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

CUMBERLAND SYSTEMS LLC, Plaintiff, **v.** **IREVERSE HOME LOANS, LLC,** Defendant.	**CIVIL ACTION NO 6:17-cv-274** **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 iReverse Home Loans, LLC.

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, iReverse Home Loans, LLC ("Defendant" or "iReverse") is a limited liability company organized and existing under the laws of the State of Maryland, with its principal place of business at the offices of Bay Bank, FSB, 7151 Columbia Gateway Dr, Suite A, Columbia MD 21046.

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 Sookasa products 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, IReverse submits a user identification for a user from a user computer to a server computer. For example, IReverse employees utilize Sookasa's encryption solution for storing, managing and sharing confidential information through a special Sookasa folder on a cloud storage such as one provided by Google Drive or Dropbox. To use Sookasa, IReverse's employees submit a user identification from their computer to a server computer controlled by Sookasa and/or IReverse. This user identification is submitted in the form of at least an email address and a hash of the employee's Master Password. Further, upon information and belief, IReverse may use a multi-factor authentication supported by Sookasa, wherein a IReverse employee submits a user identification, the user identification being a combination of user email address, hash of Master Password and a time-based one-time-password (TOTP).

11. Based on present information and belief, IReverse receives a set of information at the user computer, wherein the set of information includes a parameter of a key. For example, IReverse employees utilize Sookasa's encryption solution for storing, managing and sharing confidential information through a special Sookasa folder on a cloud storage such Google Drive or Dropbox. Further, when a IReverse employee logs into Sookasa and creates a file in the Sookasa folder, upon information and belief, the employee receives at his computer a file key from the Sookasa servers. In addition, the employee also receives either a team master key or a copy of the file key that has been encrypted using a team master key. To the extent the team master key is received by an employee at his computer from Sookasa – the team master key is the claimed parameter of a key. If however the employee does not receive the team master key but instead receives a copy of the file key that has already been encrypted with the master key, the encrypted file key is the claimed parameter of a key.

12. Based on information and belief, IReverse uses the user computer to convert user confidential information to a number x, wherein the number x is dependent on the user confidential information. For example, IReverse employees use their user computer to store and encrypt documents and files on Sookasa for Dropbox and/or Sookasa for Google Drive. Sookasa application converts the content of each file placed in the special Sookasa folder into a number x as part of the AES encryption.

13. Based on present information and belief, IReverse 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, when IReverse employees add a file in the special Sookasa folder, they use their computer to apply at least a MixColumns transformation as part of the AES encryption – the AES algorithm computes a series of numbers (claimed number e) from the numerical representation of the file contents (claimed x).

14. Based on present information and belief, IReverse 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, when IReverse employees add a file in the special Sookasa folder, they apply at least a AddRoundKey() transformation to the numerical representation of the file contents (claimed number x). The AddRoundKey() includes an XOR transformation which results in a padded representation.

15. Based on present information and belief, IReverse uses the user computer to encrypt xp 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, when IReverse employees add a file in the special Sookasa folder, they use their computer to encrypt their file contents (specifically the result of AddRoundKey() transformation) using at least the result of the MixColumns() transformation (claimed number e). Further, using the Sookasa application, they also either encrypt the file key with a team master key or use a copy of the file key that has already been encrypted using the team master key – and embed the encrypted file key within the file. To the extent the team master key is received by an employee at his computer from Sookasa – the team master key is the claimed parameter of a key. If however the employee does not receive the team master key but instead receives a copy of the file key that has already been encrypted with the master key, the encrypted file key is the claimed parameter of a key. In either case, the parameter of a key so received is used along with the claimed number e to encrypt the file, resulting in an encrypted file (claimed cipher C).

16. Based on present information and belief, IReverse submits the cipher C from the user computer to the server computer. Depending on which cloud storage is used by IReverse, such as Dropbox and Google Drive, IReverse submit the encrypted files in the special Sookasa folder to Dropbox and/or Google Drive servers.

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

Dated: May 8, 2017

By: */s/ Papool S. Chaudhari*
_____

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

ATTORNEY FOR PLAINTIFF
CUMBERLAND SYSTEMS LLC