UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND
SOUTHERN DIVISION

KEYSEE SOFTWARE LTD.,

Plaintiff,

v.

DIGITAL RECEIVER TECHNOLOGY, INC.,

Defendant.

Civil Action No. _____

JURY TRIAL DEMANDED

ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff KeySee Software Ltd. ("KeySee") files this Original Complaint and demand for jury trial seeking relief for patent infringement by Digital Receiver Technology, Inc. ("DRT"). KeySee states and alleges as follows:

NATURE OF THE ACTION

1. This is a civil action arising out of DRT's patent infringement in violation of the Patent Laws of the United States, U.S.C. §§ 101 *et seq*.

PARTIES

2. Plaintiff KeySee Software Ltd. is an Israeli limited liability company, with its principal place of business located at 12 Habanim St., Kfar-Sirkin, Israel 49935.

3. On information and belief, Defendant DRT is a corporation organized and existing under the laws of the State of Maryland, with its principal place of business located at 12409 Milestone Center Dr., Germantown, Maryland 20876.

4. Defendant DRT may be served through its registered agent, CSC-LAWYERS INCORPORATING SERVICE COMPANY, which is located at 7 Saint Paul Street, Suite 820; Baltimore, MD 21202.

JURISDICTION AND VENUE

5. This action arises under the Patent Laws of the United States. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. §§ 1331 and 1338(a).

6. The Court has personal jurisdiction over DRT because DRT is organized and is existing under the laws of the State of Maryland; because DRT regularly conducts business in the State of Maryland and therefore has substantial and continuous contacts within this judicial district; because DRT has purposefully availed themselves to the privileges of conducting business in this judicial district; and because DRT has committed acts of patent infringement in this judicial district.

7. Venue is proper in this judicial district pursuant to 28 U.S.C. §§ 1391(b) and (c) and 28 U.S.C. § 1400(b) at least because Defendant DRT is organized and is existing under the laws of the State of Maryland and because defendant DRT has a regular and established place of business within this judicial district.

KEYSEE CRYPTANALYSIS PATENTS

8. The patents asserted in this action are U.S. Patent No. 8,009,826; U.S. Patent No. 8,295,477; U.S. Patent No. 9,038,192; and U.S. Patent No. 10,447,666 (collectively, the "Asserted Patents" or "KeySee Cryptanalysis Patents"). The KeySee Cryptanalysis Patents relate to cryptanalysis methods and systems, and more particularly to cryptanalysis methods and systems enabling interception and decryption of encrypted wireless communications.

9. The first named inventor of the KeySee Cryptanalysis Patents is Dr. Elad Barkan. The second named inventor is Prof. Eli Biham. Dr. Barkan received his Ph.D. from the Technion – Israel Institute of Technology. Dr. Barkan's Ph.D. thesis related to security in GSM mobile networks. In connection with his thesis, Dr. Elad Barkan and Prof. Biham developed the inventions claimed in the Asserted Patents. Technion released the invention to inventors, Dr. Barkan and his Ph.D. advisor Prof. Biham, who assigned his rights to Dr. Barkan. Dr. Barkan's work related to security in GSM mobile networks received world-wide coverage in the media. Dr. Barkan eventually commercialized his inventions in KeySee to assist law-enforcement agencies. KeySee is the current assignee of the KeySee Cryptanalysis Patents.

10. On August 30, 2011, the United States Patent and Trademark Office duly and legally issued U.S. Patent 8,009,826 ("the '826 patent"), entitled "Cryptoanalysis Method and System." The '826 patent is duly and legally assigned to KeySee, which is the assignee of all right, title, and interest in and to the '826 patent and possesses the exclusive right of recovery for past, present, and future infringement. A true and correct copy of the '826 patent is attached as **Exhibit A**.

11. On October 23, 2012, the United States Patent and Trademark Office duly and legally issued U.S. Patent 8,295,477 ("the '477 patent"), entitled "Cryptoanalysis Method and System." The '477 patent is duly and legally assigned to KeySee, which is the assignee of all right, title, and interest in and to the '477 patent and possesses the exclusive right of recovery for past, present, and future infringement. A true and correct copy of the '477 patent is attached as **Exhibit B**.

12. On May 19, 2015, the United States Patent and Trademark Office duly and legally issued U.S. Patent 9,038,192 ("the '192 patent"), entitled "Cryptoanalysis Method and System."

The ’192 patent is duly and legally assigned to KeySee, which is the assignee of all right, title, and interest in and to the ’192 patent and possesses the exclusive right of recovery for past, present, and future infringement. A true and correct copy of the ’192 patent is attached as **Exhibit C**.

13. On October 15, 2019, the United States Patent and Trademark Office duly and legally issued U.S. Patent 10,447,666 (“the ’666 patent”), entitled “Cryptoanalysis Method and System.” The ’666 patent is duly and legally assigned to KeySee, which is the assignee of all right, title, and interest in and to the ’666 patent and possesses the exclusive right of recovery for past, present, and future infringement. A true and correct copy of the ’666 patent is attached as **Exhibit D**.

14. The KeySee Cryptanalysis Patents share a common specification and are generally directed to a novel and inventive technical solution to a problem relating to computer and networking technology, and in particular, to ciphertext-only cryptanalysis of encrypted messages under the GSM cellular network protocol. *See*, *e.g.*, Exhibit A (’826 patent) at 1:5-7, 1:14-25, and Abstract.

15. Encryption of messages is frequently attained by the use of an encryption key per session which is generated by sophisticated algorithms, and which is only known to the sender and the intended recipient. The sender takes unencrypted data (“plaintext”) and uses a secret session key generated by an algorithm, to convert the plaintext into encrypted data (“ciphertext”). The recipient uses a similar algorithm, to generate the secret session key, and uses it to convert the ciphertext back into the original plaintext. Cryptanalysis refers to methods that allow a person, known as an “attacker,” to decrypt encrypted messages and gain the unencrypted contents of the encrypted messages without prior knowledge of the used session

key. Frequently, the aim of cryptanalysis is to determine the secret session key and then use it to decipher all communications which were encrypted using that key. However, in some cases decryption can be achieved without the attacker gaining access to the session key.

16. All cryptanalyses rely on known or assumed information about the plaintext as well as the encryption algorithm. The prior knowledge on the plaintext is called "redundancy." In some cases, the requisite redundancy can only be secured by gaining actual access to plaintext, and to the corresponding ciphertext, and using this information to infer the value of the secret session key. This is called a known-plaintext attack. However, this is not a practical solution, since in real life scenarios it is unlikely that the attacker will have the opportunity to gain access to plaintext messages prior to encryption. Consequently, known-plaintext attacks are largely academic, and have little practical utility. In most scenarios, the attacker only has access to ciphertext, and has no access to plaintext. Instead, the attacker may use other information about the plaintext, such as what human language it is in, protocol structure and behavior, guessing anticipated plaintext message or some other structural constraint, together with some knowledge of the encryption algorithm to aid in the cryptanalysis. In such cases, cryptanalyses is far more challenging, since it is more difficult to find sufficient redundancies that would facilitate the cryptanalysis. Cryptanalysis in which the attacker has no access to plaintext messages before they were encrypted is known as ciphertext-only cryptanalysis.

17. The GSM cellular network protocol is a well-known and widely used protocol for cellular communications. GSM was first introduced in 1991, and soon became one of two dominant second-generation (2G) cellular network protocols. Although cellular technology has advanced to now include 3G, 4G, and 5G network protocols, hundreds of millions of GSM capable devices remain in circulation around the world, and most United States mobile carriers

continued to support GSM devices at least through 2020. Moreover, in many countries outside of the United States, GSM devices are ubiquitous and cellular networks continue to support GSM communications. Accordingly, law enforcement and intelligence agencies seeking to intercept encrypted cellular communications have had, and continue to have, a need for solutions that are capable of cryptanalysis of GSM encrypted communications. Moreover, because such agencies have a need to intercept and decrypt encrypted GSM communications for which they do not have access to the data prior to its encryption (i.e. to plaintext), such agencies need the ability to perform ciphertext-only cryptanalysis on encrypted GSM communications.

18. In reference to the prior art, the KeySee Cryptanalysis Patents explain that certain theoretical work existed that proposed known-plaintext attacks on one variant of the GSM encryption algorithm. *See, e.g., id.* at 2:32-3:55. These theoretical attacks were not feasible in real-life as they were missing the critical part of how to gain the required redundancy. As such, they were not practical solutions for interception and decryption of encrypted GSM communications in real world situation and were largely employed as academic tools to assess the strength of such ciphers. *See*, *e.g.*, *id.* at 1:26-39.

19. The inventions of the KeySee Cryptanalysis Patents provide technical solutions to the aforementioned problems in the prior art. The KeySee Cryptanalysis Patents seek to address these and other problems in the prior art by providing non-conventional, novel solutions that allow for effective, fast, time-efficient ciphertext-only cryptanalysis of encrypted communications over wireless communication networks. *See*, *e.g.*, *id.* at 1:36-39, 6:10-56, 7:54-60, 8:26-34, 10:13-21, 11:14-15, and 12:23-25. The inventions of the KeySee Cryptanalysis Patents further provide for improved computer and network operation by enabling such cryptanalysis using reasonable amounts of computer resources such as computer memory. *See*,

e.g., *id.* The KeySee Cryptanalysis Patents further provide for improved computer and network operation by enabling such cryptanalysis to recover the session encryption key even without prior knowledge such as the used session key, and without access to the original unencrypted messages. *See*, *e.g.*, *id.* at 5:56-6:5, 7:54-60, 7:64-8:9, 8:22-25, 12:33-43, and 13:21-28.

20. Furthermore, the patents teach a variety of novel active attacks in which the attacker poses as either the mobile phone or as the base station with which it communicates or both, and can allow the attacker to intercept communication of a base station using one encryption scheme—typically harder to cryptanalyze, while using a more convenient encryption algorithm or settings towards the mobile phone, where the attacker needs to cryptanalyze just the communication with the mobile phone and use the result to encrypt/decrypt communication towards the base station. *See*, *e.g.*, *id.* at 5:56-6:5, 7:54-60, 7:64-8:9, 8:22-25, 12:33-43, and 13:21-28.

21. Prior to the discovery of the inventions of the KeySee Cryptanalysis Patents, there were no known mechanisms for ciphertext-only cryptanalysis of GSM encrypted communications. The solution to the problem of ciphertext-only cryptanalysis of encrypted GSM communications provided by the inventions of the KeySee Cryptanalysis Patents was a pioneering technological breakthrough in the field of cryptography that enabled for the first time sophisticated active ciphertext-only attacks on encrypted GSM communications.

GENERAL ALLEGATIONS

22. On information and belief, DRT uses, manufactures, and sells products and services, including past and current versions, and including without limitation those marketed as DRTBOX IMSI-catcher, DRT Flashpoint, Multi-Protocol Survey, and Software-Defined Radios (SDRs), that are capable of performing ciphertext-only interception and decryption of encrypted

GSM wireless communications (collectively, the "Wireless Interception Products"). *See*, *e.g.*, **Exhibit E** (DRT webpage) and **Exhibit F** (DRT presentation).

23. Because access to the DRT Wireless Interception Products and in particular its code is limited to DRT and possibly to its customers, and because DRT does not publicize details of how its Wireless Interception Products intercept and decrypt encrypted GSM wireless communications, KeySee has been unable to establish with certainty that the DRT Wireless Interception Products infringe the KeySee Cryptanalysis Patents. Nonetheless, upon information and belief based on a reasonable investigation under the circumstances, there are no known methods for ciphertext-only cryptanalysis of encrypted GSM wireless communications that do not infringe at least one claim of each of the KeySee Cryptanalysis Patents. Accordingly, KeySee has a good-faith, reasonable belief that the DRT manufacture and sale of the Wireless Interception Products directly or indirectly infringe at least one claim of each of the KeySee Cryptanalysis Patents.

24. In order to confirm KeySee's belief that the DRT Wireless Interception Products infringe at least one claim of each of the KeySee Cryptanalysis Patents, on September 25, 2020, counsel for KeySee, Mr. Carl Bruce, sent a letter via Federal Express to Mr. Jay Turner, President of DRT, informing DRT of the KeySee Cryptanalysis Patents, requesting information concerning DRT's Wireless Interception Products that would allow KeySee to confirm whether those products infringed the KeySee Cryptanalysis Patents, and requesting an opportunity to discuss licensing terms with DRT for the Wireless Interception Products. A copy of the letter is attached as **Exhibit G**, and the proof of its delivery is attached as **Exhibit H** (showing that DRT received the letter on September 29, 2020). Neither Mr. Turner nor anyone else from DRT responded to the September 25, 2020 letter.

25. On October 19, 2020, Mr. Bruce sent a subsequent letter via Federal Express to Mr. Turner. **Exhibit I**. When DRT failed to respond to this letter, Mr. Bruce sent third letter to Mr. Turner on November 16, 2020 and copied DRT's registered agent, CSC-LAWYERS INCORPORATING SERVICE COMPANY. **Exhibit J**.

26. Despite repeated attempts to contact DRT about the KeySee Cryptanalysis Patents, DRT failed to respond to any of the letters.

27. Because DRT has refused to respond to KeySee's inquiries, KeySee has not been able to confirm DRT's infringement. Therefore, relying on the precedent established in *Hoffman-La Roche, Inc., v. Invamed Inc.*, 213 F.3d 1359 (Fed. Cir. 2000), and on information and belief, KeySee alleges that DRT has made, used, sold, and offered for sale within the United States, and is currently making, using, selling, and offering for sale within the United States, systems, including at least the Wireless Interception Products, that are covered by at least one claim, or that perform methods covered by at least one claim, of each of the KeySee Cryptanalysis Patents.

COUNT ONE: INFRINGEMENT OF U.S. PATENT NO. 8,009,826

28. All of the allegations set forth in the preceding paragraphs are incorporated herein by reference.

29. KeySee Cryptanalysis Patents including the '826 patent, as discussed above, are generally directed to a novel and inventive technical solution to a problem relating to computer and networking technology, and in particular to the problems of network security and cryptanalysis, which includes lawful interception and decryption of encrypted communications, in wireless communication systems. The '826 patent claims a particular technique of recovering an encryption key used to encrypt wireless communications between a cellular network and a mobile device such that another party can, for example, decrypt the communications. Further, the

claims of the ’826 patent cover systems and methods for performing an effective ciphertext-only cryptanalysis of encrypted communications received off the air to recover the encryption key. For example, claim 1 of the ’826 patent, which is a system for decrypting an encrypted cellular signal, includes a transmitter, receiver, and processing circuitry to recover the encryption key. In sum, the ’826 patent provides significant improvements in computer-related technology and solves computer and network-related problems with technical solutions. Furthermore, the inventions claimed in the ’826 patent provided the first known solutions to the problem of ciphertext-only cryptanalysis of GSM encrypted communications. The inventions claimed in ’826 patent thus provide a solution to a problem for which there was no conventional solution in the prior art.

30. On information and belief, DRT uses KeySee’s patented features of the ’826 patent in its Wireless Interception Products in violation of KeySee’s patent rights. DRT’s Wireless Interception Products include radio technology, such as SDRs, that transmit, receive, and process wireless signals. *See*, *e.g.*, Exhibit E (DRT webpage). Further, DRT’s Wireless Interception Products provide a multi-protocol survey capability that supports simultaneously surveying a number of modern 2G, 3G, and 4G technologies including GSM, cdma2000, 1xEV-DO, UMTS WCDMA, TD-SCDMA, and LTE. Exhibit F (DRT presentation) at p. 10. On information and belief, DRT’s Wireless Interception Products practice one or more claims of the ’826 patent by performing, for example, a ciphertext-only cryptanalysis of encrypted GSM communications.

31. On information and belief, all encrypted GSM communications are first encoded according to an error correction coding scheme before encryption. On information and belief, the ciphertext-only cryptanalysis of encrypted GSM communications performed by DRT’s Wireless

Interception Products is performed by XORing together bits of the encrypted digital communication based on an error correction coding scheme or XORing bits of said encrypted digital communication with bits which are an output of an error correction coding scheme, or both.

32. In violation of 35 U.S.C. § 271, DRT has infringed, contributed to the infringement of, and/or induced others to infringe the ’826 patent by, among other things, making, using, offering to sell, selling, and/or importing into the United States unlicensed systems, products, and/or services in a manner that infringes one or more of at least claims 1, 4, 5, 6, 7, 10, and 11 of the ’826 patent. Such unlicensed systems, products, and/or services include, by way of example and without limitation, DRT’s Wireless Interception Products. In addition, on information and belief, customers of DRT directly infringe the ’826 patent by putting the Wireless Interception Products into service by, for example, using the Wireless Interception Products to recover encryption keys which are used to encrypt wireless communications.

33. DRT has directly infringed the ’826 patent by making, using, offering to sell, selling, and/or importing the Wireless Interception Products in violation of 35 U.S.C. § 271(a). On information and belief, such manufacture, sale, and use directly infringes at least claims 1, 4, 5, 6, 7, 10, and 11 of the ’826 patent.

34. On information and belief, DRT takes steps to actively induce infringement by others of one or more of at least claims 1, 4, 5, 6, 7, 10, and 11 of the ’826 patent in violation of 35 U.S.C. § 271(b), including customers that purchase the Wireless Interception Products. Such active steps include, but are not limited to encouraging, advertising (including by websites such as https://www.drti.com/), promoting, and training others to use and/or how to use the Wireless Interception Products. *See* Exhibit E (DRT webpage).

35. On information and belief, DRT knew or should have known that such activities induce others to directly infringe one or more of at least claims 1, 4, 5, 6, 7, 10, and 11 of the '826 patent. For example, DRT knows or should have known that its actions induce others to directly infringe the '826 patent because DRT knows or should have known about the existence of the '826 patent, especially given the fact that KeySee through its counsel sent letters as discussed above to DRT's CEO Mr. Turner informing DRT about the '826 patent as early as September 29, 2020, the day on which DRT received the letter. *See* Exhibit H (showing that DRT received the letter on September 29, 2020). Moreover, there can be no question that DRT has had actual knowledge of the '826 patent and detailed knowledge of its own infringement since the day when it was served with this complaint.

36. On information and belief, DRT contributes to the infringement of at least claims 1, 4, 5, 6, 7, 10, and 11 of the '826 patent by others, including its customers, distributors, and/or authorized resellers in violation of 35 U.S.C. § 271(c). Acts by DRT that contribute to the infringement of others include, but are not limited to, the sale and offer for sale by DRT of the Wireless Interception Products. DRT's Wireless Interception Products are especially made for or adapted for use to infringe the '826 patent and are not a staple article of commerce and are not suitable for substantial non-infringing use. By way of example, the interception and decryption properties of the DRT's Wireless Interception Products are all evidence that these products are especially made or adapted to infringe the '826 patent.

37. On information and belief, DRT knew or should have known of the '826 patent, and that its sale of Wireless Interception Products would have caused direct infringement of the '826 patent by purchasers of the Wireless Interception Products, especially given the fact that KeySee through its counsel sent letters as discussed above to DRT's CEO Mr. Turner informing

DRT about the ’826 patent as early as September 29, 2020, the day on which DRT received the letter. *See* Exhibit H (showing that DRT received the letter on September 29, 2020). Moreover, there can be no question that DRT has had actual knowledge of the ’826 patent and detailed knowledge of how use of the Wireless Interception Products would infringe claims of the ’826 patent since at least the date it was served with this complaint.

38. On information and belief and based on the preceding paragraphs, there was and is an objectively high likelihood that DRT’s activities have been and are infringing the ’826 patent; DRT has been and is infringing the ’826 patent with knowledge of the patents; and DRT subjectively knew the risk of infringement of the ’826 patent and/or the risk of infringement of the ’826 patent was so obvious that DRT should have known of the risk; and thus, DRT’s infringement of the ’826 patent has been and continues to be willful.

39. On information and belief, DRT will continue to infringe the ’826 patent unless and until it is enjoined by this Court.

40. DRT has caused and will continue to cause KeySee irreparable injury and damage by infringing the Asserted Patents. KeySee will suffer further irreparable injury, for which it has no adequate remedy at law, unless and until DRT is enjoined from infringing the ’826 patent.

COUNT TWO: INFRINGEMENT OF U.S. PATENT 8,295,477

41. All of the allegations set forth in the preceding paragraphs are incorporated herein by reference.

42. KeySee Cryptanalysis Patents including the ’477 patent, as discussed above, are generally directed to a novel and inventive technical solution to a problem relating to computer and networking technology, and in particular to the problems of network security and cryptanalysis, which includes lawful interception and decryption of encrypted communications,

in wireless communication systems. The ’477 patent claims a particular technique of recovering an encryption key used to encrypt wireless communications between a cellular network and a mobile device such that another party can, for example, decrypt the communications. Further, the claims of the ’477 patent cover methods for performing an effective ciphertext-only cryptanalysis of encrypted communications received off the air to recover the encryption key. For example, claim 6 of the ’477 patent, which is a method for cryptanalyzing an encrypted digital communication, claims recovering a cryptographic key used to encrypt the encrypted digital communication by a ciphertext only cryptanalysis of the communication through the use of processing circuitry, wherein said cryptanalysis comprises deriving equations for bits of key-stream used to encrypt at least a portion of the encrypted digital communication, wherein said deriving includes XORing together bits of the encrypted digital communication based on an error correction coding scheme or XORing bits of said encrypted digital communication with bits which are an output of an error correction coding scheme, or both. In sum, the ’477 patent provides significant improvements in computer-related technology and solves computer and network-related problems with technical solutions. Furthermore, the inventions claimed in the ’477 patent provided the first known solutions to the problem of ciphertext-only cryptanalysis of GSM encrypted communications. The inventions claimed in ’477 patent thus provide a solution to a problem for which there was no conventional solution in the prior art.

43. On information and belief, DRT uses KeySee’s patented features of the ’477 patent in its Wireless Interception Products in violation of KeySee’s patent rights. DRT’s Wireless Interception Products include radio technology, such as SDRs, that transmit, receive, and process wireless signals. *See*, *e.g.*, Exhibit E (DRT webpage). Further, DRT’s Wireless Interception Products provide a multi-protocol survey capability that supports simultaneously

surveying a number of modern 2G, 3G, and 4G technologies including GSM, cdma2000, 1xEV-DO, UMTS WCDMA, TD-SCDMA, and LTE. Exhibit F (DRT presentation) at p. 10. On information and belief, DRT's Wireless Interception Products practice one or more claims of the '477 patent by performing, for example, a ciphertext-only cryptanalysis of encrypted GSM communications.

44. On information and belief, all encrypted GSM communications are first encoded according to an error correction coding scheme before encryption. On information and belief, the ciphertext-only cryptanalysis of encrypted GSM communications performed by DRT's Wireless Interception Products is performed by XORing together bits of the encrypted digital communication based on an error correction coding scheme or XORing bits of said encrypted digital communication with bits which are an output of an error correction coding scheme, or both.

45. In violation of 35 U.S.C. § 271, DRT has infringed, contributed to the infringement of, and/or induced others to infringe the '477 patent by, among other things, making, using, offering to sell, selling, and/or importing into the United States unlicensed systems, products, and/or services in a manner that infringes one or more of at least claims 1, 2, 3, 4, 6, 7, 9, and 10 of the '477 patent. Such unlicensed systems, products, and/or services include, by way of example and without limitation, DRT's Wireless Interception Products. In addition, on information and belief, customers of DRT directly infringe the '826 patent by putting the Wireless Interception Products into service by, for example, using the Wireless Interception Products to recover encryption keys which are used to encrypt wireless communications.

46. DRT has directly infringed the ’477 patent by making, using, offering to sell, selling, and/or importing the Wireless Interception Products in violation of 35 U.S.C. § 271(a). On information and belief, such manufacture, sale, and use directly infringes at least claims 1, 2, 3, 4, 6, 7, 9, and 10 of the ’477 patent.

47. On information and belief, DRT takes steps to actively induce infringement by others of one or more of at least claims 1, 2, 3, 4, 6, 7, 9, and 10 of the ’477 patent in violation of 35 U.S.C. § 271(b), including customers that purchase the Wireless Interception Products. Such active steps include, but are not limited to encouraging, advertising (including by websites such as https://www.drti.com/), promoting, and training others to use and/or how to use the Wireless Interception Products. *See* Exhibit E (DRT webpage).

48. On information and belief, DRT knew or should have known that such activities induce others to directly infringe one or more of at least claims 1, 2, 3, 4, 6, 7, 9, and 10 of the ’477 patent. For example, DRT knows or should have known that its actions induce others to directly infringe the ’477 patent because DRT knows or should have known about the existence of the ’477 patent, especially given the fact that KeySee through its counsel sent letters as discussed above to DRT’s CEO Mr. Turner informing DRT about the ’477 patent as early as September 29, 2020, the day on which DRT received the letter. *See* Exhibit H (showing that DRT received the letter on September 29, 2020). Moreover, there can be no question that DRT has had actual knowledge of the ’477 patent and detailed knowledge of its own infringement since the day when it was served with this complaint.

49. On information and belief, DRT contributes to the infringement of at least claims 1, 2, 3, 4, 6, 7, 9, and 10 of the ’477 patent by others, including its customers, distributors, and/or authorized resellers in violation of 35 U.S.C. § 271(c). Acts by DRT that contribute to the

infringement of others include, but are not limited to, the sale and offer for sale by DRT of the Wireless Interception Products. DRT's Wireless Interception Products are especially made for or adapted for use to infringe the '477 patent and are not a staple article of commerce and are not suitable for substantial non-infringing use. By way of example, the interception and decryption properties of the DRT's Wireless Interception Products are all evidence that these products are especially made or adapted to infringe the '477 patent.

50. On information and belief, DRT knew or should have known of the '477 patent, and that its sale of Wireless Interception Products would have caused direct infringement of the '477 patent by purchasers of the Wireless Interception Products, especially given the fact that KeySee through its counsel sent letters as discussed above to DRT's CEO Mr. Turner informing DRT about the '477 patent as early as September 29, 2020, the day on which DRT received the letter. *See* Exhibit H (showing that DRT received the letter on September 29, 2020). Moreover, there can be no question that DRT has had actual knowledge of the '477 patent and detailed knowledge of how use of the Wireless Interception Products would infringe claims of the '477 patent since at least the date it was served with this complaint.

51. On information and belief and based on the preceding paragraphs, there was and is an objectively high likelihood that DRT's activities have been and are infringing the '477 patent; DRT has been and is infringing the '477 patent with knowledge of the patents; and DRT subjectively knew the risk of infringement of the '477 patent and/or the risk of infringement of the '477 patent was so obvious that DRT should have known of the risk; and thus, DRT's infringement of the '477 patent has been and continues to be willful.

52. On information and belief, DRT will continue to infringe the '477 patent unless and until it is enjoined by this Court.

53. DRT has caused and will continue to cause KeySee irreparable injury and damage by infringing the Asserted Patents. KeySee will suffer further irreparable injury, for which it has no adequate remedy at law, unless and until DRT is enjoined from infringing the ’477 patent.

COUNT THREE: INFRINGEMENT OF U.S. PATENT 9,038,192

54. All of the allegations set forth in the preceding paragraphs are incorporated herein by reference.

55. KeySee Cryptanalysis Patents including the ’192 patent, as discussed above, are generally directed to a novel and inventive technical solution to a problem relating to computer and networking technology, and in particular to the problems of network security and cryptanalysis, which includes lawful interception and decryption of encrypted communications, in wireless communication systems. The ’192 patent claims a particular technique of recovering an encryption key used to encrypt wireless communications between a cellular network and a mobile device such that another party can, for example, decrypt the communications. Further, the claims of the ’192 patent cover systems, devices, and methods for utilizing an effective ciphertext cryptanalysis of encrypted communications received off the air to recover the encryption key, and use it to mount an active attack on a GSM network. For example, claim 1 of the ’192 patent, which is a method for cryptanalyzing encrypted GSM communications, in order to decrypt or encrypt GSM communications associated with a first wireless client device, claims recovering an encryption key used to encrypt the first communication by performing a ciphertext-only, distinct from a known plaintext, cryptanalysis of the first GSM encrypted communication, wherein error correction coding was applied to said communication prior to encryption. In sum, the ’192 patent provides significant improvements in computer-related technology and solves computer and network-related problems with technical solutions.

Furthermore, the inventions claimed in the '192 patent provided the first known solutions to the problem of active attacks on GSM encrypted communications while cryptanalyzing the communications. The inventions claimed in '192 patent thus provide a solution to a problem for which there was no conventional solution in the prior art.

56. On information and belief, DRT uses KeySee's patented features of the '192 patent in its Wireless Interception Products in violation of KeySee's patent rights. DRT's Wireless Interception Products include radio technology, such as SDRs, that transmit, receive, and process wireless signals. *See*, *e.g.*, Exhibit E (DRT webpage). Further, DRT's Wireless Interception Products provide a multi-protocol survey capability that supports simultaneously surveying a number of modern 2G, 3G, and 4G technologies including GSM, cdma2000, 1xEV-DO, UMTS WCDMA, TD-SCDMA, and LTE. Exhibit F (DRT presentation) at p. 10. On information and belief, DRT's Wireless Interception Products practice one or more claims of the '192 patent by performing, for example, a ciphertext-only cryptanalysis of encrypted GSM communications.

57. On information and belief, all encrypted GSM communications are first encoded according to an error correction coding scheme before encryption. On information and belief, encrypted GSM communications transmitted on an uplink (i.e., from a handset toward a base station) are encrypted using a different encryption scheme than is used to encrypt GSM communications transmitted on a downlink (i.e., from a base station toward a handset). Notwithstanding this difference, in a given GSM communication session, the handset and the base station will use the same session key for both the uplink encryption scheme and the downlink encryption scheme. Furthermore, GSM permits weaker and stronger versions of its encryption schemes to be used on both the uplink and the downlink, and both versions of the

uplink and downlink encryption schemes may utilize the same session keys. GSM permits a base station to instruct a handset to transmit using the weaker version of the uplink encryption scheme and to receive data encrypted using the weaker version of the downlink encryption scheme.

58. On information and belief, DRT's Wireless Interception Products perform so-called "man-in-the-middle" attacks on GSM encrypted communications between a handset and a GSM base station. These attacks entail DRT's Wireless Interception Products intercepting communications from a handset to a base station by simulating the base station to the handset, and intercepting communications from a base station to a handset by simulating the handset to the base station. On information and belief, the Wireless Interception Products intercept encrypted uplink communications from a handset intended for a base station that are encrypted using a first (uplink) encryption scheme, recover the session key used to encrypt the uplink communications using a ciphertext-only cryptanalysis, and then use the recovered session key to decrypt intercepted communications transmitted from the base station intended for the handset and that are encrypted by the base station using a second (downlink) encryption scheme and the recovered session key.

59. Furthermore, on information and belief, DRT's Wireless Interception Products perform man-in-the-middle attacks on communication between a handset and a base station by causing the handset to transmit encrypted uplink communications using a weaker version of the GSM uplink encryption scheme than may be required by the base station, intercepting such encrypted uplink communications from the handset, recovering the session key used to encrypt the uplink communications using a ciphertext-only cryptanalysis, decrypting the intercepted uplink communications using the recovered session key to recover plaintext, re-encrypting the

plaintext using the recovered encryption key using a stronger uplink encryption scheme that may be required by the base station, and transmitting the re-encrypted data to the base station.

60. In violation of 35 U.S.C. § 271, DRT has infringed, contributed to the infringement of, and/or induced others to infringe the '192 patent by, among other things, making, using, offering to sell, selling, and/or importing into the United States unlicensed systems, products, and/or services in a manner that infringes one or more of at least claims 1, 3, 6, 8, 11, 13, 15, 18, 21, 22, 23, 24, 26, and 29 of the '192 patent. Such unlicensed systems, products, and/or services include, by way of example and without limitation, DRT's Wireless Interception Products. In addition, on information and belief, customers of DRT directly infringe the '192 patent by putting the Wireless Interception Products into service by, for example, using the Wireless Interception Products to recover encryption keys which are used to encrypt wireless communications.

61. DRT has directly infringed the '192 patent by making, using, offering to sell, selling, and/or importing the Wireless Interception Products in violation of 35 U.S.C. § 271(a). On information and belief, such manufacture, sale, and use directly infringes at least claims 1, 3, 6, 8, 11, 13, 15, 18, 21, 22, 23, 24, 26, and 29 of the '192 patent.

62. On information and belief, DRT takes steps to actively induce infringement by others of one or more of at least claims 1, 3, 6, 8, 11, 13, 15, 18, 21, 22, 23, 24, 26, and 29 of the '192 patent in violation of 35 U.S.C. § 271(b), including customers that purchase the Wireless Interception Products. Such active steps include, but are not limited to encouraging, advertising (including by websites such as https://www.drti.com/), promoting, and training others to use and/or how to use the Wireless Interception Products. *See* Exhibit E (DRT webpage).

63. On information and belief, DRT knew or should have known that such activities induce others to directly infringe one or more of at least claims 1, 3, 6, 8, 11, 13, 15, 18, 21, 22, 23, 24, 26, and 29 of the '192 patent. For example, DRT knows or should have known that its actions induce others to directly infringe the '192 patent because DRT knows or should have known about the existence of the '192 patent, especially given the fact that KeySee through its counsel sent letters as discussed above to DRT's CEO Mr. Turner informing DRT about the '192 patent as early as September 29, 2020, the day on which DRT received the letter. *See* Exhibit H (showing that DRT received the letter on September 29, 2020). Moreover, there can be no question that DRT has had actual knowledge of the '192 patent and detailed knowledge of its own infringement since the day when it was served with this complaint.

64. On information and belief, DRT contributes to the infringement of at least claims 1, 3, 6, 8, 11, 13, 15, 18, 21, 22, 23, 24, 26, and 29 of the '192 patent by others, including its customers, distributors, and/or authorized resellers in violation of 35 U.S.C. § 271(c). Acts by DRT that contribute to the infringement of others include, but are not limited to, the sale and offer for sale by DRT of the Wireless Interception Products. DRT's Wireless Interception Products are especially made for or adapted for use to infringe the '192 patent and are not a staple article of commerce and are not suitable for substantial non-infringing use. By way of example, the interception and decryption properties of the DRT's Wireless Interception Products are all evidence that these products are especially made or adapted to infringe the '192 patent.

65. On information and belief, DRT knew or should have known of the '192 patent, and that its sale of Wireless Interception Products would have caused direct infringement of the '192 patent by purchasers of the Wireless Interception Products, especially given the fact that KeySee through its counsel sent letters as discussed above to DRT's CEO Mr. Turner informing

DRT about the '192 patent as early as September 29, 2020, the day on which DRT received the letter. *See* Exhibit H (showing that DRT received the letter on September 29, 2020). Moreover, there can be no question that DRT has had actual knowledge of the '192 patent and detailed knowledge of how use of the Wireless Interception Products would infringe claims of the '192 patent since at least the date it was served with this complaint.

66. On information and belief and based on the preceding paragraphs, there was and is an objectively high likelihood that DRT's activities have been and are infringing the '192 patent; DRT has been and is infringing the '192 patent with knowledge of the patents; and DRT subjectively knew the risk of infringement of the '192 patent and/or the risk of infringement of the '192 patent was so obvious that DRT should have known of the risk; and thus, DRT's infringement of the '192 patent has been and continues to be willful.

67. On information and belief, DRT will continue to infringe the '192 patent unless and until it is enjoined by this Court.

68. DRT has caused and will continue to cause KeySee irreparable injury and damage by infringing the Asserted Patents. KeySee will suffer further irreparable injury, for which it has no adequate remedy at law, unless and until DRT is enjoined from infringing the '192 patent.

COUNT FOUR: INFRINGEMENT OF U.S. PATENT 10,447,666

69. All of the allegations set forth in the preceding paragraphs are incorporated herein by reference.

70. KeySee Cryptanalysis Patents including the '666 patent, as discussed above, are generally directed to a novel and inventive technical solution to a problem relating to computer and networking technology, and in particular to the problems of network security and cryptanalysis, which includes lawful interception and decryption of encrypted communications,

in wireless communication systems. The ’666 patent claims a particular technique of recovering an encryption key used to encrypt wireless communications between a cellular network and a mobile device such that another party can, for example, decrypt the communications. Further, the claims of the ’666 patent cover systems for performing an effective ciphertext cryptanalysis of encrypted communications received off the air to recover the encryption key. For example, claim 1 of the ’666 patent, which is system for decrypting an encrypted wireless digital communication transmitted to or by a wireless transceiver of a wireless client device, includes communication circuitry configured to receive the encrypted digital communication and processing circuitry configured to recover the encryption key from the encrypted wireless digital communication with a recovery process of the encryption key that comprises deriving equations based on redundancy introduced by the error correction coding and using an XORing function over data bits of the encrypted wireless digital communication. In sum, the ’666 patent provides significant improvements in computer-related technology and solves computer and network-related problems with technical solutions. Furthermore, the inventions claimed in the ’666 patent provided the first known solutions to the problem of ciphertext-only cryptanalysis of GSM encrypted communications. The inventions claimed in ’666 patent thus provide a solution to a problem for which there was no conventional solution in the prior art.

71. On information and belief, DRT uses KeySee’s patented features of the ’666 patent in its Wireless Interception Products in violation of KeySee’s patent rights. DRT’s Wireless Interception Products include radio technology, such as SDRs, that transmit, receive, and process wireless signals. *See*, *e.g.*, Exhibit E (DRT webpage). Further, DRT’s Wireless Interception Products provide a multi-protocol survey capability that supports simultaneously surveying a number of modern 2G, 3G, and 4G technologies including GSM, cdma2000, 1xEV-

DO, UMTS WCDMA, TD-SCDMA, and LTE. Exhibit F (DRT presentation) at p. 10. On information and belief, DRT's Wireless Interception Products practice one or more claims of the '666 patent by performing, for example, a ciphertext-only cryptanalysis of encrypted GSM communications.

72. On information and belief, all encrypted GSM communications are first encoded according to an error correction coding scheme before encryption. The error correction coding scheme employs XORing of bits of digital communication with a keystream generated from a session key to generate the encrypted digital communication, such that the coding can be modelled as multiplication by a matrix over GF(2). On information and belief, the ciphertext-only cryptanalysis of encrypted GSM communications performed by DRT's Wireless Interception Products recovers the session key by deriving equations based, *inter alia*, on redundancy introduced by the error correction coding and by using an XORing function over data bits of the encrypted wireless digital communication. Further, on information and belief, the ciphertext-only cryptanalysis of encrypted GSM communications performed by DRT's Wireless Interception Products recovers the session key by performing a decryption process on the encrypted digital communication using a candidate session key and using an XORing function over data bits of the encrypted wireless digital communication, mathematically searching for patterns within an output of the decryption process matching, *inter alia*, a structural redundancy typical of the error correction coding scheme, and repeating these steps with different candidate session keys.

73. In violation of 35 U.S.C. § 271, DRT has infringed, contributed to the infringement of, and/or induced others to infringe the '666 patent by, among other things, making, using, offering to sell, selling, and/or importing into the United States unlicensed

systems, products, and/or services in a manner that infringes one or more of at least claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, and 15 of the '666 patent. Such unlicensed systems, products, and/or services include, by way of example and without limitation, DRT's Wireless Interception Products. In addition, on information and belief, customers of DRT directly infringe the '666 patent by putting the Wireless Interception Products into service by, for example, using the Wireless Interception Products to recover encryption keys which are used to encrypt wireless communications.

74. DRT has directly infringed the '666 patent by making, using, offering to sell, selling, and/or importing the Wireless Interception Products in violation of 35 U.S.C. § 271(a). On information and belief, such manufacture, sale, and use directly infringes at least claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, and 15 of the '666 patent.

75. On information and belief, DRT takes steps to actively induce infringement by others of one or more of at least claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, and 15 of the '666 patent in violation of 35 U.S.C. § 271(b), including customers that purchase the Wireless Interception Products. Such active steps include, but are not limited to encouraging, advertising (including by websites such as https://www.drti.com/), promoting, and training others to use and/or how to use the Wireless Interception Products. *See* Exhibit E (DRT webpage).

76. On information and belief, DRT knew or should have known that such activities induce others to directly infringe one or more of at least claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, and 15 of the '666 patent. For example, DRT knows or should have known that its actions induce others to directly infringe the '666 patent because DRT knows or should have known about the existence of the '666 patent, especially given the fact that KeySee through its counsel sent letters as discussed above to DRT's CEO Mr. Turner informing DRT about the

family of patents that includes the ’666 patent as early as September 29, 2020, the day on which DRT received the letter. *See* Exhibit H (showing that DRT received the letter on September 29, 2020). Moreover, there can be no question that DRT has had actual knowledge of the ’666 patent and detailed knowledge of its own infringement since the day when it was served with this complaint.

77. On information and belief, DRT contributes to the infringement of at least claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, and 15 of the ’666 patent by others, including its customers, distributors, and/or authorized resellers in violation of 35 U.S.C. § 271(c). Acts by DRT that contribute to the infringement of others include, but are not limited to, the sale and offer for sale by DRT of the Wireless Interception Products. DRT’s Wireless Interception Products are especially made for or adapted for use to infringe the ’666 patent and are not a staple article of commerce and are not suitable for substantial non-infringing use. By way of example, the interception and decryption properties of the DRT’s Wireless Interception Products are all evidence that these products are especially made or adapted to infringe the ’666 patent.

78. On information and belief, DRT knew or should have known of the ’666 patent, and that its sale of Wireless Interception Products would have caused direct infringement of the ’666 patent by purchasers of the Wireless Interception Products, especially given the fact that KeySee through its counsel sent letters as discussed above to DRT’s CEO Mr. Turner informing DRT about the family of patents that includes the ’666 patent as early as September 29, 2020, the day on which DRT received the letter. *See* Exhibit H (showing that DRT received the letter on September 29, 2020). Moreover, there can be no question that DRT has had actual knowledge of the ’666 patent and detailed knowledge of how use of the Wireless Interception Products would infringe claims of the ’666 patent since at least the date it was served with this complaint.

79. On information and belief and based on the preceding paragraphs, there was and is an objectively high likelihood that DRT's activities have been and are infringing the '666 patent; DRT has been and is infringing the '666 patent with knowledge of the patents; and DRT subjectively knew the risk of infringement of the '666 patent and/or the risk of infringement of the '666 patent was so obvious that DRT should have known of the risk; and thus, DRT's infringement of the '666 patent has been and continues to be willful.

80. On information and belief, DRT will continue to infringe the '666 patent unless and until it is enjoined by this Court.

81. DRT has caused and will continue to cause KeySee irreparable injury and damage by infringing the Asserted Patents. KeySee will suffer further irreparable injury, for which it has no adequate remedy at law, unless and until DRT is enjoined from infringing the '666 patent.

DEMAND FOR JURY TRIAL

82. KeySee hereby request a trial by jury on issues so triable by right.

PRAYER FOR RELIEF

83. Wherefore, KeySee respectfully requests that this Court:

A. Enter Judgment that DRT has infringed one or more claims of the Asserted Patents;

B. Enter an order permanently enjoining DRT and its officers, agents, employees, attorneys, and all persons in active concert or participation with any of them, from infringing the Asserted Patents;

C. Award KeySee damages in an amount sufficient to compensate it for DRT's infringement of the Asserted Patents, together with prejudgment and post-judgment interest and costs under 35 U.S.C. § 284;

D. Award KeySee an accounting for acts of infringement not presented at trial and an award by the Court of additional damage for any such acts of infringement;

E. Treble the damages awarded to KeySee under 35 U.S.C § 284 by reason of DRT's willful infringement;

F. Declare this case to be "exceptional" under 35 U.S.C. § 285 and award KeySee its attorney fees, expenses, and costs incurred in this action; and

G. Award KeySee such other and further relief as this Court deems just and proper.

Dated: March 2, 2021

Respectfully submitted,

/s/ Ahmed J. Davis

Ahmed J. Davis
FISH & RICHARDSON P.C.
1000 Maine Ave. SW
Suite 1000
Washington, DC 20024
Telephone: (202) 783-5070
davis@fr.com

Carl E. Bruce (*pro hac vice* to be filed)
Thomas Reger (*pro hac vice* to be filed)
Aaron Pirouznia (*pro hac vice* to be filed)
FISH & RICHARDSON P.C.
1717 Main Street, Suite 5000
Dallas, TX 75201
Telephone: (214) 747-5070
Bruce@fr.com
Reger@fr.com
pirouznia@fr.com

Lawrence Kolodney (*pro hac vice* to be filed)
Ethan Rubin (*pro hac vice* to be filed)
FISH & RICHARDSON P.C.
One Marina Park Drive
Boston, MA 02210
Telephone: (617) 542-5070
kolodney @fr.com
erubin@fr.com

John-Paul Fryckman (*pro hac vice* to be filed)
FISH & RICHARDSON P.C.
12860 El Camino Real, Suite 400
San Diego, CA 92130
Telephone: (858) 678-5070
Fryckman@fr.com

Attorneys for Plaintiff KeySee Software Ltd.