

**IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF TEXAS  
TYLER DIVISION**

**CUMBERLAND SYSTEMS LLC,**

Plaintiff,

v.

**MAINSTREAM TECHNOLOGIES, INC.,**

Defendant.

**CIVIL ACTION NO 6:17-cv-270**

**JURY TRIAL DEMANDED**

**ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT**

1. This is an action for patent infringement in which Cumberland Systems LLC makes the following allegations against Mainstream Technologies, Inc.

**PARTIES**

2. Plaintiff Cumberland Systems LLC (“Plaintiff”) is a Texas limited liability company with its principal place of business at 6800 Weiskopf Avenue, Suite 150, McKinney, TX 75070.

3. On information and belief, Mainstream Technologies, Inc. (“Defendant” or “Mainstream”) is a corporation organized and existing under the laws of the State of Arkansas, with its principal place of business at 325 West Capitol Ave, Suite 200, Little Rock, AR 72201.

**JURISDICTION AND VENUE**

4. This action arises under the patent laws of the United States, Title 35 of the United States Code. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

5. Venue is proper in this district under 28 U.S.C. §§ 1391(c) and 1400(b). On information and belief, Defendant has transacted business in this district, and has committed and/or induced acts of patent infringement in this district.

6. On information and belief, Defendant is subject to this Court's specific and general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

**COUNT I**  
**INFRINGEMENT OF U.S. PATENT NO. 8,023,647**

7. Plaintiff is the owner of United States Patent No. 8,023,647 ("the '647 patent") entitled "Password self encryption method and system and encryption by keys generated from personal secret information." The '647 Patent issued on September 20, 2011. A true and correct copy of the '647 Patent is attached as Exhibit A.

8. Defendant owns, uses, operates, advertises, controls, sells, and otherwise provides products and/or services that infringe the '647 patent. The '647 patent provides, among other things, "A method comprising: submitting a user identification for a user from a user computer to a server computer; receiving a set of information at the user computer from the server computer, in response to the submission of the user identification for the user; wherein the set of information includes a parameter of a key; and further comprising using the user computer to convert user confidential information to a number  $x$ , wherein the number  $x$  is dependent on the user confidential information; using the user computer to compute a number  $e$  which is a function of  $x$  and which is a function of the user confidential information; using the user computer to pad the number  $x$  to convert  $x$  to  $X_p$ ; using the user computer to encrypt  $x_p$  by using the parameter of the key and the number  $e$  to form a cipher  $C$ , wherein  $C$  is a function of the user confidential information; and submitting the cipher  $C$  from the user computer to the server computer."

9. Defendant directly and/or through intermediaries, made, has made, used, imported, provided, supplied, distributed, sold, and/or offered for sale products and/or services that infringed one or more claims of the '647 patent, including at least Claim 1, in this district and elsewhere in the United States. Particularly, the Defendant's use of LastPass Enterprise infringes the '647 patent. By making, using, importing, offering for sale, and/or selling such

products and services, and all like products and services, Defendant has injured Plaintiff and is thus liable for infringement of the '647 patent pursuant to 35 U.S.C. § 271.

10. Based on present information and belief, Mainstream performs the step of submitting a user identification for a user from a user computer to a server computer. For example, Mainstream employees use LastPass Enterprise password manager and a LastPass vault for storing, managing and maintaining passwords. While using LastPass Enterprise, a Mainstream employee necessarily submits a username (email address) and a master password which are entered into a one-way function to create a salted hash. PBKDF2-SHA256 is then used on the salted hash to create a password hash. This password hash is then submitted to a server controlled by LastPass in order for the server to authenticate the employee. Further, upon information and belief, Mainstream administrators activate multi-factor authentication, wherein a Mainstream employee must submit user identification in the form of a hash derived from the combination of user email address and a Master Password as well another form of authentication such as a one time password (OTP).

11. Based on present information and belief, Mainstream performs the step of receiving a set of information at the user computer, wherein the set of information includes a parameter of a key. For example, upon information and belief, Mainstream employees and administrators activate the Super Admin Password Reset functionality provided by LastPass. When activated, Mainstream employees receive at their computer a Mainstream's administrator's RSA-2048 public key of an asymmetric key pair. The private key of the asymmetric key pair is held at the Mainstream's administrator's computer and/or in LastPass's servers. The administrator's public key thus received at the employee's computer is used to encrypt the employee's vault encryption key and thus comprises the claimed parameter of a key. Further, upon information and belief, Mainstream employees and administrators activate the emergency access functionality provided by LastPass. Mainstream employees create one or more emergency contacts who would receive access to the employee's complete vault (containing usernames, passwords, notes, folders, etc.) in case of an emergency and as per criteria set by the employee and/or Mainstream's administrators. Whenever this emergency access is activated, the employee's computer receives a set of information including at least the emergency contact's public key. This public key is used to encrypt the employee's vault encryption key and thus comprises the claimed parameter of a key.

12. Based on information and belief, Mainstream performs the step of using a user computer to convert user confidential information to a number  $x$ , which is dependent on the user confidential information. For example, when Mainstream employees choose a username and Master Password, LastPass uses the employee's computer to convert user confidential information, specifically the employee's master password to a number as part of generating the employee's vault encryption key. Specifically, LastPass's software on the employee's computer uses a combination of AES and PBKDF2-SHA256 algorithms for encrypting the user confidential information in order to derive the employee's vault encryption key. These encryption techniques necessarily include converting information being encrypted into a number dependent on the information being encrypted as both PBKDF2 and AES-256 algorithms operate on numbers. For example, PBKDF2 requires that an HMAC be calculated from the user confidential information. In case of Mainstream and its use of LastPass, a SHA256 based HMAC is calculated from the employee's Master Password.

13. Based on present information and belief, Mainstream uses the user computer to compute a number  $e$  which is a function of  $x$  and which is a function of the user confidential information. For example, Mainstream employees use their computer to encrypt their LastPass vault with a vault encryption key using AES-256 and PBKDF2 SHA-256 encryption algorithms – wherein these algorithms involve computing a number  $e$  which is a function of the number  $x$  above. For example, in the specifications for the PBKDF2 algorithm, numbers such as  $T_i$  and  $mk$  are computed from the HMAC calculation – each thus comprises the number  $e$  that is a function of the HMAC (i.e. claimed number  $x$ ).

14. Based on present information and belief, Mainstream performs the step of using the user computer to pad the number  $x$  to convert  $x$  to  $x_p$ . For example, Mainstream employees use their user computer to pad the MAC of their Master Password up to 256 bits as required by the AES-256 encryption and PBKDF2 with HMAC-SHA256 algorithms.

15. Based on present information and belief, Mainstream performs the step of using the user computer to encrypt  $x_p$  by using the parameter of the key and the number  $e$  to form a cipher  $C$ , wherein  $C$  is a function of the user confidential information. For example, upon information and belief, Mainstream employees and administrators activate the Super Admin Password Reset functionality provided by LastPass. When activated, Mainstream employees use their computer to first derive a vault encryption key from their Master Password (using, as shown

above, the number e) and then encrypt the vault encryption key (using administrator's public key received from the server) to generate an encrypted vault encryption key (claimed cipher C). For example, upon information and belief, Mainstream employees and administrators activate the emergency access functionality provided by LastPass. When activated, Mainstream employees use their computer to first derive a vault encryption key from their Master Password (using, as shown above, the number e) and then encrypt the vault encryption key with their emergency contact's public key (claimed parameter of a key) to generate an encrypted vault encryption key (claimed cipher C). Whenever this emergency access is activated, the employee's computer receives a set of information including at least the emergency contact's public key. This public key is used to encrypt the employee's vault encryption key and thus comprises the claimed parameter of a key.

16. Based on present information and belief, Mainstream submits the cipher C from the user computer to the server computer. For example, a Mainstream employee submits the encrypted vault encryption key (encrypted with the administrator's and/or emergency contact's public key) to the LastPass servers so that the administrator or the emergency contact may be given access to the employee's vault encryption/decryption key if and when necessary.

17. In the alternative, because the manner of use by Defendant differs in no substantial way from language of the claims, if Defendant is not found to literally infringe, Defendant infringes under the doctrine of equivalents.

18. Defendant's aforesaid activities have been without authority and/or license from Plaintiff.

19. In addition to what is required for pleadings in patent cases, and to the extent any marking was required by 35 U.S.C. § 287, Plaintiff and all predecessors in interest to the '647 Patent complied with all marking requirements under 35 U.S.C. § 287.

20. Plaintiff is entitled to recover from Defendant the damages sustained by Plaintiff as a result of the Defendant's wrongful acts in an amount subject to proof at trial, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

#### **PRAYER FOR RELIEF**

WHEREFORE, Plaintiff respectfully requests that this Court enter:

1. A judgment in favor of Plaintiff that Defendant has infringed the '647 Patent;

2. A judgment and order requiring Defendant to pay Plaintiff its damages, costs, expenses, and prejudgment and post-judgment interest for Defendant's infringement of the '647 Patent as provided under 35 U.S.C. § 284;

3. An award to Plaintiff for enhanced damages resulting from the knowing, deliberate, and willful nature of Defendant's prohibited conduct with notice being made at least as early as the date of the filing of this Complaint, as provided under 35 U.S.C. § 284;

4. A judgment and order finding that this is an exceptional case within the meaning of 35 U.S.C. § 285 and awarding to Plaintiff its reasonable attorneys' fees; and

5. Any and all other relief to which Plaintiff may show itself to be entitled.

**DEMAND FOR JURY TRIAL**

Plaintiff, under Rule 38 of the Federal Rules of Civil Procedure, requests a trial by jury of any issues so triable by right.

Respectfully Submitted,

**CUMBERLAND SYSTEMS LLC**

*/s/ Papool S. Chaudhari*

Dated: May 8, 2017

By: \_\_\_\_\_

Papool S. Chaudhari  
Texas State Bar No. 24076978  
Chaudhari Law, PLLC  
P.O. Box 1863  
Wylie, Texas 75098  
Phone: (214) 702-1150  
Fax: (214) 705-3775  
[Papool@ChaudhariLaw.com](mailto:Papool@ChaudhariLaw.com)

**ATTORNEY FOR PLAINTIFF  
CUMBERLAND SYSTEMS LLC**