

1 Steven Ritcheson (SBN 174062)  
2 Insight, PLC  
3 578 Washington Boulevard #503  
4 Marina del Rey, California 90291  
5 Phone: (424) 289-9191  
6 switcheson@insightplc.com

7 Howard L. Wernow  
8 (*pro hac vice forthcoming*)  
9 Sand, Sebolt & Wernow Co., LPa  
10 Aegis Tower - Suite 1100  
11 4940 Munson Street, N. W.  
12 Canton, Ohio 44718  
13 Phone: (330) 244-1174  
14 howard.wernow@sswip.com

15 Attorneys for Plaintiff  
16 KWALITY IP LLC

17 **IN THE UNITED STATES DISTRICT COURT**  
18 **FOR THE CENTRAL DISTRICT OF CALIFORNIA**

19 **KWALITY IP LLC,**

20 Plaintiff,

21 v.

22 **ALLIED WALLET, INC.,**

23 Defendant.

Civil Action No.:

**TRIAL BY JURY DEMANDED**

24 **COMPLAINT FOR INFRINGEMENT OF PATENT**

25 Now comes, Plaintiff, Kwalitiy IP LLC (“Plaintiff” or “Kwalitiy”), by and  
26 through undersigned counsel, and respectfully alleges, states, and prays as follows:  
27  
28

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
**NATURE OF THE ACTION**

1. This is an action for patent infringement under the Patent Laws of the United States, Title 35 United States Code (“U.S.C.”) to prevent and enjoin Defendant Allied Wallet, Inc. (hereinafter “Defendant”), from infringing and profiting, in an illegal and unauthorized manner, and without authorization and/or consent from Plaintiff from U.S. Patent No 8,719,165 (“the ‘165 Patent” or the “Patent-in-Suit”), which is attached hereto as Exhibit A and incorporated herein by reference, and pursuant to 35 U.S.C. §271, and to recover damages, attorney’s fees, and costs.

13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
**THE PARTIES**

2. Plaintiff is a Texas limited liability company with its principal place of business at 15922 Eldorado Pkwy – Suite 500-1680, Frisco, TX 75035.

3. Upon information and belief, Defendant is a corporation organized under the laws of Nevada, having a principal place of business at 9000 West Sunset Boulevard – Suite 820, West Hollywood, California 90069. Upon information and belief, Defendant may be served with process c/o Farhad Novian, its Registered Agent, 1801 Century Park East – Suite 1201, Los Angeles, California 90067.

24  
25  
26  
27  
28  
**JURISDICTION AND VENUE**

4. This is an action for patent infringement in violation of the Patent Act of the United States, 35 U.S.C. §§1 *et seq.*

1 5. The Court has subject matter jurisdiction over this action pursuant to 28  
2 U.S.C. §§1331 and 1338(a).

3 6. This Court has personal jurisdiction over Defendant by virtue of its  
4 systematic and continuous contacts with this jurisdiction and its residence in this  
5 District, as well as because of the injury to Plaintiff, and the cause of action Plaintiff  
6 has risen in this District, as alleged herein.  
7

8 7. Defendant is subject to this Court's specific and general personal  
9 jurisdiction pursuant to its substantial business in this forum, including: (i) at least a  
10 portion of the infringements alleged herein; (ii) regularly doing or soliciting  
11 business, engaging in other persistent courses of conduct, and/or deriving substantial  
12 revenue from goods and services provided to individuals in this forum state and in  
13 this judicial District; and (iii) having a physical presence in this District.  
14  
15

16 8. Venue is proper in this judicial district pursuant to 28 U.S.C. §1400(b)  
17 because Defendant resides in this District under the Supreme Court's opinion in *TC*  
18 *Heartland v. Kraft Foods Group Brands LLC*, 137 S. Ct. 1514 (2017) through its -  
19 incorporation, and regular and established place of business in this District.  
20  
21

22 **FACTUAL ALLEGATIONS**

23 9. On May 6, 2014, the United States Patent and Trademark Office  
24 ("USPTO") duly and legally issued the '165 Patent, entitled "DELEGATED  
25 TRANSACTIONS OVER MOBILE" after a full and fair examination. The '165  
26 Patent is attached hereto as Exhibit A and incorporated herein as if fully rewritten.  
27  
28

1           10. Plaintiff is presently the owner of the ‘165 Patent, having received all  
2 right, title and interest in and to the ‘165 Patent from the previous assignee of  
3 record. Plaintiff possesses all rights of recovery under the ‘165 Patent, including the  
4 exclusive right to recover for past infringement.  
5

6           11. To the extent required, Plaintiff has complied with all marking  
7 requirements under 35 U.S.C. § 287.  
8

9           12. As identified in the ‘165 Patent, prior art systems were familiar with  
10 online purchases. See Ex. A at Col 1:6-9.

11           13. More particularly, the ‘165 Patent identifies that the prior art provided a  
12 scenario where a customer operates a full-featured and secure computing device to  
13 access a website operated by a merchant. Ex. A at Col. 1:10-11. The customer enters  
14 transaction data in a web-based form, and uses a website user interface to finalize  
15 the transaction. Ex. A at Col. 1:11-13. The merchant receives the transaction data,  
16 verifies payment, confirms that payment was received, confirms that the goods will  
17 be delivered accordingly, and subsequently delivers the goods. Ex. A at Col. 1:13-  
18  
19  
20

21 16.

22           14. Further, prior to the ‘165 Patent, electronic transactions using mobile  
23 devices were much less common than those using a fully featured laptop or desktop  
24 computer. Ex. A at Col. 2:10-14.  
25

26           15. To address the limitations, the computer-centric or network-centric that  
27 resulted in a computing gap between smartphones and computers, the present  
28

1 provided a system and method that generally relates to enabling completion of  
2 secure transactions using mobile devices that may or may not have appropriate  
3 security features needed or desired for the transaction. Ex. A at Col. 2:31-35. In  
4 some embodiments, a transaction may be partially completed by a secure computing  
5 device, and partially completed by a mobile device. Ex. A at Col. 2:35-37. The  
6 secure computing device can be arranged to delegate one or more transaction  
7 operation(s) to the mobile device. Ex. A at Col. 2:37-40. For example, a customer  
8 may initiate a transaction from a customer secure computing device, such as, for  
9 example, a secure personal computer (PC) in the customer's home or office. Ex. A at  
10 Col. 2:40-44. Instead of completing the transaction, however, the customer may  
11 delegate a transaction operation to a delegate mobile device. Ex. A at Col. 2:44-45.  
12 Upon receiving an appropriate communication from the delegate mobile device, the  
13 customer secure computing device may then complete the transaction. Ex. A at Col.  
14 2:45-47. Similarly, a merchant may delegate transaction operation(s) to delegate  
15 mobile device(s). Ex. A at Col. 2:47-49.

16  
17  
18  
19  
20  
21 16. To address this specific technical problem, Claim 1 in the '165 Patent  
22 comprises a non-abstract method for delegated transaction over mobile.

23  
24 17. Particularly, Claim 1 of the '165 Patent provides:

25 "1. A method for completing, by a customer secure computing  
26 device, a secure transaction between a customer and a merchant,  
27 wherein the customer is associated with the customer secure computing  
28 device and a delegate mobile device, the method comprising:

1           acquiring customer delegate mobile device identification  
2 information and secure transaction data, by the customer secure  
3 computing device, comprising:

4           receiving, by the customer secure computing device,  
5 secure transaction data associated with a delegated transaction, the  
6 secure transaction data comprising a merchant identification associated  
7 with the merchant;

8           receiving, by the customer secure computing device,  
9 customer delegate mobile device identification information associated  
10 with a customer delegate mobile device authorized by the customer for  
11 the delegated transaction with the merchant; and

12           storing, by the customer secure computing device, the  
13 secure transaction data and customer delegate mobile device  
14 identification information; and

15           subsequent to acquiring customer delegate mobile device  
16 identification information and secure transaction data by the customer  
17 secure computing device, automatically completing the secure  
18 transaction, by the customer secure computing device, in response to  
19 receiving a communication from the identified previously authorized  
20 customer delegate mobile device, comprising:

21           receiving, by the customer secure computing device, a  
22 communication from the identified previously authorized customer  
23 delegate mobile device;

24           checking, by the customer secure computing device, a  
25 status identifier in the communication from the identified previously  
26 authorized customer delegate mobile device; and

27           automatically initiating, by the customer secure computing  
28 device, using the secure transaction data, payment to the merchant by  
the customer secure computing device in response to receiving the  
communication from the identified previously authorized customer  
delegate mobile device, when the status identifier indicates that the  
delegated transaction is complete.” See Exhibit A.

1           18. Claim 1 of the '165 Patent addressed the specific need for an improved  
2 delegated transaction over mobile or through mobile networks.

3           19. Specifically, to deal delegated mobile device, the method of Claim 1 in  
4 the '165 patent requires (a) receiving, by the customer secure computing device,  
5 *secure transaction data associated with a delegated transaction*, the secure  
6 transaction data comprising *a merchant identification associated with the merchant*;  
7 (b) receiving, by the customer secure computing device, customer delegate mobile  
8 device identification information associated with a customer delegate mobile device  
9 *authorized by the customer for the delegated transaction with the merchant*; (c)  
10 *subsequent* to acquiring customer delegate mobile device identification information  
11 and secure transaction data by the customer secure computing device, *automatically*  
12 *completing the secure transaction*, by the customer secure computing device, *in*  
13 *response to receiving a communication from the identified previously authorized*  
14 *customer delegate mobile device*; and (d) receiving, and checking, by the customer  
15 secure computing device, a status identifier in the communication from the  
16 identified previously authorized customer delegate mobile device; and *automatically*  
17 *initiating*, by the customer secure computing device, *using the secure transaction*  
18 *data, payment to the merchant by the customer secure computing device in response*  
19 *to receiving the communication from the identified previously authorized customer*  
20 *delegate mobile device, when the status identifier indicates that the delegated*  
21 *transaction is complete*. These specific elements, as combined, accomplish the  
22  
23  
24  
25  
26  
27  
28

1 desired result improving the previous computer-centric or network-centric problems  
2 associated with delegated transactions over mobile device or through mobile  
3 networks.

4  
5 20. Further, these specific elements also accomplish these desired results to  
6 overcome the then existing problems in the relevant field of network communication  
7 systems. *Ancora Technologies, Inc. v. HTC America, Inc.*, 908 F.3d 1343, 1348  
8 (Fed. Cir. 2018) (holding that improving computer security can be a non-abstract  
9 computer-functionality improvement if done by a specific technique that departs  
10 from earlier approaches to solve a specific computer problem). See also *Data*  
11 *Engine Techs. LLC v. Google LLC*, 906 F.3d 999 (Fed. Cir. 2018); *Core Wireless*  
12 *Licensing v. LG Elecs., Inc.*, 880 F.3d 1356 (Fed. Cir. 2018); *Finjan, Inc. v. Blue*  
13 *Coat Sys., Inc.*, 879 F.3d 1299 (Fed. Cir. 2018); *Uniloc USA, Inc. v. LG Electronics*  
14 *USA, Inc.*, 957 F.3d 1303 (Fed. Cir. April 30, 2020).

15  
16  
17  
18 21. Claims need not articulate the advantages of the claimed combinations  
19 to be eligible. *Uniloc USA, Inc. v. LG Elecs. USA, Inc.*, 957 F.3d 1303, 1309 (Fed.  
20 Cir. 2020).

21  
22 22. These specific elements of Claim 1 of the '165 Patent were an  
23 unconventional arrangement of elements because the prior art methodologies would  
24 not use delegate transaction which made them less secure. By adding the specific  
25 elements of Claim 1 of the '165 Patent, an improved method was able to  
26  
27  
28



1 unconventionally complete a secure transaction. *Cellspin Soft, Inc. v. FitBit, Inc.*,  
2 927 F.3d 1306 (Fed. Cir. 2019).

3 23. Further, regarding the specific non-conventional and non-generic  
4 arrangements of known, conventional pieces to overcome an existing problem, the  
5 method of Claim 1 in the '165 Patent provides a method of completing a secure  
6 transaction that would not preempt all ways of completing a transaction between a  
7 merchant and customer because completing the transaction is based on *authorization*  
8 *by the customer for the delegated transaction with the merchant; automatically*  
9 *completing the secure transaction, by the customer secure computing device, in*  
10 *response to receiving a communication from the identified previously authorized*  
11 *customer delegate mobile device; and receiving, checking, by the customer secure*  
12 *computing device, a status identifier in the communication from the identified*  
13 *previously authorized customer delegate mobile device; and automatically*  
14 *initiating, by the customer secure computing device, using the secure transaction*  
15 *data, payment to the merchant by the customer secure computing device in response*  
16 *to receiving the communication from the identified previously authorized customer*  
17 *delegate mobile device, when the status identifier indicates that the delegated*  
18 *transaction is complete, any of which could be removed or performed differently to*  
19 *permit a method of gaining completing the secured transaction in a different way.*

20  
21  
22  
23  
24  
25  
26 *Bascom Global Internet Servs., Inc. v. AT&T Mobility LLC*, 827 F.3d 1341 (Fed.  
27  
28

1 Cir. 2016); See also *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245 (Fed.  
2 Cir. 2014).

3 24. Based on the allegations, it must be accepted as true at this stage, that  
4 Claim 1 of the ‘165 Patent recites a specific, plausibly inventive way of completing  
5 a secure transaction and using specific protocols rather than the general idea of  
6 transacting between merchant and customer. *Cellspin Soft, Inc. v. Fitbit, Inc.*, 927  
7 F.3d 1306, 1319 (Fed. Cir. 2019), *cert. denied sub nom. Garmin USA, Inc. v.*  
8 *Cellspin Soft, Inc.*, 140 S. Ct. 907, 205 L. Ed. 2d 459 (2020).

9  
10  
11 25. Alternatively, there is at least a question of fact that must survive the  
12 pleading stage as to whether These specific elements of Claim 1 of the ‘165 Patent  
13 were an unconventional arrangement of elements. *Aatrix Software, Inc. v. Green*  
14 *Shades Software, Inc.*, 882 F.3d 1121 (Fed. Cir. 2018) See also *Berkheimer v. HP*  
15 *Inc.*, 881 F.3d 1360 (Fed. Cir. 2018), *cert. denied*, 140 S. Ct. 911, 205 L. Ed. 2d 454  
16 (2020).

17  
18  
19 26. Defendant commercializes, inter alia, methods that perform all the steps  
20 recited in at least one claim of the ‘165 Patent. More particularly, Defendant  
21 commercializes, inter alia, methods that perform all the steps recited in Claim 1 of  
22 the ‘165 Patent. Specifically, Defendant makes, uses, sells, offers for sale, or  
23 imports a method that encompasses that which is covered by Claim 1 of the ‘165  
24 Patent.

25  
26  
27 **DEFENDANT’S PRODUCT(S)**

1           27. Defendant offers solutions, such as the “Allied Wallet WS & Allied  
2           Wallet credit card reader” system (the “Accused Product”), that enables a method of  
3           complete a secure transaction. A non-limiting and exemplary claim chart comparing  
4           the Accused Product of Claim 1 of the ‘165 Patent is attached hereto as Exhibit B  
5           and is incorporated herein as if fully rewritten.  
6

7           28. As recited in Claim 1, a system, at least in internal testing and usage,  
8           utilized by the Accused Product practices a method for completing, by a customer  
9           secure computing device (e.g., Allied Wallet credit card reader), a secure transaction  
10          (e.g., Data required to complete the delegated transaction such as Credit Card  
11          number, expiry date, CVV, details related to merchant device (Allied Wallet credit  
12          card reader) such as device address to identify the merchant, etc. received in the  
13          encoded form) between a customer and a merchant, wherein the customer is  
14          associated with the customer secure computing device (e.g., Allied Wallet credit  
15          card reader) and a delegate mobile device (e.g., Smartphone with Allied Wallet WS  
16          connected to the Allied Wallet credit card reader). See E. B.  
17

18          29. As recited in one step of Claim 1, the system, at least in internal testing  
19          and usage, utilized by the Accused Product practices acquiring customer delegate  
20          mobile device identification information (e.g., information of the smartphone used  
21          to connect the phone with the Allied Wallet credit card reader) and secure  
22          transaction data (e.g., Data required to complete the delegated transaction such as  
23          Credit Card number, expiry date, CVV, details related to merchant device (Allied  
24          25          26          27          28

1 Wallet credit card reader) such as device address to identify the merchant, etc.  
2 received in the encoded form), by the customer secure computing device (e.g.,  
3 Allied Wallet credit card reader). See Ex. B.  
4

5 30. As recited in another step of Claim 1, the system, at least in internal  
6 testing and usage, utilized by the Accused Product practices receiving, by the  
7 customer secure computing device (e.g., Allied Wallet credit card reader), secure  
8 transaction data (e.g., Data required to complete the delegated transaction such as  
9 Credit Card number, expiry date, CVV, details related to merchant device (Allied  
10 Wallet credit card reader) such as device address to identify the merchant, etc.  
11 received in the encoded form) associated with a delegated transaction (e.g., current  
12 transaction or transaction in discussion), the secure transaction data (e.g., Data  
13 required to complete the delegated transaction such as Credit Card number, expiry  
14 date, CVV, details related to merchant device (Allied Wallet credit card reader) such  
15 as device address to identify the merchant, etc. received in the encoded form)  
16 comprising a merchant identification associated with the merchant (e.g., details  
17 related to merchant device (Allied Wallet credit card reader) such as device address  
18 to identify the merchant). See Ex. B.  
19  
20  
21  
22

23 31. As recited in one step of Claim 1, the system, at least in internal testing  
24 and usage, utilized by the Accused Product practices receiving, by the customer  
25 secure computing device (e.g., Allied Wallet credit card reader), customer delegate  
26 mobile device identification information (e.g., information of the smartphone)  
27  
28

1 associated with a customer delegate mobile device (e.g., Smartphone connected to  
2 the Allied Wallet credit card reader) authorized (e.g., by connecting it with Allied  
3 Wallet credit card reader) by the customer for the delegated transaction (e.g., current  
4 transaction or transaction in discussion) with the merchant. See Ex. B.  
5

6 32. As recited in another step of Claim 1, the system, at least in internal  
7 testing and usage, utilized by the Accused Product practices storing, by the customer  
8 secure computing device (e.g., Allied Wallet credit card reader), the secure  
9 transaction data (e.g., Data required to complete the delegated transaction such as  
10 Credit Card number, expiry date, CVV, details related to merchant device (Allied  
11 Wallet credit card reader) such as device address to identify the merchant, etc.  
12 received in the encoded form) and customer delegate mobile device identification  
13 information (e.g., information of the smartphone). See Ex. B. The Allied Wallet  
14 credit card reader stores the credit card number, information of the smartphone in its  
15 memory to complete the delegated transaction. See Ex. B.  
16  
17  
18

19 33. As recited in one step of Claim 1, the system, at least in internal testing  
20 and usage, utilized by the Accused Product practices subsequent to acquiring  
21 customer delegate mobile device identification information (e.g., information of the  
22 smartphone) and secure transaction data (e.g., Data required to complete the  
23 delegated transaction such as Credit Card number, expiry date, CVV, details related  
24 to merchant device (Allied Wallet credit card reader) such as device address to  
25 identify the merchant, etc. received in the encoded form) by the customer secure  
26  
27  
28

1 computing device (e.g., Allied Wallet credit card reader), automatically completing  
2 the secure transaction, by the customer secure computing device (e.g., Allied Wallet  
3 credit card reader), in response to receiving a communication (e.g., authentication  
4 for the delegated transaction via customer's signature) from the identified previously  
5 authorized customer delegate mobile device (e.g., smartphone). See Exhibit B. After  
6 the Allied Wallet credit card reader receives the authentication for the delegate  
7 transaction via customer's signature from the smartphone, it automatically starts  
8 initiating payment to the merchant. See Ex. B.

11 34. As recited in another step of Claim 1, the system, at least in internal  
12 testing and usage, utilized by the Accused Product practices receiving, by the  
13 customer secure computing device (e.g., Allied Wallet credit card reader), a  
14 communication (e.g., authentication for the delegated transaction via customer's  
15 signature) from the identified previously authorized customer delegate mobile  
16 device (e.g., smartphone). See Ex. B.

19 35. As recited in one step of Claim 1, the system, at least in internal testing  
20 and usage, utilized by the Accused Product practices checking, by the customer  
21 secure computing device, a status identifier in the communication (e.g.,  
22 authentication for the delegated transaction via customer's signature) from the  
23 identified previously authorized customer delegate mobile device (e.g., smartphone).  
24 See Ex. B.

26  
27  
28

1           36. As recited in another step of Claim 1, the system, at least in internal  
2 testing and usage, utilized by the Accused Product practices automatically initiating,  
3 by the customer secure computing device (e.g., Allied Wallet credit card reader),  
4 using the secure transaction data (e.g., Data required to complete the delegated  
5 transaction such as Credit Card number, expiry date, CVV, details related to  
6 merchant device (Allied Wallet credit card reader) such as device address to identify  
7 the merchant, etc. received in the encoded form), payment to the merchant by the  
8 customer secure computing device in response to receiving the communication (e.g.,  
9 authentication for the delegated transaction via customer's signature) from the  
10 identified previously authorized customer delegate mobile device (e.g., smartphone),  
11 when the status identifier indicates that the delegated transaction (e.g., current  
12 transaction or transaction in discussion) is complete (e.g., when the authentication  
13 from the smartphone is completed, delegated transaction is automatically initiated to  
14 be transferred to the merchant account). See Ex. B. After the Allied Wallet credit  
15 card reader receives the authentication for the delegate transaction via customer's  
16 signature from the smartphone, it automatically starts initiating payment to the  
17 merchant. The payment only initiates to the merchant when the signature is correctly  
18 received. See Ex. B.

19  
20  
21  
22  
23  
24  
25           37. The elements described in the preceding paragraphs are covered by at  
26 least Claim 1 of the '165 Patent. Thus, Defendant's use of the Accused Product is  
27 enabled by the method described in the '165 Patent.  
28

**INFRINGEMENT OF THE PATENT-IN-SUIT**

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

38. Plaintiff realleges and incorporates by reference all of the allegations set forth in the preceding paragraphs

39. In violation of 35 U.S.C. § 271, Defendant is now, and has been directly infringing the ‘165 Patent.

40. Defendant has had knowledge of infringement of the ‘165 Patent at least as of the service of the present Complaint.

41. Defendant has directly infringed and continues to directly infringe at least one claim of the ‘165 Patent by using, at least through internal testing or otherwise, the Accused Product without authority in the United States, and will continue to do so unless enjoined by this Court. As a direct and proximate result of Defendant’s direct infringement of the ‘165 Patent, Plaintiff has been and continues to be damaged.

42. Defendant has contributed to and induced others to infringe the ‘165 Patent by encouraging infringement, knowing that the acts Defendant induced constituted patent infringement, and its encouraging acts actually resulted in direct patent infringement.

43. By engaging in the conduct described herein, Defendant has injured Plaintiff and is thus liable for infringement of the ‘165 Patent, pursuant to 35 U.S.C. § 271.



1 44. Defendant has committed these acts of infringement without license or  
2 authorization.

3 45. As a result of Defendant’s infringement of the ‘165 Patent, Plaintiff has  
4 suffered monetary damages and is entitled to a monetary judgment in an amount  
5 adequate to compensate for Defendant’s past infringement, together with interests  
6 and costs.  
7

8 46. Plaintiff will continue to suffer damages in the future unless  
9 Defendant’s infringing activities are enjoined by this Court. As such, Plaintiff is  
10 entitled to compensation for any continuing and/or future infringement up until the  
11 date that Defendant is finally and permanently enjoined from further infringement.  
12

13 47. Plaintiff reserves the right to modify its infringement theories as  
14 discovery progresses in this case; it shall not be estopped for infringement  
15 contention or claim construction purposes by the claim charts that it provides with  
16 this Complaint. The claim chart depicted in Exhibit B is intended to satisfy the  
17 notice requirements of Rule 8(a)(2) of the Federal Rule of Civil Procedure and does  
18 not represent Plaintiff’s preliminary or final infringement contentions or preliminary  
19 or final claim construction positions.  
20  
21  
22

23 **DEMAND FOR JURY TRIAL**

24 48. Plaintiff demands a trial by jury of any and all causes of action.  
25

26 **PRAYER FOR RELIEF**

27 WHEREFORE, Plaintiff prays for the following relief:  
28

1 a. That Defendant be adjudged to have directly infringed the '165 Patent  
2 either literally or under the doctrine of equivalents;

3 b. An accounting of all infringing sales and damages including, but not  
4 limited to, those sales and damages not presented at trial;

5  
6 c. That Defendant, its officers, directors, agents, servants, employees,  
7 attorneys, affiliates, divisions, branches, parents, and those persons in active concert  
8 or participation with any of them, be permanently restrained and enjoined from  
9 directly infringing the '165 Patent;

10  
11 d. An award of damages pursuant to 35 U.S.C. §284 sufficient to compensate  
12 Plaintiff for the Defendant's past infringement and any continuing or future  
13 infringement up until the date that Defendant is finally and permanently enjoined  
14 from further infringement, including compensatory damages;

15  
16 e. An assessment of pre-judgment and post-judgment interest and costs  
17 against Defendant, together with an award of such interest and costs, in accordance  
18 with 35 U.S.C. §284;

19  
20  
21 f. That Defendant be directed to pay enhanced damages, including Plaintiff's  
22 attorneys' fees incurred in connection with this lawsuit pursuant to 35 U.S.C. §285;  
23 and

24  
25 g. That Plaintiff be granted such other and further relief as this Court may  
26 deem just and proper.

27  
28

1 Dated: September 29, 2020

Respectfully submitted,

2

/s/

3

Steven Ritcheson

4

Insight, PLC

5

578 Washington Boulevard #503

6

Marina del Rey, California 90291

7

Phone: (424) 289-9191

8

switcheson@insightplc.com

9

Together with:

10

SAND, SEBOLT & WERNOW CO., LPA

11

Howard L. Wernow

12

*(pro hac vice forthcoming)*

13

Aegis Tower – Suite 1100

14

4940 Munson Street NW

15

Canton, Ohio 44718

16

Phone: 330-244-1174

17

Fax: 330-244-1173

18

Email: [Howard.Wernow@sswip.com](mailto:Howard.Wernow@sswip.com)

19

ATTORNEYS FOR PLAINTIFF

20

21

22

23

24

25

26

27

28