Patricia L. Peden, Esq. (SBN 206440)
patricia.peden@leclairryan.com
LECLAIRRYAN, LLP
44 Montgomery Street
Suite 3100
San Francisco, CA 94104
Phone: (415) 391.7111
Fax: (415) 391.8766

Christopher J. Lee (*Pro Hac Vice Pending*)
clee@leesheikh.com
David J. Sheikh (*Pro Hac Vice Pending*)
dsheikh@leesheikh.com
Richard B. Megley, Jr. (*Pro Hac Vice Pending*)
rmegley@leesheikh.com
Brian E. Haan (*Pro Hac Vice Pending*)
bhaan@leesheikh.com
Ashley E. LaValley (*Pro Hac Vice Pending*)
alavalley@leesheikh.com
Dragan Gjorgiev (*Pro Hac Vice Pending*)
dgjorgiev@leesheikh.com
LEE SHEIKH MEGLEY & HAAN LLC
111 West Jackson Boulevard, Suite 2230
Chicago, IL 60604
Phone: (312) 982-0070
Fax: (312) 982-0071

Attorneys for Plaintiff
MPH TECHNOLOGIES OY

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

MPH TECHNOLOGIES OY,

Plaintiff,

vs.

APPLE INC.,

Defendant.

Case No. _____

COMPLAINT FOR INFRINGEMENT OF U.S. PATENT NOS. 8,346,949; 9,762,397; 9,712,494; 9,712,502; 9,838,362; 7,620,810; 7,937,581; AND 8,037,302

JURY TRIAL DEMANDED

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff, MPH Technologies Oy ("MPH"), complains of Defendant, Apple Inc. ("Apple"), as follows:

THE NATURE OF THE LAWSUIT

1. This is a claim for patent infringement arising under the patent laws of the United States, Title 35 of the United States Code § 1 *et seq.* This Court has exclusive jurisdiction over the subject matter of the Complaint under 28 U.S.C. §§ 1331 and 1338(a).

INTRODUCTION

2. This action arises out of Apple's unauthorized and continued use of MPH's technologies claimed and described in the patents being asserted in this Complaint, which relate to, among other things, virtual private network (VPN) and secure messaging technologies.

3. More than two years before the filing of this lawsuit, MPH amicably approached Apple and informed it of MPH's technologies and patents. In the ensuing discussions, MPH repeatedly and dutifully provided the substantial information that Apple demanded from MPH, including detailed claim charts showing what MPH believed to be Apple's infringing use of MPH's patented technologies. MPH also substantively responded to each and every alleged "non-infringement" and "invalidity" argument made by Apple through numerous letter exchanges and multiple lengthy teleconferences attended by Apple's in-house and outside counsel. MPH exhausted all non-litigation options to make Apple aware of its need for a license from MPH and resolve this dispute amicably before filing this lawsuit.

4. Apple initially expressed a potential interest in MPH's patent rights and continued to engage MPH in substantive discussions. After all of its alleged non-infringement positions had been addressed and undermined by MPH in writing, Apple claimed to possess and offered to share with MPH prior art that it claimed was relevant to the validity of MPH's patent rights. For more than a year later, Apple has provided no such prior art to MPH and, instead, has continued to use the patented technologies in its then-existing and additional products and services.

5. MPH seeks to hold Apple accountable for its unlawful conduct and substantial harm

that it has inflicted upon MPH through, among other things, its knowing, continued and unauthorized infringement of MPH's patent rights.

THE PARTIES

6. MPH is a Finnish company with its principal place of business at Keilaranta 1, 02150 Espoo, Finland.

7. MPH owns all right, title, interest in and has standing to sue for the infringement of United States Patent No. 8,346,949 B2, entitled Method and System for Sending a Message Through a Secure Connection, issued on January 1, 2013, and corrected via a Certification of Correction on November 21, 2017 by the United States Patent and Trademark Office ("the '949 Patent"). A copy of the '949 Patent is attached as **Exhibit A**.

8. MPH owns all right, title, interest in and has standing to sue for the infringement of United States Patent No. 9,762,397 B2, entitled Method and System for Sending a Message Through a Secure Connection and issued on September 12, 2017 by the United States Patent and Trademark Office ("the '397 Patent"). A copy of the '397 Patent is attached as **Exhibit B**.

9. MPH owns all right, title, interest in and has standing to sue for the infringement of United States Patent No. 9,712,494 B2, entitled Method and System for Sending a Message Through a Secure Connection and issued on July 18, 2017 by the United States Patent and Trademark Office ("the '494 Patent"). A copy of the '494 Patent is attached as **Exhibit C**.

10. MPH owns all right, title, interest in and has standing to sue for the infringement of United States Patent No. 9,712,502 B2, entitled Method and System for Sending a Message Through a Secure Connection and issued on July 18, 2017 by the United States Patent and Trademark Office ("the '502 Patent"). A copy of the '502 Patent is attached as **Exhibit D**.

11. MPH owns all right, title, interest in and has standing to sue for the infringement of United States Patent No. 9,838,362 B2, entitled Method and System for Sending a Message Through a Secure Connection and issued on December 5, 2017 by the United States Patent and Trademark Office ("the '362 Patent"). A copy of the '362 Patent is attached as **Exhibit E**.

12. MPH owns all right, title, interest in and has standing to sue for the infringement of United States Patent No. 7,620,810 B2, entitled Method and Network for Ensuring Secure

Forwarding of Messages and issued on November 17, 2009 by the United States Patent and Trademark Office ("the '810 Patent"). A copy of the '810 Patent is attached as **Exhibit F**.

13. MPH owns all right, title, interest in and has standing to sue for the infringement of United States Patent No. 7,937,581 B2, entitled Method and Network for Ensuring Secure Forwarding of Messages and issued on May 3, 2011 by the United States Patent and Trademark Office ("the '581 Patent"). A copy of the '581 Patent is attached as **Exhibit G**.

14. MPH owns all right, title, interest in and has standing to sue for the infringement of United States Patent No. 8,037,302 B2, entitled Method and System for Ensuring Secure Forwarding of Messages and issued on October 11, 2011 by the United States Patent and Trademark Office ("the '302 Patent"). A copy of the '302 Patent is attached as **Exhibit H**.

15. The technologies and inventions claimed and described in the above patents were initially conceived and developed by Intrasecure Networks Oy. Intrasecure Networks Oy (later known as Netseal Oy) ("Netseal") was a Finnish company founded in 1996 to develop and commercialize cutting-edge technologies in the area of mobility and network security, and became a technology leader in the area of mobile communication security.

16. Netseal's extensive research and development efforts were funded by a number of prominent venture capital and mutual fund companies and Finnish governmental agencies. For instance, in its early stages, Netseal received funding from Fidelity Ventures, Tekes and Finnvera, and CapMan Oyj. Netseal's R&D efforts resulted in significant and valuable technologies in the areas of network mobility and security which are protected by numerous patent applications and issued patents in the United States, Finland, Germany, France, Austria, Italy, Spain, Sweden, Great Britain and elsewhere in Europe.

17. The technologies developed and marketed by Netseal were recognized and accepted by the global mobile communications industry. For example, one of the first implementations of Netseal's technologies was for Avecra Oy, the catering service provider for the Finnish national railway. Netseal's technology enabled transmission of real-time inventory and other sensitive information securely to Avecra's servers while trains were moving from one station to another, and hence, from one network to another.

18. In a September 2001 article, Computer World listed Avecra Oy as one of the "Top 25 Wireless Innovators," specifically attributing this innovation to the use of Netseal's technology.

19. By 2004, Netseal's technology was implemented in over sixty installations, including national and regional information and communications technology (ICT) providers in Norway and Finland, institutions in the Finnish public sector (such as governmental offices and universities), and the mobile workforce in Finland, the United Kingdom, and elsewhere in Europe.

20. Netseal Oy assets were purchased and incorporated into Netseal Mobility Technologies – NMT Oy. Netseal's patented technologies were later assigned from Netseal Mobility Technologies – NMT Oy to MPH, which is managed by former officers of Netseal Oy and Netseal Mobility Technologies – NMT Oy.

21. MPH has continued its business of developing and licensing network mobility and security technologies developed by Netseal. MPH's patented technologies have been adopted and utilized by mobile and secure communications industries. A number of these patented technologies have been adopted by these industries and incorporated into their product lines as standard or "default" features. These technologies are crucial to, among other things, allowing corporate or enterprise VPN users to move freely with mobile devices while ensuring uninterrupted and secure VPN connectivity over often unsecure networks.

22. Defendant Apple Inc. is a corporation organized and existing under the laws of the State of California, with its principal place of business at 1 Infinite Loop, Cupertino, California, 95014.

23. Apple has sold and provided products and services in the United States that are accused of infringing one or more of the patents being asserted in this lawsuit.

PERSONAL JURISDICTION AND VENUE

24. This Court has personal jurisdiction over Apple because, among other things, Apple regularly conducts business in California and this District; Apple maintains its principal place of business in California and this District; Apple is registered to do business in the State of California; and Apple has designated an agent for service of process in the State of California.

25. Venue is proper in this judicial district under 28 U.S.C. §§ 1391 and 1400(b) because a substantial part of the events giving rise to the claims occurred in this judicial District, Apple resides in this judicial District, and Apple has committed acts of infringement and has a regular and established place of business in this District.

PRIOR DEALINGS BETWEEN APPLE AND MPH

26. MPH first notified Apple of MPH's patents through a series of email exchanges between MPH and Apple, starting on July 1, 2016. The initial exchange of emails between MPH and Apple led to a phone call with Apple's patent acquisitions executive on July 15, 2016.

27. On October 18, 2016, as a follow up to their July 15, 2016 conversation, MPH wrote to Apple's patent acquisitions executive to discuss Apple's evaluation of and interest in obtaining rights to MPH's patents. As requested by Apple, in the letter, MPH provided Apple with additional background information on MPH and explained in detail the applicability of MPH's patented technologies to Apple's business.

28. In this October 18, 2016 communication, MPH informed Apple of its ongoing infringement of the '810 Patent, '581 Patent, '302 Patent, and '949 Patent. MPH also provided detailed claim charts for the '581 and '810 Patents showing the relevance of the MPH patents to Apple's products, including Apple's adoption of "MOBIKE" technologies (IETF RFC 4555) in its iOS and OS X/macOS devices and services. MPH also notified Apple of the existence of then-pending Application No. 13/685,544, which has since issued as the '397 Patent. MPH offered to engage in discussions for an amicable resolution for Apple's use of the patented technologies of MPH.

29. On October 18, 2016, Apple's patent acquisitions executive referred MPH to Apple's in-house patent counsel to handle MPH's inquiry.

30. On November 22, 2016, MPH provided detailed claim charts for the '302 Patent and '949 Patent regarding Apple's Always-On VPN feature and iMessage end-to-end encryption functionality, respectively, further showing the relevance of the MPH patents to Apple's products, including its iOS and OS X/macOS devices such as its desktop and laptop computers, iPhones and iPads.

31. On November 29, 2016, Apple's counsel wrote to MPH indicating that Apple would review the submitted materials and that "a face-to-face meeting would be helpful" after Apple completed its initial assessment.

32. On December 15, 2016, Apple's counsel sent a letter to MPH indicating that Apple was analyzing MPH's patents and the additional documentation provided by MPH.

33. Apple's counsel further responded to MPH's prior correspondence through a letter dated February 18, 2017. The letter included conclusory assertions of non-infringement and invalidity while stating that Apple had "carefully reviewed the five patents, their prosecution history, the information you provided, and other relevant materials." Apple's letter stated that it did not "believe a license is required, as the asserted patents are not infringed and/or invalid as MPH appears to be interpreting the claims." Apple qualified its response, stating that its letter merely "sets forth a high level summary of our investigation, and we reserve any omitted non-infringement, invalidity, or other defenses in the interests of brevity." Apple invited MPH to "provide a detailed explanation of your position" in the event MPH disagreed with Apple's assessment.

34. MPH responded to Apple's assertions made in Apple's February 18, 2017 letter with a detailed response letter on March 6, 2017, which explained why Apple's conclusory assertions of alleged non-infringement and invalidity lacked merit. MPH also provided Apple with a detailed claim chart mapping allowed claim 1 of U.S. Patent Application No. 13/685,544 to Apple's iMessage platform. MPH again invited Apple to engage in further discussions so that an amicable resolution could be achieved.

35. On March 30, 2017, Apple's counsel wrote to MPH requesting a substantive discussion, either by phone or in person, and reiterating conclusory assertions of alleged non-infringement and invalidity previously made by Apple and rebutted by MPH.

36. On April 7, 2017, MPH promptly responded to Apple's March 30, 2017 letter and again refuted Apple's vague and conclusory assertions of non-infringement and invalidity. MPH also provided Apple with a copy of published U.S. Patent Application No. 13/685,544 (Patent Application Publication No. US 2017/0093580 A9), which later issued as the '397 Patent, as well as the corresponding Notice of Allowance. MPH also informed Apple that MPH's U.S. Patent Application

No. 15/372,208 had been published (Patent Application Publication No. US 2017/0093799 A1) and was allowed by the United States Patent and Trademark Office. MPH provided a copy of this publication and Notice of Allowance.

37. On April 19, 2017, MPH informed Apple that MPH's Application No. 15/376,558 had recently been allowed by the United States Patent and Trademark Office. MPH also provided a copy of U.S. Patent Application Publication No. US 2017/0099266 A1 and the Notice of Allowance.

38. Apple (through its in-house and outside counsel) and MPH subsequently discussed whether Apple was interested in obtaining a license to MPH's patents during a May 3, 2017 teleconference. Apple and MPH continued discussions on whether Apple was interested in obtaining a license to MPH's patents during their May 5, 2017, May 17, 2017 and May 31, 2017 teleconferences.

39. During the May 2017 licensing discussions, Apple's counsel indicated that Apple was preparing and would shortly send an analysis concerning alleged invalidity of one or more of MPH's patents based on prior art. As of the filing of this Complaint, however, Apple has not sent such an analysis to MPH.

40. On July 18, 2017, Applications No. 15/372,208 and No. 15/376,558 issued as the '494 Patent and '502 Patent, respectively. That same day, MPH's counsel notified Apple's counsel of their issuance. MPH also provided claim charts comparing claims of the issued patents to Apple's iMessage and FaceTime services.

41. On July 19, 2017, Apple's counsel acknowledged their receipt of MPH's July 18, 2017 communication, and indicated that Apple would respond to that communication. As of the filing of this Complaint, however, Apple's counsel has not provided any response to MPH's July 18, 2017 communication.

42. Contrary to its representation that a "face-to-face meeting would be helpful" after its initial review of MPH's submissions and its representations to MPH that it had carefully reviewed MPH's patents, the patent file histories and the materials provided by MPH, Apple has not met with MPH after its initial or subsequent review of the patents, file histories and claim charts provided by MPH.

43. In July 2017, an executive of RPX Corporation, a then publicly traded company whose member-clients such as Apple pay for access to RPX's portfolio of patent risk solutions and patents, contacted MPH ostensibly on behalf of and for the benefit of Apple.

44. In addition to being an early member of RPX, Apple has had a close business relationship and engaged in numerous business dealings with RPX. For example, RPX paid $900 million to purchase a portfolio of 4,000 patent assets in 2014 from Rockstar Consortium LLC, a non-producing patent holding and monetization entity whose founding members included, among others, Apple.

45. Apple has also been a member and privy of RPX, which has petitioned and prosecuted an administrative procedure known as "inter partes review" of duly-issued United States patents before the United States Patent and Trademark Office's Patent Trial and Appeal Board for Apple's benefit.

46. Despite MPH's extensive efforts to license its technology to Apple amicably over a two-year period, Apple has ultimately refused to take a license under the MPH patents or resolve this dispute without the need for litigation. Instead, Apple has chosen to willfully disregard MPH's patent rights and continue its unauthorized use of MPH's technology.

APPLE'S ACCUSED IMESSAGE AND FACETIME INSTRUMENTALITIES

47. Apple's iMessage is a messaging service specifically designed for Apple devices, including various models of the iPhone, iPad, iPod, Apple Watch, and Mac computer products.

48. Apple's iMessage is one of the most widely deployed secure messaging services. In 2014, Apple's CEO, Tim Cook, stated that Apple handles several billion iMessages per day. And, in February 2016, Eddy Cue, Apple's senior vice president of Internet Software and Services, stated that the system transmits as many as 200,000 messages per second. The use of the iMessage service and the resulting volume of messages have increased since the above-referenced statements were made by Messrs. Cook and Cue.

49. Apple has touted that messages sent through Apple's iMessage platform are protected by end-to-end encryption so no one but the sender and the receiver can access the encrypted contents of the messages. In its security documentation, Apple claims that even Apple itself is unable to

decrypt the encrypted contents of messages sent through the iMessage platform. One practical benefit of this secure mobile messaging platform technology, as claimed and described in one or more of MPH's patents, is the ability for a sender using his or her mobile device to send encrypted messages securely to a mobile device of an intended recipient using unsecure Internet connections without compromising the integrity and security of the message contents.

50. For example, Apple states in the August 2018 version of its iOS Security Guide:

> Apple doesn't log the contents of messages or attachments, which are protected by end-to-end encryption so no one but the sender and receiver can access them. Apple can't decrypt the data.

51. Apple has implemented the accused iMessage platform in at least the following operating systems that run on Apple devices: iOS 8, iOS 9, iOS 10, iOS 11, iOS 12, OS X Yosemite, OS X El Capitan, macOS Sierra, macOS High Sierra, macOS Mojave, WatchOS 2, WatchOS 3, WatchOS 4 and WatchOS 5.

52. Apple's FaceTime is a service that allows users to make video and audio calls using their Apple devices, including iPhones, iPads, iPods, Apple Watches, and Mac computers.

53. According to Apple, FaceTime uses end-to-end encryption to protect FaceTime audio and video contents. As with the iMessage platform, Apple has stated that it is unable to decrypt the data sent through FaceTime.

54. Apple has made FaceTime available on at least the following operating systems that run on Apple devices: iOS 8, iOS 9, iOS 10, iOS 11, iOS 12, OS X Yosemite, OS X El Capitan, macOS Sierra, macOS High Sierra, macOS Mojave, WatchOS 2, WatchOS 3, WatchOS 4 and WatchOS 5.

55. Apple owns, controls, maintains or operates servers, data centers, databases and other network resources to provide the accused iMessage and FaceTime services.

56. Apple's iMessage application makes extensive use of Apple Push Notification service ("APNs"), including to transmit iMessage content. Apple owns and operates the APNs servers.

57. Apple's FaceTime service also uses APNs. For example, FaceTime calls use the APNs to establish an initial connection.

58. Apple Watch also uses APNs to support end-to-end encryption.

59. Other Apple features, including Handoff, Universal Clipboard, iPhone Cellular Call Relay, and iPhone Text Message Forwarding, also use APNs to support end-to-end encryption.

60. Apple devices, such as iPhones, iPads, iPods, Apple Watches, and Mac computers, can send secure messages via the APNs servers to other Apple devices, such as iPhones, iPads, iPods, Apple Watches, and Mac computers, using iMessage and FaceTime services.

61. Apple's iMessage and FaceTime services also utilize Apple's directory service, Apple Identity Service (a.k.a. "IDS"). The IDS is responsible for distributing a user's public keys and APNs addresses on request.

APPLE'S INSTRUCTIONS TO AND CONTROL OVER USERS OF THE IMESSAGE AND FACETIME SERVICES

62. Apple maintains absolute control over the operation of its iMessage and FaceTime services, including its operation of the software, servers, and databases that support such services.

63. As a condition of using Apple's iMessage and FaceTime services, users of these services are required to sign up and agree to numerous terms and conditions unilaterally imposed by Apple, including in its user software licenses, iTunes account agreement, and privacy agreement.

64. For example, Apple begins its iOS Software License Agreement by stating that "BY USING YOUR iPHONE, iPAD or iPOD Touch ("iOS DEVICE"), YOU ARE AGREEING TO BE BOUND BY THE FOLLOWING TERMS." *See* Apple Inc. iOS Software License Agreement (www.apple.com/legal/sla/docs/iOS112.pdf); *see also* Apple Inc. Software License Agreement for macOS High Sierra (www.apple.com/legal/sla/docs/macOS1013.pdf).

65. The Apple iOS Software License Agreement, to which each Apple iOS device user wishing to have access to, receive the benefit of, and use iMessage and FaceTime must agree, also provides:

> The software (including Boot ROM code, embedded software and third party software), documentation, interfaces, content, fonts and any data that came with your iOS Device ("Original iOS Software"), as may be updated or replaced by feature enhancements, software updates or system restore software provided by Apple ("iOS Software Updates"), whether in read only memory, on any other media or in any other form (the Original iOS Software and iOS Software Updates are collectively referred to as the "iOS Software") are licensed, not sold, to you by Apple Inc. ("Apple") for use only under the terms of this License. Apple and its licensors retain ownership of the iOS Software itself and reserve all rights not expressly granted to you. You agree that the terms of this License will apply to any Apple-branded app that may be built-in on your iOS Device, unless such app is accompanied by a separate license,

in which case you agree that the terms of that license will govern your use of that app.

66. Similarly, the Apple macOS software license agreement states:

> The Apple software (including Boot ROM code), any third party software, documentation, interfaces, content, fonts and any data accompanying this License whether preinstalled on Apple-branded hardware, on disk, in read only memory, on any other media or in any other form (collectively the "Apple Software") are licensed, not sold, to you by Apple Inc. ("Apple") for use only under the terms of this License. Apple and/or Apple's licensors retain ownership of the Apple Software itself and reserve all rights not expressly granted to you. You agree that the terms of this License will apply to any Apple-branded application software product that may be preinstalled on your Apple-branded hardware, unless such product is accompanied by a separate license, in which case you agree that the terms of that license will govern your use of that product.

67. Additionally, Apple requires each user of iMessage and FaceTime to register and obtain an Apple ID as a prerequisite to using these services. Prior to using the services, each user must first log in and then provide and allow Apple to access, store, and use the user's unique identifier. These requirements are set forth in Apple's software license agreements for both iOS and macOS:

> Use of the App Store requires a unique user name and password combination, known as an Apple ID. An Apple ID is also required to access app updates and certain features of the iOS Software and Services.
>
> * * *
>
> **Consent to Use of Data.** When you use your device, your phone number and certain unique identifiers for your iOS Device are sent to Apple in order to allow others to reach you by your phone number when using various communication features of the iOS Software, such as iMessage and FaceTime. When you use iMessage, Apple may hold your messages in encrypted form for a limited period of time in order to ensure their delivery.
>
> * * *
>
> By using this software in connection with an Apple ID, or other Apple Service, you agree to the applicable terms of service for that Service, such as the latest Apple Media Services Terms and Conditions for the country in which you access such Services, which you may access and review at http://www.apple.com/legal/internet-services/itunes/ww/.

Apple Inc. iOS Software License Agreement; *see also* Apple Inc. Software License Agreement for macOS High Sierra.

68. Apple also requires end users to provide personal information and other identifying information to access the iMessage and FaceTime services and receive benefits from such services:

> Personal information is data that can be used to identify or contact a single person. You may be asked to provide your personal information anytime you are in contact with Apple or an Apple affiliated company. Apple and its affiliates may share this personal information with each other and use it consistent with this Privacy Policy. They may also combine it with other information to provide and improve our products, services, content, and advertising. You are not required to provide the personal information that we have requested, but, if you chose not to do so, in many cases we will not be able to provide you with our products or services or respond to any queries you may have.
>
> * * *
>
> We may collect information such as occupation, language, zip code, area code, unique device identifier, referrer URL, location, and the time zone where an Apple product is used so that we can better understand customer behavior and improve our products, services, and advertising. https://www.apple.com/privacy/privacy-policy/.

69. Based on the above facts, among other things, Apple directs or controls the performance of end users of its devices operating Apple's iMessage and FaceTime services. Apple has the right and ability to stop or limit use of its iMessage and FaceTime service. Apple conditions use of its software, including use of the iMessage and FaceTime applications and the benefits derived therefrom, upon agreeing to the above terms, including performance of the relevant acts of infringement carried out by its devices, as set forth below. Apple also establishes the manner and timing of such performance.

APPLE'S MOBIKE-ENABLED PRODUCTS

70. Internet Key Exchange (IKEv2) Mobility and Multihoming Protocol (MOBIKE) is a protocol that is a mobility and multihoming extension to IKEv2.

71. The MOBIKE protocol provides seamless mobility for IPsec connections.

72. MOBIKE allows the IP addresses associated with IKEv2 and tunnel mode IPsec Security Associations to change. The main scenario for MOBIKE is enabling a remote access VPN user to move from one address to another without re-establishing all security associations with the VPN gateway.

73. IKEv2 is used for performing mutual authentication, as well as establishing and maintaining IPsec Security Associations.

74. Apple has made IKEv2 the default virtual private network (VPN) type for every iOS product since iOS 9.

75. Apple has made IKEv2 the default VPN type for every OS X/macOS product since OS

X El Capitan.

76. Apple has enabled MOBIKE by default in every iOS product since iOS 9.

77. Apple has enabled MOBIKE by default in every OS X/macOS product since OS X El Capitan.

78. Apple's products, including without limitation, Apple's iPhones, iPads, iPods, and Mac computers that contain versions of iOS, OS X and macOS software that are configured to have IKEv2 as the VPN type and enable MOBIKE are hereinafter referred to as "the accused Apple MOBIKE-implemented products." This includes every iOS product since iOS 9 and every OS X/macOS product since OS X El Capitan, and any subsequently introduced iOS/macOS products that incorporate the same or substantially the same IKEv2 VPN and MOBIKE enabled features or functionality.

79. Apple's iOS and OS X/macOS devices are set up by Apple to support IKEv2.

80. Apple provides VPN setup guidelines for IKEv2 setup.

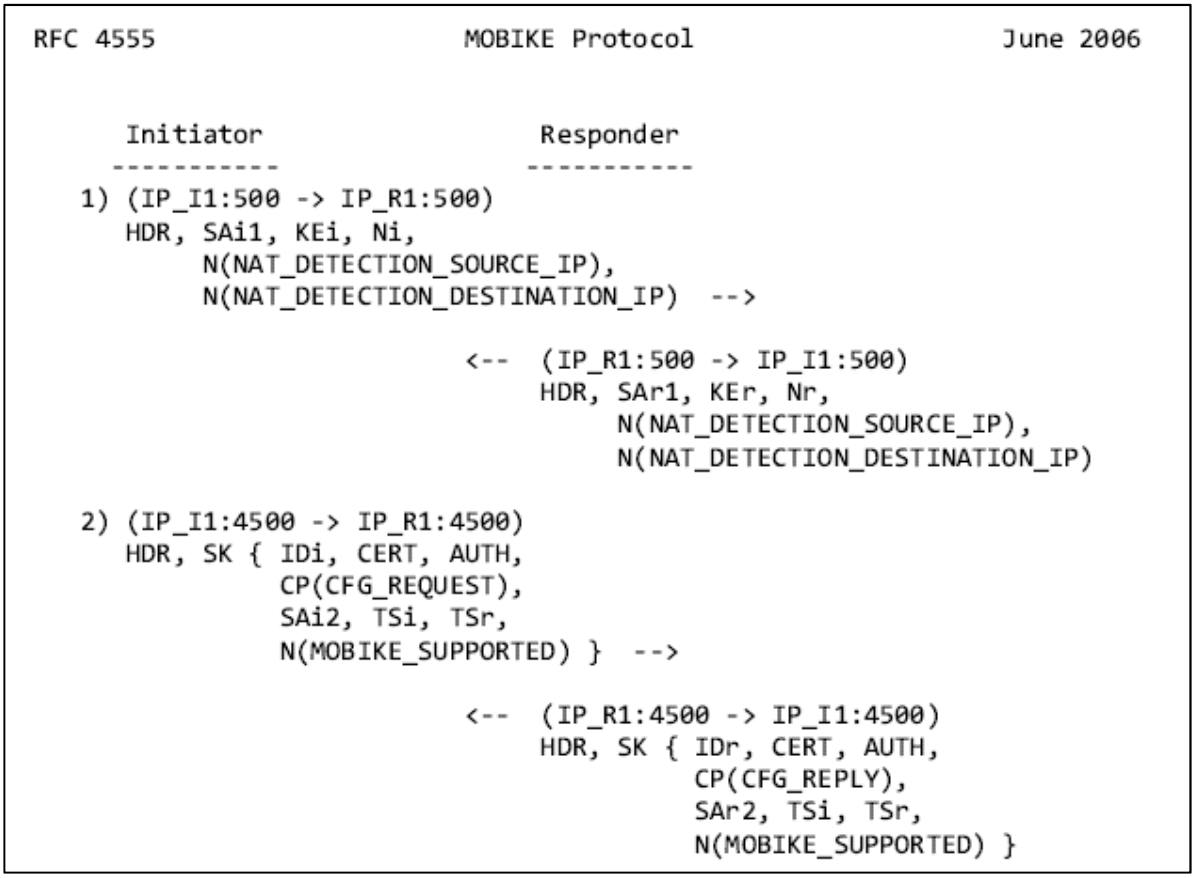
81. At the 2015 Worldwide Developers Conference (WWDC15), Apple announced that MOBIKE was supported in its products.

82. Apple products that support IKEv2 can forward messages via a security gateway to other hosts in networks.

83. Apple provides a built-in VPN client in iOS and OS X/macOS devices that is enabled from network preferences.

84. The Internet Engineering Task Force (IETF) Request for Comments (RFC) 4555, at https://www.ietf.org/rfc/rfc4555.txt, sets forth the MOBIKE protocol, which Apple has implemented in its accused products and services.

85. Beginning at page 6 of RFC 4555, a simple MOBIKE exchange in a mobile scenario is illustrated in Section 2.2. Reproduced below are Steps 1 and 2 of that illustration as set forth on page 7 of RFC 4555, which show the normal IKE_INIT exchange and the peers informing each other that they support MOBIKE:



```
RFC 4555                    MOBIKE Protocol                    June 2006


      Initiator                    Responder
     -----------                  -----------
   1) (IP_I1:500 -> IP_R1:500)
      HDR, SAi1, KEi, Ni,
           N(NAT_DETECTION_SOURCE_IP),
           N(NAT_DETECTION_DESTINATION_IP)  -->

                              <--  (IP_R1:500 -> IP_I1:500)
                                   HDR, SAr1, KEr, Nr,
                                        N(NAT_DETECTION_SOURCE_IP),
                                        N(NAT_DETECTION_DESTINATION_IP)

   2) (IP_I1:4500 -> IP_R1:4500)
      HDR, SK { IDi, CERT, AUTH,
                CP(CFG_REQUEST),
                SAi2, TSi, TSr,
                N(MOBIKE_SUPPORTED) }  -->

                              <--  (IP_R1:4500 -> IP_I1:4500)
                                   HDR, SK { IDr, CERT, AUTH,
                                             CP(CFG_REPLY),
                                             SAr2, TSi, TSr,
                                             N(MOBIKE_SUPPORTED) }
```

86. The accused Apple MOBIKE-implemented products use the normal IKE_INIT exchange set forth in step 1 recited above from RFC 4555 when establishing a secure connection with a VPN gateway.

87. The accused Apple MOBIKE-implemented products transmit using the packet protocol set forth under the "Initiator" column and are designed to receive the packet protocol set forth under the "Responder" column in step 2 recited above from RFC 4555 when establishing a secure connection with a VPN gateway.

88. Step 3 shown on page 7 of RFC 4555 illustrates when the Initiator such as a mobile device notices a change in its own address and informs the responder about that change. The Initiator informs the responder of its new address by sending an INFORMATIONAL request containing an UPDATE_SA_ADDRESSES notification. The request is sent using the new IP address of the Initiator. At this point, the Initiator starts to use the new address as a source address in the Initiator's outgoing ESP traffic. Upon receiving the UPDATE_SA_ADDRESSES notification, the Responder

records the new address. Step 3 as shown on page 7 of RFC 4555 is reproduced below:

```
(Initiator gets information from lower layers that its attachment
point and address have changed.)

3) (IP_I2:4500 -> IP_R1:4500)
   HDR, SK { N(UPDATE_SA_ADDRESSES),
             N(NAT_DETECTION_SOURCE_IP),
             N(NAT_DETECTION_DESTINATION_IP) }  -->

                         <-- (IP_R1:4500 -> IP_I2:4500)
                             HDR, SK { N(NAT_DETECTION_SOURCE_IP),
                                  N(NAT_DETECTION_DESTINATION_IP) }
```

89. The accused Apple MOBIKE-implemented products use the packet exchange shown in step 3 recited above from RFC 4555 when the IP address of the accused Apple MOBIKE-implemented products used for the secure connection with a VPN Gateway changes.

90. The accused Apple MOBIKE-implemented products work with VPN servers that support IPsec Security Associations.

91. The accused Apple MOBIKE-implemented products are designed to be capable of connecting with a VPN gateway using an IPsec tunnel connection.

92. The accused Apple MOBIKE-implemented products can transmit and receive IPsec packets from a VPN server that are UDP encapsulated.

93. The accused Apple MOBIKE-implemented products can transmit and receive IPsec packets from a VPN server that have payloads that are encrypted and authenticated.

94. At least some of the accused Apple MOBIKE-implemented products further include Wi-Fi Calling, a feature by which users can make or receive a phone call if they have a Wi-Fi connection in an area with little or no cellular coverage. Ports used by Apple products for the Wi-Fi Calling feature include 500 and 4500 with UDP and employ the IKEv2 protocol. *See* https://support.apple.com/lv-lv/HT202944.

APPLE'S ALWAYS-ON VPN SERVICE

95. Apple's "Always-on VPN" is a feature provided by Apple which forces applications running on Apple devices to connect only via an VPN tunnel.

96. Apple encourages and instructs organizations to use Always-on VPN to monitor and filter traffic to and from Apple devices, secure data within a network, and restrict device access to the Internet.

97. Apple in its iOS Security document dated January 2018 and in earlier versions of the document, has stated:

> Always-on VPN [] can be configured for devices managed via MDM and supervised using Apple Configurator 2, the Device Enrollment Program, or Apple School Manager. This eliminates the need for users to turn on VPN to enable protection when connecting to cellular and Wi-Fi networks. Always-on VPN gives an organization full control over device traffic by tunneling all IP traffic back to the organization. The default tunneling protocol, IKEv2, secures traffic transmission with data encryption. The organization can monitor and filter traffic to and from its devices, secure data within its network, and restrict device access to the Internet.

98. Always-on VPN activation requires device supervision. After the Always-on VPN profile is installed on a device, Always-on VPN automatically activates with no user interaction, and it stays activated (including across reboots) until the Always-on VPN profile is uninstalled.

99. Always-on VPN supports per-interface tunnels. For iOS devices, there is one tunnel for each active IP interface, i.e., one tunnel for the cellular interface and one tunnel for the Wi-Fi interface.

100. Apple's Always-on VPN feature is designed for situations where iOS devices move between networks such as cellular (e.g., 3G, 4G, or LTE) and Wi-Fi networks.

101. Apple introduced the Always-on VPN feature with its iOS 8 operating system.

102. Apple has since provided Always-on VPN capability on all Apple iOS devices, including iPhones and iPads, with the iOS 8, iOS 9, iOS 10, iOS 11 and iOS 12 operating systems.

103. Apple provides extensive instructions and guidelines for setting up and using Always-on VPN. Apple also provides software and tools to configure, activate, and supervise devices utilizing Always-on VPN including Apple Configurator, Apple Configurator 2, Apple Device Enrollment Program, Apple School Manager, and Apple Business Manager.

104. Apple has submitted the Always-on VPN client for "Common Criteria Evaluation" through the National Information Assurance Partnership (NIAP). As part of Apple's submissions to NIAP, evaluations were completed by Acumen Security and atsec information security on behalf of

and sponsored by Apple. The evaluations included tests performed in an environment where Apple iOS devices were connected to both Wi-Fi and cellular networks.

COUNT I - INFRINGEMENT OF U.S. PATENT NO. 8,346,949

105. MPH incorporates by reference paragraphs 1-104 as if fully set forth herein.

106. As described below, Apple has infringed and continues to infringe, literally or through the doctrine of equivalents, at least claims 1, 3, 9, 11, 12, 13, and 28 of the '949 Patent.

107. The Apple iMessage and FaceTime services enable Apple devices to send and receive secure messages over a telecommunications network, i.e., the Internet.

108. When operated as intended and required by Apple and under Apple's direction and control, pursuant to Apple's software licenses, privacy policies, and other user agreements, Apple devices, including iPhones, iPads, iPods, Apple Watches, and Mac computers, establish a secure connection with one another by negotiating and exchanging keys with one another according to a key exchange protocol through intermediate Apple servers.

109. Each Apple device is configured to be assigned with an IP address, which may change including, for example, when the connection is changed from a cellular network to a Wi-Fi network.

110. Intermediate Apple servers, including APNs servers, are configured to securely send and receive messages to and from Apple devices to provide the iMessage and FaceTime services.

111. When operated as intended and required by Apple and under Apple's direction and control, pursuant to Apple's software licenses, privacy policies, and other user agreements, Apple devices are configured to form secure messages using the functionalities of iMessage and FaceTime.

112. Messages sent through iMessage and FaceTime include a device token, which is a unique identifier assigned by Apple that identifies a unique app-device combination, which is used to forward messages to receiving Apple devices. Messages formed by Apple devices also include an address of Apple servers, including Apple's APNs servers. Such messages include payloads encrypted using encryption keys from a key exchange protocol.

113. Intermediate Apple servers, including Apple's APNs servers, receive encrypted message payloads sent by Apple devices to provide the iMessage and FaceTime services.

114. Apple servers, including its APNs servers, decrypt device tokens and use such tokens

to locate the addresses of the intended recipients of encrypted message payloads. The decrypted tokens are included with the encrypted message payloads, thus, replacing the encrypted device tokens. Apple is unable to decrypt the payloads of the messages.

115. Apple's APNs servers map device tokens with connections to receiving devices.

116. Apple utilizes a table located at Apple's APNs servers to map a device token to connection information of the receiving device.

117. Apple utilizes a table located at Apple's APNs servers to map a device token to connection information of the receiving device including the receiving device's location or address. Apple devices register their current locations with the APNs servers with a request and reply message exchange.

118. Apple's servers, including its APNs servers, forward the encrypted message payloads to the receiving Apple devices.

119. Apple's APNs servers and Apple devices sending and receiving messages through iMessage and FaceTime communicate using a TLS protocol.

120. Based on the above, Apple has infringed and continues to infringe at least claims 1, 3, 9, 11, 12, 13, and 28 of the '949 Patent under 35 U.S.C. § 271(a) by, among other things, making and/or using within the United States Apple devices, servers, and associated software that support and enable its iMessage and FaceTime services on Apple devices, including iPhones, iPads, iPods, Apple Watches, and Mac computers running the following Apple operating systems, as well as all other software versions which provide the same or substantially the same features and functionalities: iOS 8, iOS 9, iOS 10, iOS 11, iOS 12, OS X Yosemite, OS X El Capitan, macOS Sierra, macOS High Sierra, macOS Mojave, WatchOS 2, WatchOS 3, WatchOS 4 and WatchOS 5. Apple's acts of direct infringement include, without limitation, testing and otherwise using the foregoing instrumentalities by Apple's employees and agents, as well as directing and controlling, and conditioning its customers' and end users' participation and use of and receipt of the benefits of iMessage and FaceTime upon, the performance of steps of claims of the '949 Patent and establishing the manner or timing of that performance. Other Apple features, including Handoff, Universal Clipboard, iPhone Cellular Call Relay, and iPhone Text Message Forwarding, also use Apple's APNs to support end-to-

end encryption and, thus, Apple further infringes the foregoing claims of the '949 Patent under 35 U.S.C. § 271(a).

121. The acts of infringement of the '949 Patent by Apple have injured MPH, and MPH is entitled to recover damages adequate to compensate it for such infringement from Apple, but in no event less than a reasonable royalty. Further, the acts of infringement of the '949 Patent by Apple have injured and will continue to injure MPH unless and until this Court enters an injunction prohibiting further infringement of the '949 Patent.

122. Apple's infringement of the '949 Patent has been and continues to be willful, wanton, malicious, in bad faith, deliberate, consciously wrong, and flagrant. MPH provided Apple with detailed notice of its infringement of the '949 Patent by at least October 17, 2016 in a letter to Apple's patent acquisitions executive. On November 22, 2016, MPH's counsel also provided detailed claim charts for the '949 Patent regarding Apple's iMessage service, further showing Apple's infringement of the '949 Patent. Despite knowledge of its infringement, Apple continues its acts of infringement of the '949 Patent, as stated above. As such, Apple's infringement of the '949 Patent is willful.

COUNT II - INFRINGEMENT OF U.S. PATENT NO. 9,762,397

123. MPH incorporates by reference paragraphs 1-122 as if fully set forth herein.

124. As described below, Apple has infringed and continues to infringe, literally or through the doctrine of equivalents, at least claim 1 of the '397 Patent.

125. The Apple iMessage and FaceTime services enable the accused Apple devices to send and receive secure messages over a telecommunications network, i.e., the Internet.

126. When operated as intended and conditioned and required by Apple and under Apple's direction and control, pursuant to Apple's software licenses, privacy policies, and other user agreements, Apple devices, including iPhones, iPads, iPods, Apple Watches, and Mac computers, establish a secure connection by negotiating and exchanging keys according to a key exchange protocol through intermediate Apple servers.

127. Intermediate Apple servers, including Apple's APNs servers, receive encrypted message payloads sent by Apple devices to provide the iMessage and FaceTime services. The

encrypted message payloads are sent to the address of the intermediate Apple servers, including the APNs servers.

128. A device token is a unique identifier assigned by Apple to a specific app on a specific Apple device. Messages sent through iMessage and FaceTime include a device token that identifies a unique app-device combination. Apple's servers, including its APNs servers, are configured to decrypt and read these device tokens and use such tokens to locate the intended recipients of a message.

129. Apple's servers, including its APNs servers, forward the encrypted message payload to the receiving Apple device.

130. Based on the above, Apple has infringed and continues to infringe at least claim 1 of the '397 Patent under 35 U.S.C. § 271(a) by, among other things, making and/or using within the United States Apple devices, servers, and associated software that support its iMessage and FaceTime services on Apple devices, including iPhones, iPads, iPods, Apple Watches, and Mac computers running the following Apple operating systems, as well as all other software versions which provide the same or substantially the same features and functionalities: iOS 8, iOS 9, iOS 10, iOS 11, iOS 12, OS X Yosemite, OS X El Capitan, macOS Sierra, macOS High Sierra, macOS Mojave, WatchOS 2, WatchOS 3, WatchOS 4 and WatchOS 5.

131. Apple's acts of direct infringement include, without limitation, testing and otherwise using the foregoing instrumentalities by Apple's employees and agents, as well as directing and controlling, and conditioning its customers' and end users' participation and use and receipt of the benefits of iMessage and FaceTime upon, the performance of steps of claims of the '397 Patent and establishing the manner or timing of that performance. Other Apple features, including Handoff, Universal Clipboard, iPhone Cellular Call Relay, and iPhone Text Message Forwarding, also use Apple's APNs to support end-to-end encryption and, thus, Apple further infringes the foregoing claims of the '397 Patent under 35 U.S.C. § 271(a).

132. The acts of infringement of the '397 Patent by Apple have injured MPH, and MPH is entitled to recover damages adequate to compensate it for such infringement from Apple, but in no event less than a reasonable royalty. Further, the acts of infringement of the '397 Patent by Apple

have injured and will continue to injure MPH unless and until this Court enters an injunction prohibiting further infringement of the '397 Patent.

133. Apple's infringement of the '397 Patent has been and continues to be willful, wanton, malicious, in bad faith, deliberate, consciously wrong, and flagrant. MPH provided Apple with notice of the application that later issued as the '397 Patent by October 17, 2016. On March 6, 2017, MPH also provided Apple with a detailed claim chart mapping allowed claim 1 of U.S. Patent Application No. 13/685,544 to Apple's iMessage. Then, on April 7, 2017, MPH gave Apple a copy of the published application (Patent Application Publication No. US 2017/0093799 A1) which issued as the '397 Patent and the corresponding Notice of Allowance issued by the U.S. Patent and Trademark Office. Despite knowledge of its infringement, Apple continues its acts of infringement of the '397 Patent, as stated above. As such, Apple's infringement of the '397 Patent is willful.

COUNT III - INFRINGEMENT OF U.S. PATENT NO. 9,712,494

134. MPH incorporates by reference paragraphs 1-133 as if fully set forth herein.

135. As described below, Apple has infringed and continues to infringe, literally or through the doctrine of equivalents, at least claims 1, 2, 3, 4, 5, 6, 7, 9, 10, and 11 of the '494 Patent.

136. The Apple iMessage and FaceTime services enable Apple devices to send and receive secure messages over a telecommunications network, i.e., the Internet.

137. Apple utilizes intermediate servers, including its APNs servers, to send and receive messages to provide the iMessage and FaceTime services.

138. Apple controls, owns, and operates servers used for the iMessage and FaceTime services, including the APNs servers.

139. Apple's servers used for the iMessage and FaceTime services, including its APNs servers, are connected to the Internet.

140. Apple's servers used for iMessage and FaceTime, including its APNs servers, are configured with one or more IP addresses. An entire address block is assigned to Apple.

141. Apple's servers, including its APNs servers, are configured to receive secure messages from Apple devices to provide the iMessage and FaceTime services. The payloads of messages are encrypted using encryption keys from a key exchange protocol.

142. A device token is a unique identifier assigned by Apple to a specific app on a specific Apple device. Messages sent through iMessage and FaceTime include a device token that identifies a unique app-device combination. Apple's servers, including its APNs servers, are configured to decrypt and read these device tokens and use such tokens to locate the intended recipients of a message. Apple's APNs servers map device tokens with connections to receiving devices. Apple utilizes a table located at Apple's APNs servers to map a device token to connection information of the receiving device including location or address. Apple's servers, including its APNs servers, forward encrypted message payloads to the receiving Apple devices. The decrypted tokens are included with the encrypted message payloads, thus replacing the encrypted device tokens. Apple devices register their current locations with the APNs servers with a request and reply message exchange.

143. Apple's APNs do not have the keys to decrypt the payloads of messages or data sent through the iMessage and FaceTime services.

144. Apple's APNs are not configured to access the keys to decrypt the payloads of messages or data sent through the iMessage and FaceTime services.

145. Apple's APNs servers and Apple devices that send and receive messages through iMessage and FaceTime communicate using a TLS protocol.

146. Based on the above, Apple has infringed and continues to infringe at least claims 1, 2, 3, 4, 5, 6, 7, 9, 10, and 11 of the '494 Patent under 35 U.S.C. § 271(a) by, among other things, making, using, operating, and importing into the United States the servers, such as APNs servers, and associated software that support and provide its iMessage and FaceTime services for Apple devices, including iPhones, iPads, iPods, Apple Watches, and Mac computers running the following Apple operating systems, as well as all other software versions which provide the same or substantially the same features and functionalities: iOS 8, iOS 9, iOS 10, iOS 11, iOS 12, OS X Yosemite, OS X El Capitan, macOS Sierra, macOS High Sierra, macOS Mojave, WatchOS 2, WatchOS 3, WatchOS 4 and WatchOS 5. Other Apple features, including Handoff, Universal Clipboard, iPhone Cellular Call Relay, and iPhone Text Message Forwarding, also use Apple's APNs to support end-to-end encryption and, thus, Apple further infringes the foregoing claims of the '494 Patent under 35 U.S.C.

§ 271(a).

147. The acts of infringement of the '494 Patent by Apple have injured MPH, and MPH is entitled to recover damages adequate to compensate it for such infringement from Apple, but in no event less than a reasonable royalty. Further, the acts of infringement of the '494 Patent by Apple have injured and will continue to injure MPH unless and until this Court enters an injunction prohibiting further infringement of the '494 Patent.

148. Apple's infringement of the '494 Patent has been and continues to be willful, wanton, malicious, in bad faith, deliberate, consciously wrong, and flagrant. MPH provided Apple with notice of Apple's infringement of the '494 Patent by at least July 18, 2017, including with claim charts comparing the claims to Apple's iMessage and FaceTime services. Despite knowledge of its infringement, Apple continues its acts of infringement of the '494 Patent, as stated above. As such, Apple's infringement of the '494 Patent is willful.

COUNT IV - INFRINGEMENT OF U.S. PATENT NO. 9,712,502

149. MPH incorporates by reference paragraphs 1-148 as if fully set forth herein.

150. As described below, Apple has infringed and continues to infringe, literally or through the doctrine of equivalents, at least claims 1, 2, 7, 8, 9, and 10 of the '502 Patent.

151. Apple devices, including iPhones, iPads, iPods, Apple Watches, and Mac computers, are configured by Apple to send and receive secure messages over the Internet through the Apple iMessage and FaceTime services.

152. Apple devices, including iPhones, iPads, iPods, Apple Watches, and Mac computers, are configured by Apple to connect to a telecommunications network.

153. Apple devices, including iPhones, iPads, iPods, Apple Watches, and Mac computers, are also configured by Apple to be assigned with an IP address.

154. Apple devices, including iPhones, iPads, iPods, Apple Watches, and Mac computers, are mobile computers in that the address of the mobile computer changes.

155. Utilizing the iMessage and FaceTime services, Apple devices, including iPhones, iPads, iPods, Apple Watches, and Mac computers, are configured by Apple to form secure messages. Such messages include payloads encrypted using encryption keys from a key exchange protocol.

Messages sent through iMessage and FaceTime also include a device token, which is a unique identifier assigned by Apple that identifies a unique app-device combination, which is used to forward messages to receiving Apple devices. Messages formed by Apple devices also include an address of Apple servers, including Apple's APNs servers. Apple servers, including its APNs servers, decrypt and read these device tokens and use such tokens to locate the intended recipients of a message.

156. Utilizing the iMessage and FaceTime services' functionalities, Apple devices are configured by Apple to send the secure messages to Apple's servers for forwarding of the encrypted data payload to the intended recipients of a message.

157. Apple devices are configured by Apple to set up a secure connection using a key exchange protocol.

158. Apple devices are configured by Apple to form secure messages using messages received by the Apple devices. For example, an Apple iPhone forms a secure message for iMessage using a message received from an Apple Watch.

159. Apple devices are configured by Apple to send signaling messages to Apple's servers when they change IP addresses such that Apple's servers know that their addresses changed. Such signaling messages are sent via a TLS connection, and are thus encrypted and authenticated.

160. Based on the above, Apple has infringed and continues to infringe at least claims 1, 2, 7, 8, 9, and 10 of the '502 Patent under 35 U.S.C. § 271(a) by, among other things, making, using, selling, offering for sale, and importing into the United States infringing Apple devices, including iPhones, iPads, iPods, Apple Watches, and Mac computers running the following Apple operating systems, as well as all other software versions which provide the same or substantially the same features and functionalities: iOS 8, iOS 9, iOS 10, iOS 11, iOS 12, OS X Yosemite, OS X El Capitan, macOS Sierra, macOS High Sierra, macOS Mojave, WatchOS 2, WatchOS 3, WatchOS 4 and WatchOS 5. Other Apple features, including Handoff, Universal Clipboard, iPhone Cellular Call Relay, and iPhone Text Message Forwarding, also use Apple's APNs to support end-to-end encryption and, thus, Apple further infringes the foregoing claims of the '502 Patent under 35 U.S.C. § 271(a).

161. Apple has and continues to knowingly and actively induce infringement of at least claims 1, 2, 7, 8, 9, and 10 of the '502 Patent under 35 U.S.C. §271(b) by, among other things, making, using, selling, offering for sale, and importing within and into the United States infringing Apple devices, including iPhones, iPads, iPods, Apple Watches, and Mac computers running the following Apple operating systems, as well as all other software versions which provide the same or substantially the same features and functionalities: iOS 8, iOS 9, iOS 10, iOS 11, iOS 12, OS X Yosemite, OS X El Capitan, macOS Sierra, macOS High Sierra, macOS Mojave, WatchOS 2, WatchOS 3, WatchOS 4 and WatchOS 5, and by advertising, promoting, encouraging, instructing and aiding others, such as resellers and end-user customers, to use, sell, or offer to sell infringing Apple devices within the United States in an infringing matter. Such acts constitute direct infringement.

162. Apple has had actual notice of its infringement of the '502 Patent by no later than July 18, 2017 when it received MPH's letter advising Apple of the '502 Patent and providing a claim chart comparing the claims to Apple's iMessage and FaceTime services. Apple has carried out these actions with the specific intent to induce infringement of the '502 Patent and with knowledge that such acts constitute infringement of the '502 Patent. Other Apple features, including Handoff, Universal Clipboard, iPhone Cellular Call Relay, and iPhone Text Message Forwarding, also use Apple's APNs to support end-to-end encryption and, thus, Apple further infringes the foregoing claims of the '502 Patent under 35 U.S.C. § 271(b).

163. Apple has also contributed to the infringement of at least claims 1, 2, 7, 8, 9, and 10 of the '502 Patent under 35 U.S.C. § 271(c) by, among other things, making, using, selling, offering for sale, and importing into the United States the infringing Apple devices, including iPhones, iPads, iPods, Apple Watches, and Mac computers running the following Apple operating systems, as well as all other software versions which provide the same or substantially the same features and functionalities: iOS 8, iOS 9, iOS 10, iOS 11, iOS 12, OS X Yosemite, OS X El Capitan, macOS Sierra, macOS High Sierra, macOS Mojave, WatchOS 2, WatchOS 3, WatchOS 4 and WatchOS 5, and by advertising, promoting, encouraging, instructing and aiding others, such as end-user customers, to use them in an infringing manner. Apple has engaged in these activities knowing that these Apple devices are especially made and adapted for use, and in fact used, in a manner that

constitutes infringement of the '502 Patent. These Apple devices configured with Apple's software constitute material parts of the patented inventions of the '502 Patent, which are not staple articles of commerce suitable for substantial non-infringing uses. The direct infringers for Apple's contributory infringement under 35 U.S.C. § 271(c) include, without limitation, users and resellers of the infringing Apple devices. Other Apple features, including Handoff, Universal Clipboard, iPhone Cellular Call Relay, and iPhone Text Message Forwarding, also use Apple's APNs to support end-to-end encryption and, thus, Apple further infringes the foregoing claims of the '502 Patent under 35 U.S.C. § 271(c).

164. The acts of infringement of the '502 Patent by Apple have injured MPH, and MPH is entitled to recover damages adequate to compensate it for such infringement from Apple, but in no event less than a reasonable royalty. Further, the acts of infringement of the '502 Patent by Apple have injured and will continue to injure MPH unless and until this Court enters an injunction prohibiting further infringement of the '502 Patent.

165. Apple's infringement of the '502 Patent has been and continues to be willful, wanton, malicious, in bad faith, deliberate, consciously wrong, and flagrant. MPH provided Apple with notice of Apple's infringement of the '502 Patent by at least July 18, 2017, including with claim charts comparing the claims to Apple's iMessage and FaceTime services. Despite knowledge of its infringement, Apple continues its acts of infringement of the '502 patent, as stated above. As such, Apple's infringement of the '502 Patent is willful.

COUNT V - INFRINGEMENT OF U.S. PATENT NO. 9,838,362

166. MPH incorporates by reference paragraphs 1-165 as if fully set forth herein.

167. As described below, Apple has infringed and continues to infringe, literally or through the doctrine of equivalents, at least claims 1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14, and 16 of the '362 Patent.

168. The Apple iMessage and FaceTime services enable Apple devices to send and receive secure messages over a telecommunications network, i.e., the Internet.

169. Apple utilizes intermediate servers, including its APNs servers, to send and receive messages to provide the iMessage and FaceTime services.

170. Apple controls, owns, and operates servers used for the iMessage and FaceTime services, including the APNs servers.

171. Apple's servers used for iMessage and FaceTime, including its APNs servers, are connected to the Internet.

172. Apple's servers used for iMessage and FaceTime, including its APNs servers, are configured with one or more IP addresses. An entire address block is assigned to Apple.

173. Apple's servers, including its APNs servers, are configured to receive secure messages from Apple devices to provide the iMessage and FaceTime services. The payloads of messages are encrypted using encryption keys from a key exchange protocol.

174. A device token is a unique identifier assigned by Apple to a specific app on a specific Apple device. Messages sent through iMessage and FaceTime include a device token that identifies a unique app-device combination. Apple's servers, including its APNs servers, are configured to decrypt these device tokens and use such tokens to locate the intended recipients of a message through mapping. Apple's APNs servers map device tokens with connections to receiving devices. Apple's servers, including its APNs servers, forward encrypted message payloads to the receiving Apple devices. The decrypted tokens are included with the encrypted message payloads.

175. Apple's APNs do not have the keys to decrypt the payloads of messages or data sent through the iMessage and FaceTime services.

176. Apple's APNs are not configured to access the keys to decrypt the payloads of messages or data sent through the iMessage and FaceTime services.

177. Apple utilizes a table to map a device token to connection information of the receiving device including location or address. Such mapping occurs at Apple's APNs servers.

178. Apple's APNs servers and Apple devices sending and receiving messages through iMessage and FaceTime communicate using a TLS protocol.

179. Based on the above, Apple has infringed and continues to infringe at least claims 1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14, and 16 of the '362 Patent under 35 U.S.C. § 271(a) by, among other things, making, using, operating, and importing into the United States the servers, such as APNs servers, and associated software that support its iMessage and FaceTime services on Apple devices,

including iPhones, iPads, iPods, Apple Watches, and Mac computers running the following Apple operating systems, as well as all other software versions which provide the same or substantially the same features and functionalities: iOS 8, iOS 9, iOS 10, iOS 11, iOS 12, OS X Yosemite, OS X El Capitan, macOS Sierra, macOS High Sierra, macOS Mojave, WatchOS 2, WatchOS 3, WatchOS 4 and WatchOS 5. Other Apple features, including Handoff, Universal Clipboard, iPhone Cellular Call Relay, and iPhone Text Message Forwarding, also use Apple's APNs to support end-to-end encryption and, thus, Apple further infringes the foregoing claims of the '362 Patent under 35 U.S.C. § 271(a).

180. The acts of infringement of the '362 Patent by Apple have injured MPH, and MPH is entitled to recover damages adequate to compensate it for such infringement from Apple, but in no event less than a reasonable royalty. Further, the acts of infringement of the '362 Patent by Apple have injured and will continue to injure MPH unless and until this Court enters an injunction prohibiting further infringement of the '362 Patent.

181. Apple's infringement of the '362 Patent has been and continues to be willful, wanton, malicious, in bad faith, deliberate, consciously wrong, and flagrant. MPH, among other things, provided Apple with notice of the pendency of U.S. Patent Application No. 15/609,312, which issued as the '362 Patent, by at least July 18, 2017. Despite knowledge of its infringement of the related '949, '397, '494 and '502 Patents, and application which issued as the '362 Patent, Apple continued and continues its acts of infringement of the '362 Patent, as stated above. As such, Apple's infringement of the '362 Patent is willful.

COUNT VI - INFRINGEMENT OF U.S. PATENT NO. 7,620,810

182. MPH incorporates by reference paragraphs 1-181 as if fully set forth herein.

183. As described below, Apple has infringed and continues to infringe, literally or through the doctrine of equivalents, claims 1-7 of the '810 Patent.

184. Apple designed the accused Apple MOBIKE-implemented products with the specific intent that they be capable of being used, and would in fact be used, as part of a method for ensuring that messages would be forwarded in a secure manner in a telecommunications network.

185. The accused Apple MOBIKE-implemented products are mobile terminals that can

have a first address that can have a secure connection with an address of a security gateway.

186. The accused Apple MOBIKE-implemented products are mobile and can change from a first address to a second address.

187. As noted above, while connected through a VPN connection to a security gateway, the accused Apple MOBIKE-implemented products send the packet shown in the Initiator column of step 3 on page 7 of RFC 4555 to the security gateway when moving from a first address to a second address. That packet is a request message that is sent to the address of the security gateway to request that the security gateway change the secure connection to be defined between the second address and the address of the security gateway.

188. Upon receiving the packet shown in the Initiator column of step 3 on page 7 of RFC 4555, the security gateway changes the address definition of the accused Apple MOBIKE-implemented product with which it is connected from the first address to the second address. Thereafter, the accused Apple MOBIKE-implemented product is configured to send a secure message in a secure connection from its second address to another terminal such as another accused Apple MOBIKE-implemented product that is mobile via the security gateway. The other accused Apple MOBIKE-implemented product is configured to send a message back to the second address of the accused Apple MOBIKE-implemented product. The other accused Apple MOBIKE-implemented product sends the message via the security gateway.

189. The accused Apple MOBIKE-implemented products are configured to establish secure connections with a VPN gateway or server using the IPsec protocol which forms a Security Association.

190. The accused Apple MOBIKE-implemented products are configured to encrypt and authenticate the request message shown in the Initiator column of step 3 on page 7 of RFC 4555 to the security gateway using the same security association that was used for the secure connection between the first address of the accused Apple MOBIKE-implemented products and the security gateway.

191. The accused Apple MOBIKE-implemented products are configured to receive a reply message such as the message shown in the Responder column of step 3 on page 7 of RFC 4555,

namely, the following:

```
<-- (IP_R1:4500 -> IP_I2:4500)
    HDR, SK { N(NAT_DETECTION_SOURCE_IP),
          N(NAT_DETECTION_DESTINATION_IP) }
```

192. The reply message shown above is configured to confirm the address change when an accused Apple MOBIKE-implemented product moves from a first IP address to a second IP address.

193. The IPsec protocol used to establish the secure connection between an accused Apple MOBIKE-implemented product and a security gateway is a tunneling protocol.

194. Apple designed the accused Apple MOBIKE-implemented products to implement and enable MOBIKE.

195. Apple provides its iOS deployment reference to guide and instruct its customers and end users on how to deploy accused Apple MOBIKE-implemented products in private corporate networks using VPN protocols.

196. Apple provides its iOS deployment reference to guide and instruct its customers and end users on how to deploy accused Apple MOBIKE-implemented products in private corporate networks using VPN protocols including IKEv2 and MOBIKE.

197. Apple provides its iOS deployment reference to guide and instruct its customers and end users on how to deploy accused Apple MOBIKE-implemented products including VPN Setup Guidelines with an IKEv2 setup.

198. Apple provides iOS and macOS Security whitepapers that encourage the use of accused Apple MOBIKE-implemented products in virtual private networking.

199. Apple published the iOS Deployment Overview for Business whitepaper to encourage customers and end users to securely access company resources remotely via their iOS devices.

200. Apple provides programs including Apple Configurator, Apple School Manager and Apple Business Manager and instructions for using the programs including, for example, to configure accused Apple MOBIKE-implemented products for use in virtual private networking.

201. Apple has knowingly and actively induced infringement of claims 1-7 of the ‘810

Patent under 35 U.S.C. §271(b) by, among other things, selling and offering for sale in the United States, and importing into the United States, Apple devices including iPhones, iPads, iPod Touch and Mac computers running the following Apple operating systems that provide IKEv2 type VPN and enable MOBIKE, as well as all other software versions which provide the same or substantially the same features and functionalities: iOS 8, iOS 9, iOS 10, iOS 11, iOS 12, OS X El Capitan, macOS Sierra, macOS High Sierra and macOS Mojave, and by advertising, aiding, encouraging and instructing others, such as its enterprise and other end-user customers, including without limitation, those that use AppleCare for Enterprise, to use them in an infringing manner. Such direct infringers include customers such as corporations and other entities setting up IKEv2 type MOBIKE enabled virtual private networks to make sure users are able to securely access resources remotely via, for example, their iOS devices.

202. Apple has had actual notice of its infringement of the ‘810 Patent by no later than October 17, 2016 when it received MPH’s letter advising Apple of the ‘810 Patent and providing a detailed claim chart applying the ‘810 Patent to Apple’s iOS and OS X/macOS devices. Apple has carried out these actions with the specific intent to induce infringement of the ‘810 Patent and with knowledge that such acts constitute infringement of the ‘810 Patent.

203. Apple has also contributed to the infringement of claims 1-7 of the ‘810 Patent under 35 U.S.C. §271(c) by, among other things, selling and offering for sale in the United States, and importing into the United States, Apple devices including iPhones, iPads, iPod Touch and Mac computers running the following Apple operating systems that provide IKEv2 type VPN and enable MOBIKE, as well as all other software versions which provide the same or substantially the same features and functionalities: iOS 8, iOS 9, iOS 10, iOS 11, iOS 12, OS X El Capitan, macOS Sierra, macOS High Sierra and macOS Mojave, and by advertising, promoting, encouraging, instructing and aiding others, such as end-user customers, to use them in an infringing manner. Apple has engaged in these activities knowing that the Apple devices running operating systems that provide IKEv2 type VPN and enable MOBIKE are especially made and adapted for use, and in fact used, in a manner that constitutes infringement of the ‘810 Patent. These instrumentalities constitute material parts of the patented inventions of the ‘810 Patent which are not staple articles of commerce suitable for

substantial non-infringing uses.

204. The direct infringers for Apple's contributory infringement under 35 U.S.C. §271(c) include, without limitation, users that use the accused Apple MOBIKE-implemented products in an enterprise IKEv2 MOBIKE enabled VPN to make sure users are able to securely access resources remotely via, for example, their iOS devices, including without limitation, those users or customers that use AppleCare for Enterprise.

205. The acts of infringement of the '810 Patent by Apple have injured MPH, and MPH is entitled to recover damages adequate to compensate it for such infringement from Apple, but in no event less than a reasonable royalty. Further, the acts of infringement of the '810 Patent by Apple have injured and will continue to injure MPH unless and until this Court enters an injunction prohibiting further infringement of the '810 Patent.

206. Apple's infringement of the '810 Patent has been and continues to be willful, wanton, malicious, in bad faith, deliberate, consciously wrong, and flagrant. MPH provided Apple with notice of Apple's infringement of the '810 Patent by at least October 17, 2016 including detailed claim charts for the '810 Patent showing the relevance of the '810 Patent to Apple's adoption and implementation of "MOBIKE" technologies (IETF RFC 4555) in its iOS and OS X/macOS device. With full awareness of the '810 Patent, and despite the knowledge that its actions would induce others to infringe and contribute to the infringement of others of the '810 Patent, Apple continued selling and offering for sale in the United States, and importing into the United States, the accused Apple MOBIKE-implemented products.

COUNT VII - INFRINGMENT OF U.S. PATENT NO. 7,937,581

207. MPH incorporates by reference paragraphs 1-206 as if fully set forth herein.

208. As described below, Apple has infringed and continues to infringe, literally or through the doctrine of equivalents, claims 1-9 of the '581 Patent.

209. Apple designed the accused Apple MOBIKE-implemented products with the specific intent that they be capable of being used, and would in fact be used, as part of a method for ensuring that messages would be forwarded in a secure manner in a telecommunications network.

210. The accused Apple MOBIKE-implemented products are mobile terminals that can

have a first address as first end-point that can have a secure connection with an address of a security gateway as a second end-point.

211. The accused Apple MOBIKE-implemented products are mobile and can change from a first address to a second address.

212. As noted above, while connected through a VPN connection to a security gateway, the accused Apple MOBIKE-implemented products send the packet shown in the Initiator column of step 3 on page 7 of RFC 4555 to the security gateway when moving from a first address to a second address. That packet is a request message that is sent to the address of the security gateway to request that the security gateway change the secure connection to be defined between the second address and the gateway address of the security gateway.

213. Upon receiving the packet shown in the Initiator column of step 3 on page 7 of RFC 4555, the security gateway changes the address definition of the secure connection of the accused Apple MOBIKE-implemented product with which it is connected from the first address to the second address. Thereafter, the accused Apple MOBIKE-implemented product is configured to send a secure message in a secure connection from its second address to another terminal such as another accused Apple MOBIKE-implemented product that is mobile via the security gateway.

214. The accused Apple MOBIKE-implemented products are configured to establish secure connections with a VPN gateway or server using the IPsec protocol which forms a Security Association.

215. The accused Apple MOBIKE-implemented products are configured to encrypt and authenticate the request message shown in the Initiator column of step 3 on page 7 of RFC 4555.

216. The accused Apple MOBIKE-implemented products are configured to receive a reply message such as the message shown in the Responder column of step 3 on page 7 of RFC 4555, namely, the following:

```
<-- (IP_R1:4500 -> IP_I2:4500)
    HDR, SK { N(NAT_DETECTION_SOURCE_IP),
              N(NAT_DETECTION_DESTINATION_IP) }
```

217. The accused Apple MOBIKE-implemented products are configured to receive reply

message above after the request from the accused Apple MOBIKE-implemented products to change the address.

218. The accused Apple MOBIKE-implemented products are configured to receive the reply message above that is encrypted and authenticated.

219. The reply message set forth above is sent back from the security gateway to the accused Apple MOBIKE-implemented product, which is a mobile terminal, at the second address to confirm the address change.

220. The accused Apple MOBIKE-implemented products are configured to establish an end-to-end connection with, for example, another accused Apple MOBIKE-implemented product, using an IPsec tunnel connection for the secure connection.

221. The other accused Apple MOBIKE-implemented product is configured to send a message back to the second address of the accused Apple MOBIKE-implemented product. The other accused Apple MOBIKE-implemented product sends the message via the security gateway. When the security gateway receives the message from the other accused Apple MOBIKE-implemented product, the security gateway forwards the message as an encrypted message to the second address of the accused Apple MOBIKE-implemented product.

222. The IPsec protocol used to establish the secure connection between an accused Apple MOBIKE-implemented product and a security gateway is a tunneling protocol.

223. Apple designed the accused Apple MOBIKE-implemented product to be MOBIKE enabled.

224. Apple provides its iOS deployment reference to guide and instruct its customers and end users on how to deploy accused Apple MOBIKE-implemented products in private corporate networks using VPN protocols.

225. Apple provides its iOS deployment reference to guide and instruct its customers and end users on how to deploy accused Apple MOBIKE-implemented products in private corporate networks using VPN protocols including IKEv2 and MOBIKE.

226. Apple provides its iOS deployment reference to guide and instruct its customers and end users on how to deploy accused Apple MOBIKE-implemented products including VPN Setup

Guidelines with an IKEv2 setup.

227. Apple provides iOS and macOS Security whitepapers that encourage the use of accused Apple MOBIKE-implemented products in virtual private networking.

228. Apple published the iOS Deployment Overview for Business whitepaper to encourage customers and end users to securely access company resources remotely via their iOS devices.

229. Apple provides programs including Apple Configurator, Apple School Manager and Apple Business Manager and instructions for using the programs including, for example, to configure accused Apple MOBIKE-implemented products for use in virtual private networking.

230. Apple has knowingly and actively induced infringement of claims 1-9 of the '581 Patent under 35 U.S.C. §271(b) by, among other things, selling and offering for sale in the United States, and importing into the United States, Apple devices including iPhones, iPads, iPod Touch and Mac computers running the following Apple operating systems that provide IKEv2 type VPN and enable MOBIKE, as well as all other software versions which provide the same or substantially the same features and functionalities: iOS 9, iOS 10, iOS 11, iOS 12 OS X El Capitan, macOS Sierra, macOS High Sierra and macOS Mojave, and by advertising, aiding, encouraging and instructing others, such as its enterprise and other end-user customers, including without limitation, those that use AppleCare for Enterprise, to use them in an infringing manner. Such direct infringers include customers such as corporations and other entities setting up IKEv2 type MOBIKE enabled virtual private networks to make sure users are able to securely access resources remotely via, for example, their iOS devices.

231. Apple has had actual notice of its infringement of the '581 Patent by no later than October 17, 2016 when it received MPH's letter advising Apple of the '581 Patent and providing a detailed claim chart applying the '581 Patent to Apple's iOS and OS X/macOS devices. Apple has carried out these actions with the specific intent to induce infringement of the '581 Patent and with knowledge that such acts constitute infringement of the '581 Patent.

232. Apple has also contributed to the infringement of claims 1-9 of the '581 Patent under 35 U.S.C. §271(c) by, among other things, selling and offering for sale in the United States, and importing into the United States, Apple devices including iPhones, iPads, iPod Touch and Mac

computers running the following Apple operating systems that provide IKEv2 type VPN and enable MOBIKE, as well as all other software versions which provide the same or substantially the same features and functionalities: iOS 9, iOS 10, iOS 11, iOS 12, OS X El Capitan, macOS Sierra, macOS High Sierra and macOS Mojave, and by advertising, promoting, encouraging, instructing and aiding others, such as end-user customers, to use them in an infringing manner. Apple has engaged in these activities knowing that the Apple devices running operating systems that provide IKEv2 type VPN and enable MOBIKE are especially made and adapted for use, and in fact used, in a manner that constitutes infringement of the '581 Patent. These instrumentalities constitute material parts of the patented inventions of the '581 Patent which are not staple articles of commerce suitable for substantial non-infringing uses. The direct infringers for Apple's contributory infringement under 35 U.S.C. §271(c) including, without limitation, users that use the accused Apple MOBIKE-implemented products in an enterprise IKEv2 MOBIKE enabled VPN to make sure users are able to securely access resources remotely via, for example, their iOS devices, including without limitation, those users or customers that use AppleCare for Enterprise.

233. The acts of infringement of the '581 Patent by Apple have injured MPH, and MPH is entitled to recover damages adequate to compensate it for such infringement from Apple, but in no event less than a reasonable royalty. Further, the acts of infringement of the '581 Patent by Apple have injured and will continue to injure MPH unless and until this Court enters an injunction prohibiting further infringement of the '581 Patent.

234. Apple's infringement of the '581 Patent has been and continues to be willful, wanton, malicious, in bad faith, deliberate, consciously wrong, and flagrant. MPH provided Apple with notice of Apple's infringement of the '581 Patent by at least October 17, 2016 including detailed claim charts for the '581 Patent showing the relevance of the '581 Patent to Apple's adoption of "MOBIKE" technologies (IETF RFC 4555) in its iOS and OS X/macOS device. With full awareness of the '581 Patent, and despite the knowledge that its actions would induce others to infringe and contribute to the infringement of others of the '581 Patent, Apple continued selling, offering for sale and importing into the United States the accused Apple MOBIKE-implemented products.

COUNT VIII - INFRINGEMENT OF U.S. PATENT NO. 8,037,302

235. MPH incorporates by reference paragraphs 1-234 as if fully set forth herein.

236. As described below, Apple has infringed and continues to infringe, literally or through the doctrine of equivalents, at least claims 1, 2, 3, 4, 5, 6, 9, 10, 11, 13, and 16 of the '302 Patent.

237. Apple provides Always-on VPN on Apple iOS devices, including iPhones and iPads, running iOS 8, iOS 9, iOS 10, and iOS 11. Apple encourages and instructs its customers how to enable, set up, and configure Always-on VPN.

238. Apple's Always-on VPN enables devices to simultaneously connect to two secure network connections, i.e., a Wi-Fi connection and a cellular connection. With the Always-on VPN feature, Apple devices can move between networks, such as from a Wi-Fi connection to cellular connection and vice-versa, without reestablishing the connection.

239. When an Apple device using Always-on VPN has both Wi-Fi and cellular connections, it automatically establishes two secure VPN connections, a first secure connection over Wi-Fi and a second secure cellular connection. When a device is connected to Wi-Fi, the Wi-Fi VPN connection is used for traffic, whereas the cellular VPN connection is used as a backup. If a device loses its connection to Wi-Fi, it will use the cellular VPN connection without needing to reestablish the secure connection.

240. An Apple device using Always-on VPN will have two separate IP addresses for simultaneously existing Wi-Fi and cellular VPN connections. Thus, when a device begins using a different connection, i.e., changes from a Wi-Fi to a cellular connection or vice-versa, it will change IP addresses.

241. When an Apple device using Always-on VPN changes to a new address, it will confirm whether a secure connection already exists using a connection table. If it does not, then it will establish the secure connection.

242. An Apple device using Always-on VPN can register a second secure connection for immediate and/or later use.

243. Apple's Always-on VPN uses IKEv2 as the default tunneling protocol to establish secure connections.

244. IKEv2 is a component of IPsec.

245. IKEv2 is a key exchange.

246. Because Always-on VPN uses IKEv2 tunnels to secure traffic, the accused Apple devices send messages using IP packets.

247. Based on the above, Apple has infringed and continues to infringe at least claims 1, 2, 3, 4, 5, 6, 9, 10, 11, 13, and 16 of the '302 Patent under 35 U.S.C. § 271(a) through, among other things, its employees and agents' testing and other use of Always-on VPN on Apple iOS devices, including iPhones and iPads, with the iOS 8, iOS 9, iOS 10, iOS 11 and iOS 12 operating systems with VPN gateways. For example, Apple's direct infringement includes, without limitation, the testing of Always-on VPN for evaluation by the NIAP, as described above.

248. Apple has and continues to knowingly and actively induce infringement of at least claims 1, 2, 3, 4, 5, 6, 9, 10, 11, 13, and 16 of the '302 Patent under 35 U.S.C. § 271(b) by, among other things, selling, offering for sale, and importing in and into the United States infringing Apple iOS devices with the Always-On VPN feature, including iPhones and iPads running the following Apple operating systems, as well as all other software versions which provide the same or substantially the same features and functionalities: iOS 8, iOS 9, iOS 10, iOS 11, and iOS 12 and by advertising, aiding, encouraging and instructing others, such as its enterprise customers, to use the Accused Apple Always-On VPN feature in a manner that directly infringes claims 1, 2, 3, 4, 5, 6, 9, 10, 11, 13, and 16 of the '302 Patent.

249. Apple has had actual notice of its infringement of the '302 Patent by no later than October 18, 2016 when it received MPH's letter advising Apple of the '302 Patent, and further on November 22, 2016 when MPH provided a claim chart comparing the claims to Apple's Always-On VPN feature. Apple has carried out these actions with the specific intent to induce infringement of the '302 Patent and with knowledge that such acts constitute infringement of the '302 Patent.

250. Apple has also contributed to the infringement of at least claims 1, 2, 3, 4, 5, 6, 9, 10, 11, 13, and 16 of the '302 Patent under 35 U.S.C. § 271(c) by, among other things, selling, offering

for sale, and importing in and into the United States infringing Apple iOS devices with the Always-On VPN feature, including iPhones and iPads running the following Apple operating systems, as well as all other software versions which provide the same or substantially the same features and functionalities: iOS 8, iOS 9, iOS 10, iOS 11 and iOS 12, and by advertising, aiding, encouraging and instructing others, such as its enterprise customers, to use the Accused Apple Always-On VPN feature in a manner that directly infringes claims 1, 2, 3, 4, 5, 6, 9, 10, 11, 13, and 16 of the '302 Patent. Apple has engaged in these activities knowing that these Apple devices are especially made and adapted for use, and in fact used, in a manner that constitutes infringement of the '302 Patent. These Apple devices configured with Apple software constitute material parts of the patented inventions of the '302 Patent, which are not staple articles of commerce suitable for substantial non-infringing uses. The direct infringers for Apple's contributory infringement under 35 U.S.C. § 271(c) include, without limitation, its enterprise customers.

251. The acts of infringement of the '302 Patent by Apple have injured MPH, and MPH is entitled to recover damages adequate to compensate it for such infringement from Apple, but in no event less than a reasonable royalty. Further, the acts of infringement of the '302 Patent by Apple have injured and will continue to injure MPH unless and until this Court enters an injunction prohibiting further infringement of the '302 Patent.

252. Apple's infringement of the '302 Patent has been and continues to be willful, wanton, malicious, in bad faith, deliberate, consciously wrong, and flagrant. MPH provided Apple with notice of Apple's infringement of the '302 Patent by at least October 17, 2016. On November 22, 2016, MPH's counsel provided detailed claim charts for the '302 Patent regarding Apple's Always-On VPN feature, further showing the relevance of the MPH patents to Apple's products, including its iOS and OS X/macOS devices. Despite knowledge of its infringement, Apple continues its acts of infringement of the '302 patent, as stated above. As such, Apple's infringement of the '302 Patent is willful.

NOTICE OF INFRINGEMENT AND "EXCEPTIONAL CASE"

253. To the extent required by law, MPH has complied with the applicable provisions of 35 U.S.C. § 287.

254. This is an "exceptional case" under 35 U.S.C. § 285 because it stands out from others with respect to the lack of substantive strength underlying Apple's positions. Accordingly, MPH is entitled to an award of its attorneys' fees.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, MPH, asks this Court to enter judgment against Apple and its subsidiaries, affiliates, agents, servants, employees and all persons in active concert or participation with them, granting the following relief:

A. An award of damages adequate to compensate MPH for the infringement that has occurred, together with prejudgment interest from the date infringement of the patents-in-suit began;

B. An award to MPH of all remedies available under 35 U.S.C. § 154(d) and 35 U.S.C. § 284;

C. An award to MPH of all remedies available under 35 U.S.C. § 285;

D. A permanent injunction under 35 U.S.C. § 283 prohibiting further infringement, inducement of infringement, and contributory infringement of the '949 Patent, '397 Patent, '494 Patent, '502 Patent, '362 Patent, '810 Patent, '581 Patent, and '302 Patent; and

E. Such other and further relief as this Court or a jury may deem proper and just.

JURY DEMAND

MPH demands a trial by jury on all issues so triable.

Dated: September 27, 2018

Respectfully Submitted,

/s/ Patricia L. Peden
Patricia L. Peden, Esq. (SBN 206440)
patricia.peden@leclairryan.com
LECLAIRRYAN, LLP
44 Montgomery Street
Suite 3100
San Francisco, CA 94104
Phone: (415) 391.7111
Fax: (415) 391.8766

Christopher J. Lee
(Pro Hac Vice Application Pending)

clee@leesheikh.com
David J. Sheikh
(Pro Hac Vice Application Pending)
dsheikh@leesheikh.com
Richard B. Megley, Jr.
(Pro Hac Vice Application Pending)
rmegley@leesheikh.com
Brian E. Haan
(Pro Hac Vice Application Pending)
bhaan@leesheikh.com
Ashley E. LaValley
(Pro Hac Vice Application Pending)
alavalley@leesheikh.com
Dragan Gjorgiev
(Pro Hac Vice Application Pending)
dgjorgiev@leesheikh.com
LEE SHEIKH MEGLEY & HAAN LLC
111 West Jackson Boulevard, Suite 2230
Chicago, IL 60604
Phone: (312) 982-0070
Fax: (312) 982-0071

Attorneys for Plaintiff
MPH TECHNOLOGIES OY