on LastPass, message headers, user preferences, and certain activity logs.

31. In my training and experience, a social networking user's IP log, stored electronic communications, and other data retained by a provider like LogMeIn, Inc., can indicate who has used or controlled the user's account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the LastPass account at a relevant time. Further, LastPass account activity can show how and when the account was accessed or used. For example, as described herein, LogMeIn, Inc. logs the IP addresses from which users access their accounts 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 account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of LastPass access, use, and events relating to the crime under investigation. Additionally, LastPass and LogMeIn would maintain passwords to sites or

programs regularly visited by a user, including sites primarily utilized for illicit activities, such as cryptocurrency wallets. Lastly, LastPass account activity may provide relevant insight into the LastPass account owner's state of mind as it relates to the offense under investigation. For example, information on the LastPass account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

32. On October 18, 2018, agents sent a preservation request to LogMeIn, Inc., the owner of LastPass, pertaining to all records associated with email account stephan4096@gmail.com. In general, electronic data sent to a LogMeIn, Inc. subscriber is stored in the subscriber's LastPass account information or LogMeIn, Inc. servers until the subscriber deletes the electronic data. If the subscriber does not delete the data, the data can remain on LogMeIn, Inc. servers indefinitely. Even if the subscriber deletes the data, it may continue to be available on LogMeIn, Inc.'s servers for a certain period of time.

33. Therefore, the computers of LogMeIn, Inc. are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of LastPass, such as account access information, transaction information, and other account information.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

34. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using

the warrant to require LogMeIn, 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.

CONCLUSION

35. Based on the forgoing, I request that the Court issue the proposed search warrant relating to the LastPass user account associated with the email stephan4096@gmail.com.

36. Because the warrant will be served on LogMeIn, Inc., 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,

s/Todd Emery

Todd M. Emery
Special Agent
Drug Enforcement Administration

Subscribed and sworn to before me on 1/31, 2018

s/Eric I. Long

The Honorable Eric I. Long
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the user account associated with email **stephan4096@gmail.com** that is stored at premises owned, maintained, controlled, or operated by LogMeIn, Inc., a company headquartered at 323 Summer Street, Boston, Massachusetts.

ATTACHMENT B

Particular Things to be Seized

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

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, and 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 March 29, 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 account, 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 account, 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 all usernames, passwords, 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;

f. All records pertaining to content of private messages between users or communities (e.g. modmail), content of information posted to Services (e.g. text, photos, videos, link), transactional information from purchase of products or services (e.g. LastPass), and information provided directly to LogMeIn, Inc. via forms, contests, sweepstakes, or promotions; and

g. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

The Provider is hereby ordered to disclose the above information to the government within fourteen days of the issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 21 U.S.C. §§ 841(a)(1) and 846 those violations involving Stephan Caamano (email account stephan4096@gmail.com) and occurring after January 1, 2016, to the present, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) "the sale of illegal drugs"; "dark web or dark web marketplaces"; "conversations about Xanax, narcotics, drugs, or any pharmaceutical pills or materials"; "communications between Googleplex and any of the following users: barcentral, alpraking, eastcoastbarbarian, quantikxanax, quantik, galacticagora, candyland134, quanitkusa, lordxanaxusa, secondchanceusername, tote32, xanax empire, pestcontrol1, tiz_time, younginlam, hulkpresser, lexie, jackxcarter, pharmaking, plexiglass, jack, theory of harmony ;" "preparatory steps taken in furtherance of the scheme".

(b) Passwords stored and maintained by LastPass associated with the account linked to stephan4096@gmail.com;

(c) Evidence indicating how and when the 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;

(d) Evidence indicating the account owner's state of mind as it relates to the crime under investigation;

(e) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s);

(f) The identity of the person(s) who communicated with the user ID about matters relating to manufacturing and distributing counterfeit pharmaceuticals/narcotics, including records that help reveal their whereabouts.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by LogMeIn, Inc., and my official title is _____. I am a custodian of records for LogMeIn, Inc.. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of LogMeIn, Inc., and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of LogMeIn, Inc.; and

c. such records were made by LogMeIn, Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

_____ _____

Date Signature