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

PLANO ENCRYPTION TECHNOLOGIES, LLC, Plaintiff, **v.** **ALKAMI TECHNOLOGY, INC.,** Defendant.	**Case No. 2:16-cv-1032-JRG** **JURY TRIAL DEMANDED**

FIRST AMENDED COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Plano Encryption Technologies, LLC, by and through its attorneys, alleges as follows:

PARTIES

1. Plano Encryption Technologies, LLC ("Plano Encryption") is a limited liability company organized and existing under the laws of the State of Texas, with its principal place of business at 903 E. 18th Street, Suite 224, Plano, Texas 75074.

2. Upon information and belief, Defendant Alkami Technology, Inc. ("Defendant" or "Alkami"), is a Delaware corporation, with its headquarters and principal place of business at 5601 Granite Parkway, Suite 120, Plano, Texas 75024.

JURISDICTION AND VENUE

3. This is an action for patent infringement arising under the patent laws of the United States, Title 35 of the United States Code. This Court has jurisdiction over the subject matter of this action under 28 U.S.C. §§ 1331 and 1338(a).

4. Venue is proper in the Eastern District of Texas under 28 U.S.C. §§ 1391(b) and (c) and 1400(b) because Defendant resides within this district, has committed acts and/or induced acts of patent infringement within this judicial district giving rise to this action, and/or Defendant continues to conduct business in this judicial district, including one or more acts of selling, using, offering for sale, licensing and/or distributing infringing products or providing service and support to Defendant's customers in this District.

5. This Court has personal jurisdiction over Defendant for at least the following reasons: (i) Alkami's principal place of business is in this District and in this State; (ii) Alkami has committed acts of patent infringement and/or induced acts of patent infringement by others in this District and this State and continues to do so; (iii) Alkami regularly does business or solicits business, engages in other persistent courses of conduct, and/or derives substantial revenue from products and/or services provided to its customers in this District and in this State; (iv) Alkami has purposefully established substantial, systematic and continuous contacts with this State and District and expects or should reasonably expect to be subjected to this Court's jurisdiction.

BACKGROUND

6. Plaintiff Plano Encryption is the owner by assignment of United States Patent No. 5,991,399 ("the '399 Patent" or "Patent-In-Suit"), issued November 23, 1999, for "Method for Securely Distributing a Conditional Use Private Key to a Trusted Entity on a Remote System." A true and correct copy of the '399 Patent was previously attached to the Original Complaint as Exhibit A.

7. Plano Encryption is the owner by assignment of United States Patent No. 5,974,550 ("the '550 Patent") entitled "Method for Securely Authenticating Another Process in a

Different Address Space." The '550 Patent issued on October 26, 1999. A true and correct copy of the '550 Patent was previously attached to the Original Complaint as Exhibit B.

8. Plano Encryption holds all right, title and interest in the '399 Patent and the '550 Patent (collectively, the "Asserted Patents" or "Patents-in-Suit"), including all rights to bring suit and recover for all past, present and future infringements thereof.

9. The invention of the '399 Patent relates to methods used to secure communications between parties. The '399 Patent represents fundamental technology in the field of encryption and secured online data communications. The '399 Patent has been referenced hundreds of times by other patents and patent applications. Nearly every computer company of any prominence has cited the patent more than once during prosecution of their own patents, including leaders in the field of software and computing, such as Microsoft (more than 75 citations) and IBM (more than 20 citations). The patent has also been cited as prior art by U.S. Patent Examiners more than 150 times during the prosecution of other patents.

10. The invention of the '550 Patent also relates to methods and apparatuses used to secure communications between parties. The '550 Patent has also been cited many times by leaders in the fields of software and computing.

11. Various terms of the '399 and '550 patents were construed by this Court on July 22, 2016. *Plano Encryption Techs., LLC v. Am. Bank of Tex. et al.*, Case No. 2:15-cv-1273-JRG, (lead case), Dkt 104. For purposes of this complaint, the claims have been interpreted in light of those constructions.

12. Alkami is in the business of making, selling, offering to sell, licensing and distributing secure, mobile and online banking software solutions, including mobile banking applications products and services, such as, upon information and belief, the mobile apps for

Inspirus Credit Union, available at https://itunes.apple.com/us/app/school-employees-credit-union/id464447129?mt=8 (for iOS) and https://play.google.com/store/apps/details?id=com.ifs.banking.fiid8022 (for Android).

13. Alkami's mobile banking application products and services ("mobile applications" or "mobile apps"), are specifically developed, marketed, licensed and distributed by Alkami to be downloaded onto Apple iOS or Android-enabled mobile or tablet devices. Upon information and belief, Alkami is liable for directly infringing the Asserted Patents because it forms a joint enterprise with Apple and Google respectively with respect to building and distributing its mobile apps, such that to the extent that any infringing steps are performed by Apple/Google, these acts are attributable to Alkami.

14. Upon information and belief, there are numerous express and implied agreements between Alkami and Apple regarding its mobile apps. *See*, Apple Developer Agreement, https://developer.apple.com/programs/terms/apple_developer_agreement.pdf; *see also*, iOS Developer Program License Agreement, https://developer.apple.com/programs/terms/ios/standard/ios_program_standard_agreement_20140909.pdf.

15. Upon information and belief, there is a common purpose between Alkami and Apple regarding its mobile apps, namely to develop and distribute mobile apps for use by customers of Apple's smartphone products.

16. Upon information and belief, Alkami and Apple share a community of pecuniary interests in the development and distribution of mobile apps. For example, upon information and belief, there are express revenue sharing provisions in certain circumstances, as set forth in the agreements between the two companies. *See*, iOS Developer Program License Agreement

https://developer.apple.com/programs/terms/ios/standard/ios_program_standard_agreement_20140909.pdf. Upon information and belief, both Alkami and Apple derive financial benefit from the development and distribution of Alkami's mobile apps.

17. Upon information and belief, both Alkami and Apple have an equal right to a voice in the direction of the enterprise, which gives an equal right of control. Pursuant to the agreements between the parties, Alkami has the right to control the mobile app, since the mobile app cannot be built or uploaded without Alkami's consent. Alkami also has the right to remove the mobile apps from Apple's distribution network pursuant to the terms and conditions of their agreements. *Id.* Likewise, upon information and belief, Apple has the right to remove mobile apps, including Alkami's, from its distribution network. *Id.* Indeed, upon information and belief, Apple has purged thousands of mobile apps from its app store "that no longer worked as intended or didn't follow guidelines from the App Store." *See* http://www.digitaltrends.com/mobile/apple-app-store-purge-beginning/#ixzz4QNeOkqbD.

18. Upon information and belief, even if Apple and Alkami are not found to be in a joint enterprise, equity would demand liability for the acts of the other given their close and pervasive express and implied agreements, common interest, shared pecuniary interest and shared control over the mobile apps.

19. Alternatively, upon information and belief, Alkami is liable for the acts of Apple with respect to its mobile apps, since upon information and belief, Alkami has expressly agreed that Apple serves as its agent for purposes of marketing and distributing its mobile apps, and has agreed that Alkami is responsible for infringement of any third party intellectual property rights with respect to Alkami's mobile apps. *See, e.g.,* Schedule 1, iOS Developer Program License Agreement

https://developer.apple.com/programs/terms/ios/standard/ios_program_standard_agreement_20140909.pdf.

20. Similarly, on information and belief, there are numerous express and implied agreements between Alkami and Google concerning the development and distribution of Alkami's mobile apps. Alkami must sign in and register with Android Developer Console, enter into a Developer Distribution Agreement with Google, and pay a registration fee in order to develop and distribute mobile apps through the Google Play Store for download by users onto an Android mobile device or tablet. *See, e.g.*, Google Play Developer Console Signup Webpage, https://play.google.com/apps/publish/signup/; and Google Developer Distribution Agreement, https://play.google.com/about/developer-distribution-agreement.html.

21. Upon information and belief, there is a common purpose between Alkami and Google regarding its mobile apps, namely to develop and distribute mobile apps for use by customers of Google's Android smartphone products.

22. Upon information and belief, Alkami and Google share a community of pecuniary interests in the development and distribution of mobile apps. For example, upon information and belief, there are express revenue sharing provisions in certain circumstances, as set forth in the agreements between the two companies. *See,* Google Developer Distribution Agreement, https://play.google.com/about/developer-distribution-agreement.html. Upon information and belief, both Alkami and Google derive financial benefit from the development and distribution of Alkami's mobile apps.

23. Upon information and belief, both Alkami and Google have an equal right to a voice in the direction of the enterprise, which gives an equal right of control. Pursuant to the agreements between the parties, Alkami has the right to control its mobile apps, since its mobile

apps cannot be built or uploaded without Alkami's consent. Alkami also has the right to remove its mobile apps from Google's distribution network pursuant to the terms and conditions of their agreements. Likewise, upon information and belief, Google has the right to remove Android compatible mobile apps, including Alkami's, from distribution network. *See id.*

24. Upon information and belief, even if Google and Alkami are not found to be in a joint enterprise, equity would demand liability for the acts of the other given their close and pervasive express and implied agreements, common interest, shared pecuniary interest and shared control over the mobile apps.

25. Alternatively, upon information and belief, Alkami is liable for the acts of Google with respect to its mobile apps, since upon information and belief, Alkami has acknowledged and agreed that Google acts on behalf of Alkami for purposes of displaying, marketing and distributing its mobile apps, and that Alkami is responsible for infringement of any third party intellectual property rights. *See id*.

26. Between May and July of 2015, Plaintiff began giving notice to various customers of Alkami (including Empower Federal Credit Union and Idaho Central Credit Union) of Plano Encryption's rights in the Patents-in-Suit. Thus, on information and belief, Alkami has been aware of the Patents-in-Suit when Plaintiff provided notice to Defendant's customers, and at the very least, as of the date the Original Complaint was served on Defendant. Thus, upon information and belief, Alkami has had notice and actual or constructive knowledge of the Patents-in-Suit.

27. Moreover, upon information and belief, Alkami's joint enterprise partners and/or contractual agents Apple and Google were certainly aware of the Asserted Patents prior to the filing of this complaint. Upon information and belief, the website www.google.com/patents is

owned and run by Google. Upon information and belief, according to that website, the '399 Patent has been cited over 800 times by other patents and patent applications during prosecution.

28. Upon information and belief, the '399 Patent has been cited by either Google or the examiner in patents or patent applications owned or assigned to Google approximately fifty times. Upon information and belief, many of these patents and applications were related to encryption and/or distribution of encrypted information or software. Upon information and belief, the '399 Patent has been cited by either Apple or the examiner in patents or patent applications owned or assigned to Apple approximately 8 times. Upon information and belief, some of these patents and applications were related to encryption and/or distribution of encrypted information or software.

29. Upon information and belief, the acts, knowledge and intent of Google and Apple as alleged herein and detailed further below, should be imputed to Alkami since Google and Apple are agents or act on behalf of Alkami for purposes of building, distributing and marketing Defendant's mobile apps.

30. Furthermore, upon information and belief, Defendant as the developer of its mobile apps is permitted by contract to notify Apple and/or Google of any intellectual property claims, and to request the take-down of its apps from the app store when subject to an infringement claim, but apparently has not done so. Moreover, as previously alleged, Alkami has agreed to be responsible for infringement of any intellectual property right with respect to its mobile apps. Upon information and belief, in light of Defendant's knowledge and awareness of the Patents-in-Suit and PET's infringement claims, its ongoing infringement has been willful.

31. For all the above reasons, Alkami has been and continues to willfully infringe the '399 patent.

32. Even if Alkami is not somehow liable for direct infringement, upon information and belief, Apple conditions both the manner and timing of the performance of steps by Alkami in building and distributing its mobile apps, and is thus liable for direct infringement of the '399 Patent, as set forth below.

33. Upon information and belief, even if not liable as a direct infringer, Alkami is liable for inducing Apple's infringement.

34. Upon information and belief, prior to uploading its mobile apps to the Apple or Google platforms, and before Alkami can distribute its iOS and Android compatible mobile apps (the "Accused Products") on the Apple App Store and Google Play Store for download on iOS or Android mobile or table devices, Alkami must follow certain mandatory developer guidelines, procedures, terms and conditions as set forth and dictated by Apple and Google respectively. In this way, on information and belief, Apple and Google condition participation in, and the receipt of the benefit namely, the ability to distribute Alkami's apps on the Apple App Store and Google Play Store, upon compliance with certain procedures and guidelines for the development, building and uploading of Alkami's apps. *See e.g.*, App Developer Program, https://developer.apple.com/programs/ and App Distribution Guide, https://developer.apple.com/library/content/documentation/IDEs/Conceptual/AppDistributionGuide/Introduction/Introduction.html.

35. By way of example, and on information and belief, in order to participate as an Apple Developer, Alkami must enroll in the Apple Developer Program, agree to the terms and conditions of the Apple Developer Agreement and pay Apple an annual non-refundable program fee to participate in the Apple Developer Program, as consideration for the rights and licenses. granted to Alkami by Apple. *See, e.g.*, Apple Developer Agreement,

https://developer.apple.com/programs/terms/apple_developer_agreement.pdf. By agreeing to the terms and conditions of the Apple Developer Agreement, Alkami receives certain developer benefits and resources provided by Apple, that are necessary for the development of iOS compatible apps including software, documentation, tools, and licenses thereto, for app development and testing, and such other content, materials, resources and services including application programmer interfaces (APIs) for iOS technologies such as Wallet, Apple Pay, in-App Purchases, Data Protection, Background Modes, etc., developer guides, API references, and technical notes as provided on the Apple developer website.

36. On information and belief, in order to release its apps on the Apple App Store for distribution to end users, Alkami must further enter into additional agreements with Apple including but not limited to an iOS Developer Program License Agreement. *See*, https://developer.apple.com/programs/terms/ios/standard/ios_program_standard_agreement_20140909.pdf. On information and belief, Alkami must also meet Apple's Documentation and Program Requirements, which may be modified from time to time by Apple, before it can submit its mobile apps for consideration by Apple for distribution via the App Store. On information and belief, Alkami must also further agree pursuant to the iOS Developer Program License Agreement that Apple may cease distribution of Alkami's mobile apps at any time. On information and belief, pursuant to Schedule 1 of the iOS Developer Program License Agreement, Alkami designates Apple as its agent for the marketing and end-user download of its mobile apps in the United States. *Id.* Once selected by Apple for distribution on the Apple App Store, Alkami's mobile apps may be downloaded onto mobile devices for use by its customers' retail and commercial account holders. Alkami's mobile apps allow users to access, engage and

complete financial transactions with its customers' servers from the users' mobile or tablet devices.

37. Similarly, on information and belief, Alkami must sign in and register with Android Developer Console, enter into a Developer Distribution Agreement with Google, and pay a registration fee in order to develop and distribute mobile apps through the Google Play Store for download by users onto an Android mobile device or tablet. *See, e.g.*, Google Play Developer Console Signup Webpage, https://play.google.com/apps/publish/signup/; and Google Developer Distribution Agreement, https://play.google.com/about/developer-distribution-agreement.html. On information and belief, any mobile apps distributed through Google Play Store, must adhere to Google's Developer Program Policies and follow the procedures and guidelines for developing, uploading and distributing mobile apps dictated by Google as set forth in the Android Developer Console. Google further reserves the right to take down Alkami's mobile apps, under certain conditions at its discretion. *See* Google Developer Distribution Agreement, https://play.google.com/about/developer-distribution-agreement.html.

38. Accordingly, on information and belief, any steps or acts performed by Alkami, are attributable to Apple and Google respectively, who condition participation in and the receipt of a benefit, namely, the distribution of Alkami's iOS and Android compatible mobile apps through the Apple App Store and the Google Play Store, upon compliance with certain mandatory procedures and guidelines dictated by Apple and Google respectively in the building and upload of Alkami's mobile apps, and Alkami induces infringement by Apple and/or Google respectively in the building, marketing and distribution of Alkami's mobile apps.

39. Alkami actively distributes and promotes its mobile applications for use by its customers' retail and commercial account holders on their mobile or tablet devices. In doing so,

Alkami actively markets and widely touts the importance of the security of its mobile application solutions.

40. With knowledge of the Patents-in-Suit, Alkami intentionally makes, sells, offers to sell, licenses and distributes its mobile applications, whether directly, or through intermediaries, to customers in the Eastern District of Texas with the intention that its mobile apps are to be downloaded for use on Android and iOS operating systems as found and used in all Android and iOS smart phones and tablets.

41. On information and belief, Alkami has been, among other things, purposefully, actively, and voluntarily making, selling, offering for sale, using, licensing and/or distributing infringing products and services, including but not limited to, its mobile applications products and services, with the expectation that they will be distributed, licensed and/or used by consumers after downloading the same onto their mobile devices. Customized versions of its mobile applications have been and continue to be developed, purchased, used, licensed and distributed onto the Android and Apple app stores in the Eastern District of Texas, and downloaded and used by their customers' account holders both in and outside of the Eastern District of Texas. Alkami has thus committed acts of patent infringement within the State of Texas and in this District and/or is inducing others to use, license and/or distribute its products and services in an infringing manner. By purposefully and voluntarily distributing one or more of its infringing products and services, Alkami has injured Plano Encryption and is thus liable to Plano Encryption for infringement of the Patents-in-Suit at issue in this litigation.

42. On information and belief, through its actions Alkami has infringed the Asserted Patents and actively promoted others to infringe the Patents-in-Suit, inducing acts of patent infringement by others through its use, sale, offer for sale, licensing and distribution of products

and services, including but not limited to, its mobile applications, including at least customized versions of its mobile banking products and services.

43. On information and belief, Alkami has been and now is directly infringing in the State of Texas, within this judicial district, and elsewhere in the United States, by, among other things, making, selling, offering to sell, licensing and distributing its mobile applications, which infringe one or more claims of the Patents-in-Suit, including at least claims 1 and 34 of the '399 Patent and claims 10 and 20 of the '550 Patent. Defendants are thus liable for infringement of the Patents-in-Suit pursuant to 35 U.S.C. § 271. Alkami not only makes, sells, offers to sell, leases, licenses and distributes software solutions practicing these claims, it induces infringement through the sale, offer for sale, lease, licensing and distribution of software solutions hosted by its customers.

44. Plaintiff Plano Encryption has been and will continue to suffer damages as a result of Defendant's infringing acts.

45. Plaintiff Plano Encryption seeks monetary damages and prejudgment interest for Defendant's past and ongoing infringement of the Patent-in-Suit.

46. The allegations set forth herein with respect to each asserted patent claim, each accused product, and each specific accused feature are exemplary. Plaintiff Plano Encryption reserves the right to assert additional claims, accuse additional products, and accuse additional features.

COUNT ONE

INFRINGEMENT OF U.S. PATENT NO. 5,991,399

47. Plaintiff Plano Encryption realleges and incorporates herein the preceding paragraphs of its Complaint.

48. On information and belief, Defendant has infringed and continues to infringe one or more claims of the '399 Patent pursuant to 35 U.S.C. § 271(a), literally or under the doctrine of equivalents, by practicing the methods of claims 1 and 34, without limitation, in connection with its mobile products and applications, as described in more detail herein.

49. Defendant's infringement is and has been willful, deliberate and intentional. On information and belief, and as stated above, Defendant had pre-suit knowledge of the '399 Patent no later than May or June 2015, and certainly by the service date for the Original Complaint in this action. Alkami has acted and continues to act in disregard of the high likelihood that its actions constitute direct and indirect infringement of a valid patent, and knew or should have known of that objectively high risk.

50. Defendant has directly infringed and/or has knowingly induced and continues to induce Apple and/or Google, and/or users of mobile devices (in each case depending on the asserted patent claim) to infringe one or more claims of the '399 Patent, including, at least, and as an example, claims 1 and 34, by intentionally developing, making, marketing, advertising, providing, distributing and licensing its mobile applications software, documentation, materials, training or support and aiding, abetting, encouraging, promoting or inviting use thereof.

51. As set forth above, on information and belief, to the extent any steps identified herein are performed by Apple/Google, such acts are attributable to Alkami (i) because Alkami works together with Apple and Google respectively in a joint enterprise in the building and distribution of its iOS and Android compatible mobile apps, or (ii) because Apple and Google distribute and market Alkami's mobile apps under the direction and control of Alkami, or act as agents, or on behalf of Alkami, in the building, marketing and distribution of Alkami's mobile apps.

52. Alternatively, on information and belief, any steps or acts performed by Alkami, are attributable to Apple and Google respectively, who condition participation in and the receipt of a benefit, namely, the distribution of Alkami's iOS and Android compatible mobile apps through the Apple App Store and the Google Play Store, upon compliance with certain mandatory procedures and guidelines dictated by Apple and Google respectively in the building and upload of Alkami's mobile apps, and Alkami induces infringement by Apple and/or Google respectively in the building, marketing and distribution of Alkami's mobile apps.

53. Claim 1 requires "generating an asymmetric key pair having a public key and a private key." Upon information and belief, Alkami in certain instances and Apple/Google, in other instances, generates and/or uses generated asymmetric key pairs that have a public key and a private key. Alkami both generates and uses key pairs generated by Apple/Google both to securely send data related to its mobile app, and to digitally code-sign its mobile app to make it resistant to modification.

54. Claim 1 further requires "encrypting predetermined data with the generated public key." This step is performed, for example, at least, when predetermined data, such as the pre-master secret, is encrypted with a public key matching a private key held by Apple/Google as part of the process for uploading Alkami's mobile apps onto Apple/Google servers securely by SSL/TLS. To make a secure SSL/TLS connection to an HTTPS URL, the requesting device (for example, a computer used to build mobile apps) must first perform an SSL handshake with the HTTPS server. This SSL handshake requires predetermined data such as the pre-master secret to be encrypted with a public key that matches a private key held at the server hosting the HTTPS URL. If the predetermined data encrypted by the public key did not match the private key at the server, the server could not decrypt the predetermined data used to build the mobile app securely.

55. Claim 1 further requires "building an executable tamper resistant key module identified for a selected program, the executable tamper resistant key module including the generated private key and the encrypted predetermined data." For example, each of Alkami's mobile apps is an executable tamper resistant key module at least in part because it is designed to work with other software, namely the iOS/Android operating system as well as other applications or programs installed on a user's mobile device; because the mobile app is resistant to observation and modification, as explained below; and because in building each Alkami mobile app on the Apple/Google platforms, each app during SSL transmission includes at least the claimed generated private key and the encrypted predetermined data such as the pre-master secret encrypted with the claimed generated public key when the mobile app is securely uploaded onto the Apple/Google servers.

56. On information and belief, Alkami and/or Apple/Google builds each mobile app to be tamper resistant, in particular resistant to both observation and modification. On information and belief, Alkami's mobile apps are resistant to observation, for example and at least in part, since Alkami compiles its mobile app source code before submitting the app to Apple/Google – and uploads the binary output of the compilation process rather than the source code itself.

57. On information and belief, Alkami builds mobile apps that are made further resistant to observation, for example and at least in part, because the mobile app is securely sent by SSL/TLS to Apple/Google as part of the building process. Both iTunes Connect portal (https://itunesconnect.apple.com) and Android Developer Console (https://play.google.com/apps/publish/) establish SSL/TLS communications when uploading Alkami's apps onto these respective platforms, as evidenced by the "https" in their URLs.

Sending the mobile app code by SSL/TLS is necessary to keep the code from being observed in transit from the code developer to Apple/Google. This step is required by each of Apple/Google in order to upload Alkami's mobile apps onto the Apple/Google App Stores.

58. On information and belief, Alkami builds each mobile app so that it is resistant to modification, at least in part and by way of example, because the app binary is code signed. Both Apple and Google require that each developer code sign each mobile app submission with his/her asymmetric developer key that certifies that the app has not been modified by a third party.

59. On information and belief, Alkami's mobile apps contain files such as the file _CodeSignature/CodeResources in Alkami's iOS apps and the files CERT.SF and CERT.RSA in Alkami's Android apps – all of which are generated during the code signing process.

60. Upon information and belief, asymmetrical key cryptography and hashing algorithms are used to create the unique digital signature for Android and iOS mobile apps. Upon information and belief, the digital signature is used to sign the resources in an application package, including the binary file. Upon information and belief, the private key of an asymmetric key pair that is generated for the digital code signing is used to code sign the app.

61. On information and belief, Alkami and/or Apple/Google builds each mobile app comprising a tamper resistant key module where each app includes several keys "used for secure communications" including, by way of example, at least the following: (1) the claimed private key used to upload Alkami's mobile apps onto the Apple/Google servers; (2) the claimed public key used to encrypt predetermined data during the upload of Alkami's mobile apps onto the Apple/Google servers, as well as a public key used to communicate securely with servers during operation of the mobile app; (3) the private key used to digitally sign the app code; and/or (4) the

symmetric key negotiated as part of the SSL/TLS process which is used, for example, to securely upload Alkami's mobile apps onto the Apple/Google servers, as well as the symmetric key used to communicate securely with servers during operation of the mobile app.

62. On information and belief, Alkami and/or Apple/Google builds each of its mobile apps, for example, such that each app is identified for a selected program, namely the iOS or Android operating system on a remote mobile device. As set forth above, on information and belief, the acts of Alkami and Apple/Google are attributable to each other respectively because Alkami works together with Apple and Google respectively in a joint enterprise in the building and distribution of its mobile apps. Alternatively, on information and belief, any steps performed by or acts of Apple/Google are attributable to Alkami because Apple and Google distribute and market Alkami's mobile apps under the direction and control of Alkami, or act as agents, or on behalf of Alkami, in the building, marketing and distribution of Alkami's mobile apps. Alternatively, on information and belief, any steps or acts performed by Alkami, are attributable to Apple and Google respectively, who condition participation in and the receipt of a benefit, namely, the distribution of Alkami's iOS and Android compatible mobile apps through the Apple App Store and the Google Play Store, upon compliance with certain mandatory procedures and guidelines dictated by Apple and Google respectively in the building and upload of Alkami's mobile apps, and/or, Alkami induces infringement by Apple and/or Google respectively in the building, marketing and distribution of Alkami's mobile apps. Thus, for at least these reasons, Alkami directly infringes or induces infringement of claim 1 of the '399 Patent.

63. Claim 34 is similar to claim 1, except that claim 34 requires "building an executable tamper resistant key module identified for a selected program resident on a remote

system, the executable tamper resistant key module including a private key of the asymmetric key pair and the encrypted data," but does not require the "generating" of asymmetric keys nor does it require encrypting "predetermined data." Here, for example, at least the selected programs, namely the Android and iOS operating systems, are resident on a remote system, *i.e.*, the mobile device. Moreover, the building step includes a private key and encrypted data because of the SSL handshake, as explained above with respect to claim 1.

64. Moreover, claim 34 requires "sending the executable tamper resistant key module to the remote system." On information and belief, Alkami builds its mobile apps so that the mobile app can be sent to the user via download onto the remote system, for example, at least, on a user's mobile device. The apps are sent to the remote system every time an iOS/Android mobile user selects the Alkami app for download. This downloading is also performed securely over SSL/TLS, and includes a private and public asymmetric key, as well as a symmetric key.

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

66. While, on information and belief, parts of these steps may be performed by third parties, namely Apple/Google (and/or their agents and third parties under their direction and control), these acts are attributable to Alkami, and Alkami is liable for the performance of all the steps of the claimed methods. By way of example, on information and belief, Alkami and Apple/Google are engaged in a joint enterprise, in the distribution of Alkami's mobile apps through the Apple App Store and Google Play Store. Alternatively, on information and belief, (i) any steps performed by Apple/Google in the building, marketing and distribution of iOS and Android compatible mobile apps respectively, are done as agents, at the direction and control,

and on behalf of Alkami, (ii) Apple and/or Google conditions participation in, and receipt of the benefit of marketing and distributing apps on the Apple App Store and Google Play Store, upon compliance with certain procedures and guidelines in the building and distribution of its mobile apps, and/or (iii) Alkami induces infringement by Apple and/or Google respectively in the building and distribution of Alkami's mobile apps. Upon information and belief, under any of these theories, Google and Apple specifically intend to infringe at least the '399 Patent by advertising and promoting the use and distribution of mobile apps through their app store, and requiring mobile app developers including Defendant to include a private key and encrypted predetermined data in the building of mobile apps to be made available by Apple and Google on their respective app stores.

67. To the extent that third parties Apple/Google are deemed to directly infringe, Alkami is liable for inducement of those steps by creating and uploading the code, as well as advertising and promoting the creation, development, distribution and use of its mobile apps.

68. Defendant's infringement is willful, deliberate and intentional at least as of the filing date of this Complaint.

69. Defendant is thus liable for infringement of the '399 Patent pursuant to 35 U.S.C. § 271.

70. Defendant's aforementioned acts have caused damage to Plano Encryption in the past and will continue to do so in the future.

COUNT TWO

INFRINGEMENT OF U.S. PATENT NO. 5,974,550

71. Plaintiff Plano Encryption realleges and incorporates herein the preceding paragraphs of its Complaint.

72. On information and belief, Defendant has directly infringed and continues to infringe one or more claims of the ‘550 Patent, including at least, and as an example, claims 10 and 20 of the ‘550 Patent by making, using, testing, leasing, selling, licensing, offering for sale within the United States apparatuses or instrumentalities practicing and/or embodying the invention within the United States.

73. On information and belief, Alkami develops its customized mobile applications for its customers using an apparatus as described by claim 10 and on one or more machine readable mediums having stored therein a plurality of machine readable instructions designed to be executed by a processor as described by claim 20, with the intention that the mobile apps be distributed through the Apple iOS App Store and the Google Android Play Store for download onto an Apple iOS or Android-enabled mobile tablet or device for use in connection with iOS or Android operating software. Accordingly, on information and belief, and as previously described herein, Alkami directly infringes, and/or induces infringement by Apple and/or Google for certain claims, and/or induces infringement by end-users for other claims of the ‘550 Patent.

74. On information and belief, Alkami’s mobile apps are intended for download onto mobile devices with iOS and Android-compatible operating systems, where the mobile device must have a processing unit for executing programming instructions storage medium and a local storage media which stores instructions to be executed by the mobile device processor for receiving downloads.

75. On information and belief, once downloaded, Alkami’s mobile apps may be used, for example, by its customers’ retail or commercial account holders to conduct secure financial transactions from the account holder’s mobile tablet or device.

76. Claim 10 begins "An apparatus for authenticating a first process operating in an address space different than that of a second process comprising . . ." To the extent the preamble is limiting, Alkami at least makes or uses an apparatus for authenticating a first process operating in an address space different than that of a second process. Upon information and belief, the apparatus authenticates a first process (on a mobile device) which operates in an address space (memory locations on the mobile device) which is different from the address space of the second process (memory locations used by software executed on the Alkami servers and the Apple/Google servers that make the Alkami mobile app available for download).

77. Claim 10 requires "a processing unit for executing programming instructions" which exists on the computers, servers and mobiles devices involved in the making and use of the infringing apparatus.

78. Claim 10 also requires "and a storage medium having stored therein a plurality of programming instructions of the second process to be executed by the processing unit." Again, this element exists on the computers, servers, and mobile devices involved in the making and use of the infringing apparatus.

79. Claim 10 further requires "wherein when executed, the plurality of programming instructions create a tamper resistant module containing a secret." The computers used in the development of the mobile app have programming instructions, that when executed, create a tamper resistant module. Upon information and belief, the mobile app is a tamper resistant module for at least the reasons previously set forth. The mobile app contains several secrets, including the code as a whole. Specifically, as per the SSL/TLS protocol, the mobile app contains multiple secrets, which are later used to encode communications between the server and

the mobile device, namely the cipher suite, the key exchange algorithm, pre-master SSL/TLS secret and/or the algorithm used to derive the pre-master secret.

80. Claim 10 further requires that the apparatus "create a challenge." On information and belief, Alkami creates a challenge in connection with each of its mobile apps, including by way of example, at least prompts for a username/password.

81. Claim 10 further requires the apparatus to "send the tamper resistant module and the challenge to the first process." The first process is the process running at the mobile devices. Both the tamper resistant module and the challenge are sent to the mobile device.

82. Claim 10 also requires that the apparatus "receive a response to the challenge from the first process." A response to the challenge (namely, the requested information) is sent to a server from the response.

83. Finally, claim 10 requires the apparatus to "decode the response." Since all communications regarding the Alkami mobile apps are encrypted by at least SSL, the response to the challenge must be decoded.

84. Claim 20 begins "A machine readable medium having stored therein a plurality of machine readable instructions designed to be executed by a processor, the machine readable instructions for . . . " The processes described below, for example, are all performed by one or more processors with typical storage devices that have multiple instructions.

85. Claim 20 requires "creating a tamper resistant module containing a secret . . ." On information and belief, and as described above, Alkami creates each of its mobile apps as a tamper resistant module. For example, each Alkami mobile app is software designed to work with other software, including at least the iOS or Android mobile operating system.

Furthermore, as recited above for example, the mobile app is resistant to observation and modification.

86. On information and belief, each Alkami mobile app contains many secrets, such as, for example, at least those used during the SSL/TLS protocol, which is used to encode communications between the server and the mobile device, namely the cipher suite, the key exchange algorithm, pre-master SSL/TLS secret and/or the algorithm used to derive the pre-master secret. On information and belief, as described above for example, the mobile app source code itself is also a secret in that only the binary code is uploaded onto the Apple and Google servers.

87. Claim 20 requires "creating a challenge . . ." On information and belief, Alkami creates a challenge in connection with each of its mobile apps, including by way of example, at least prompts for a username/password.

88. Claim 20 requires "sending the tamper resistant module and the challenge to a remote process . . . " On information and belief, each Alkami mobile app (which as described above comprises a tamper resistant module) and the challenge are sent to a remote process, such as, for example, the processes (including the Android/iOS platform) running on the remote mobile device.

89. Claim 20 requires "receiving a response to the challenge from the remote process . . ." On information and belief, a response to the challenge (for example, the username and password) are received from the remote process such as the processes running on the mobile device.

90. Finally, claim 20 requires "decoding the response." On information and belief, responses must be decoded, for example at least in part, since all communications are secured by SSL/TLS.

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

92. While parts of the accused infringing apparatus or storage mediums may be owned or controlled by third parties Apple/Google and/or end-users, upon information and belief, those actions are nonetheless attributable to Alkami, such that Alkami is liable. For example, on information and belief, the acts of Alkami and Apple/Google are attributable to each other respectively because, *inter alia,* Alkami works together with Apple and Google respectively in a joint enterprise in the building and distribution of its mobile apps. Alternatively, on information and belief, (i) Alkami works at the direction and control of Apple and Google respectively, in the building and distribution of iOS and Android compatible mobile apps, (ii) Alkami directs and controls, Apple and/or Google respectively, who act as agents of, or on behalf of, Alkami in the building and distribution of its mobile apps, and/or (iii) Alkami induces infringement by Apple and/or Google respectively in the building and distribution of Alkami's mobile apps.

93. To the extent that third parties, namely Apple and/or Google with respect to certain claims and/or users of the mobile device with respect to other patent claims, are deemed to directly infringe, Alkami is liable for inducement of those steps by, for example, creating and uploading the code, as well as advertising and promoting the creation, development, distribution and use of its mobile apps.

94. Defendant's infringement is willful, deliberate and intentional, as of May or June 2015 as stated above, or at the very least, as of the date the Original Complaint was served. Also, as alleged in detail above, Defendant should be liable for the knowledge of Google and/or Apple. Defendant continues to knowingly induce users of mobile devices to infringe the '550 Patent, including by intentionally developing, making, marketing, advertising, providing, distributing and licensing the software, documentation, materials, training or support and aiding, abetting, encouraging, promoting or inviting use thereof.

95. Defendant is thus liable for infringement of the '550 Patent pursuant to 35 U.S.C. § 271.

96. Defendant's aforementioned acts have caused damage to Plano Encryption in the past and will continue to do so in the future.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that this Court enter judgment and provide relief as follows:

97. That Alkami has directly infringed the Patents-in-Suit literally and/or under the doctrine of equivalents;

98. That Alkami is liable for knowledge of the Patents-in-Suit;

99. That Alkami has induced infringement of the Patents-in-Suit;

100. That Alkami has willfully infringed the Patents-in-Suit;

101. That Alkami be ordered to account for and pay to Plano Encryption past and future damages, costs, expenses, together with prejudgment and post-judgment interest to compensate for Defendant's infringement of the Patents-in-Suit as provided under 35 U.S.C. § 284, and increase such award by up to three times the amount found or assessed in accordance

with 35 U.S.C. § 284, and further including an accounting for infringing sales not presented at trial and an award by the Court of additional damages for any such infringing sales;

102. An award to Plaintiff for enhanced damages resulting from the knowing, deliberate, and willful nature of Defendant's prohibited conduct, as provided under 35 U.S.C. § 284;

103. That this case be declared exceptional and Plano Encryption be awarded its costs, expenses, and reasonable attorneys' fees in this action pursuant to 35 U.S.C. § 285; and

104. That Plaintiff Plano Encryption be awarded such other equitable or legal relief as this Court deems just and proper under the circumstances.

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,

PLANO ENCRYPTION TECHNOLOGIES, LLC

Dated: November 28, 2016

By: Jeremy S. Pitcock

Jeremy S. Pitcock
Admitted to the Eastern District of Texas
PITCOCK LAW GROUP
1501 Broadway, 12th Floor
New York, NY 10036
(646) 571-2237
(646) 571-2001 Fax
jpitcock@pitcocklawgroup.com

Elizabeth L. DeRieux
State Bar No. 05770585
Capshaw DeRieux, LLP

114 E. Commerce Ave.
Gladewater, TX 75647
Telephone: (903) 845-5770
Email: ederieux@capshawlaw.com

ATTORNEYS FOR PLAINTIFF
PLANO ENCRYPTION TECHNOLOGIES, LLC

CERTIFICATE OF SERVICE

I hereby certify that the all counsel of record who are deemed to have consented to electronic service are being served this 28th day of November, 2016, with a copy of this document via the Court's CM/ECF system per Local Rule CV-5(a)(3). Any other counsel of record will be served by electronic mail, facsimile transmission and/or first class mail on this same date.

/s/ Jeremy S. Pitcock