**IN THE UNITED STATES DISTRICT COURT**
**FOR THE NORTHERN DISTRICT OF ILLINOIS**
**EASTERN DIVISION**

| | |
|---|---|
| **BUNKER IP LLC,**<br><br>Plaintiff,<br><br>v.<br><br>**ZTE (USA) INC.,**<br><br>Defendant. | C.A. No. 1:21-cv-484<br><br>**JURY TRIAL DEMANDED**<br><br>**PATENT CASE** |

# ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Bunker IP LLC files this Original Complaint for Patent Infringement against ZTE (USA) Inc., and would respectfully show the Court as follows:

## I. THE PARTIES

1. Plaintiff Bunker IP LLC ("Bunker IP" or "Plaintiff") is a Texas limited liability company having an address at 7548 Preston Rd, Suite 141 PMB 1055, Frisco, TX 75034.

2. On information and belief, Defendant ZTE (USA) Inc. ("Defendant") is a corporation organized and existing under the laws of New Jersey, with a place of business at 8430 W. Bryn Mawr Ave., Suite 210, Chicago, IL 60631.

## II. JURISDICTION AND VENUE

3. This action arises under the patent laws of the United States, Title 35 of the United States Code. This Court has subject matter jurisdiction of such action under 28 U.S.C. §§ 1331 and 1338(a).

4. On information and belief, Defendant is subject to this Court's specific and general personal jurisdiction, pursuant to due process and the Illinois Long-Arm Statute, due at least to its business in this forum, including at least a portion of the infringements alleged herein.

Furthermore, Defendant is subject to this Court's specific and general personal jurisdiction because Defendant has a place of business in Illinois and this District.

5. On information and belief, Defendant has derived revenues from its infringing acts occurring within Illinois. Further, on information and belief, Defendant is subject to the Court's general jurisdiction, including from regularly doing or soliciting business, engaging in other persistent courses of conduct, and deriving substantial revenue from goods and services provided to persons or entities in Illinois. Further, on information and belief, Defendant is subject to the Court's personal jurisdiction at least due to its sale of products and/or services within Illinois. Defendant has committed such purposeful acts and/or transactions in Illinois such that it reasonably should know and expect that it could be haled into this Court as a consequence of such activity.

6. Venue is proper in this district under 28 U.S.C. § 1400(b). On information and belief, Defendant has a place of business in Illinois and this District. On information and belief, from and within this District Defendant has committed at least a portion of the infringements at issue in this case.

7. For these reasons, personal jurisdiction exists and venue is proper in this Court under 28 U.S.C. § 1400(b).

## III. COUNT I
## (PATENT INFRINGEMENT OF UNITED STATES PATENT NO. 7,181,237)

8. Plaintiff incorporates the above paragraphs herein by reference.

9. On February 20, 2007, United States Patent No. 7,181,237 ("the '237 Patent") was duly and legally issued by the United States Patent and Trademark Office. The '237 Patent is titled "Control of a Multi-Mode, Multi-Band Mobile Telephone via a Single Hardware and

Software Man Machine Interface." A true and correct copy of the '237 Patent is attached hereto as Exhibit A and incorporated herein by reference.

10. Bunker IP is the assignee of all right, title and interest in the '237 patent, including all rights to enforce and prosecute actions for infringement and to collect damages for all relevant times against infringers of the '237 Patent. Accordingly, Bunker IP possesses the exclusive right and standing to prosecute the present action for infringement of the '237 Patent by Defendant.

11. The claims of the '237 patent (the "Claims") relate generally to, *inter alia*, multimode, multi-band mobile telephone systems, including those controlled via a single hardware and software man machine interface ("MMI"). (Ex. A at col. 1:8-11).

12. Different scopes of interface functionality typically induce different behavior, and often require the use of different software in the MMI. (*Id.* at col. 1:26-28). Where such specific software is used for different standards or modes, specific hardware (*e.g.*, specific hard keys, displays, and the like) may be required. (*Id.* at col. 1:28-31). Alternately, there may be redundant MMI software, increasing the need for added general hardware (*e.g.*, memory, processors, and the like) and increasing complexity to the user. (*Id.* at col. 1:31-34). Moreover, such MMIs can occupy a substantial portion of the telephone's memory compared with other of the telephone's software modules. (*Id.* at col. 1:34-39). Thus, in order to provide a multiple mode mobile telephone capable using multiple standards, a substantial portion of the telephone's memory had to be dedicated to storage of software providing multiple MMIs. (*Id.* at col. 1:40-43).

13. The claims of the '237 patent provide novel and inventive systems, hardware, software and architectures comprising the above-noted mode manager comprising a router for routing information first and second protocol stacks supporting first and second modes utilizing

first and second air interface standards, chipsets providing concurrent support, a user interface for communicating information and commands between protocol stacks and a user, and a bridge for providing communication of information between the first protocol stack and the second protocol stack, wherein control of the mobile telephone is provided via a single MMI that is substantially consistent across the first and second modes, with such systems, hardware, software and architectures comprising systems for controlling multi-mode mobile telephones via a single hardware and software MMI.

14. The claimed systems comprise a novel and inventive mode manager, which comprises a router and routing architecture for routing information to one of the first protocol stack and the second protocol stack. The mode manager is capable of, *inter alia*, providing for multimode (*e.g.*, dual mode) operation, including with capability between modes based on user-selection and/or automatic selection. For example, the user interface of the mobile telephone may provide a menu screen having options that allow a user to select the technology or network mode used by the telephone. (*Id.* at col. 8:63 – col. 9:6; Fig. 5). Users may advantageously select the mode or allow the system to automatically select a mode based on predetermined criteria and/or network status. (*Id.*).

15. The claimed systems further comprise a novel and inventive bridge architecture for providing communication of information between the first protocol stack and the second protocol stack. (*E.g.*, *id.* at col. 6:10-29). Without limitation, the bridge enables routing of information and messages between protocol stacks via serial connection when the protocol stacks are running on different chipsets. (*E.g.*, *id.* at col. 7:21-27).

16. The novel and inventive architecture also facilitates reading and writing of data to respective cores and sending messages with associated structures between various layers (*e.g.*,

the user interface to application layers). (*Id.* at col. 6:39-56). Further, application layers may convert between different protocol formats. (*Id.* at col. 7:17-56).

17. The claimed systems further comprise a novel and inventive MMI which communicates information and commands between the protocol stacks and a user. (*Id.* at col. 1:63-65). An application layer can reduce the functional interface between the protocol stacks to layers of the protocol stacks subsequent to the user interface, which, *inter alia*, allows control of the mobile telephone to be provided via a single MMI that is substantially consistent across all modes. (*Id.* at col. 1:65 – col. 2:3). Including in this manner, differences in technologies employed by the different air interface standards are made substantially transparent to mobile telephone users. (*Id.* at col. 5:6-9). Further, by providing for functionality of the different air interface standards at other levels of the respective protocol stacks, applications (*e.g.*, organizers, email clients, network browsers, and the like) may be more easily added to, removed from, or modified within the user interface without modification of the different protocol stacks so that the applications may support each air interface standard without special modification. (*Id.* at col. 5:9-17). This greatly reduces the complexity of the MMI, making the mobile telephone easier to use than would be a telephone employing different MMIs for each mode, or a telephone employing an MMI that is modified with redundant software for supporting both air interface standards. (*Id.* at col. 5:17-22).

18. The claimed inventions, including as a whole, are inventive and have multiple unconventional aspects. Conventional systems, which were known at the time of the invention, are represented by the primary references cited during prosecution of the ‘237 patent, which were U.S. Patent No. 6,785,556 to Souissi, U.S. Patent No. 6,934,558 to Sainton, and U.S. Patent No. 6,035,212 to Rostocker.

19. Neither Souissi, Sainton or Rostocker had the inventive features, alone or in combination, of (1) a mode manager comprising a router for routing information to one of a first protocol stack or second protocol stack; (2) a bridge for providing communication of information between the first protocol stack and the second protocol stack; (3) a mode manager for managing switching of the system between a first mode utilizing a first air interface standard supported by a first protocol stack and a second mode utilizing a second air interface standard supported by a second protocol stack wherein the first protocol stack and the second protocol stack are supported concurrently by at least one chipset of the mobile telephone; and/or (4) a user interface for communicating information and commands between the first and second protocol stacks and a user for controlling the mobile telephone and an application layer for reducing functional interface between the first and second protocol stacks to layers of the first and second protocol stacks subsequent to the user interface, wherein control of the mobile telephone is provided via a single man machine interface that is substantially consistent across the first and second modes.

20. All of the aforementioned inventive features, alone and in combination, contrast with the conventional features of existing art, including those of the primary Souissi, Sainton and Rostocker references, and thus they evidence the unconventionality of the claimed elements, alone and in combination. All of the aforementioned inventive features, alone and in combination, constitute unconventional, inventive concepts that go well beyond any concepts present in conventional or prior art.

21. **Direct Infringement.** Upon information and belief, Defendant has been directly infringing at least claims 1, 3, 7, and 9 of the ‘237 patent in Illinois, and elsewhere in the United States, by performing actions comprising at least making, using, selling, and/or offering to sell the ZTE Blade 10 (“Accused Instrumentality”) (*e.g.*, https://www.zteusa.com/blade-10.html).

22. The Accused Instrumentality is a mobile telephone system comprising a mode manager for managing switching of the system between a first mode utilizing a first air interface standard supported by a first protocol stack and a second mode utilizing a second air interface standard supported by a second protocol stack, the first protocol stack and the second protocol stack being supported concurrently by at least one chipset of the mobile telephone, the mode manager including a router for routing information to one of the first protocol stack and the second protocol stack. For example, on information and belief, the Accused Instrumentality comprises a mode manager (*e.g.*, the operating system of the Accused Instrumentality) for managing switching of the system (*e.g.*, the switching between cellular and Wi-Fi calling) between a first mode (*e.g.*, when the device sends/receives data via cellular) utilizing a first air interface standard (*e.g.*, LTE interface) supported by a first protocol stack (*e.g.*, LTE protocol stack) and a second mode (*e.g.*, when the device sends/receives data via Wi-Fi) utilizing a second air interface standard (*e.g.*, IEEE 802.11 a/b/g/n interface) supported by a second protocol stack (*e.g.*, IEEE 802.11 protocol stack), the first protocol stack (*e.g.*, LTE protocol stack) and the second protocol stack (*e.g.*, IEEE 802.11 protocol stack) being supported concurrently by at least one chipset of the mobile telephone (*e.g.*, processor of the Accused Instrumentality), the mode manager including a router for routing information (*e.g.*, call information, contact information, etc.) to one of the first protocol stack and the second protocol stack. The Accused Instrumentality supports both LTE and Wi-Fi connectivity. It can switch between cellular (*i.e.*, a first mode) and Wi-Fi (*i.e.*, a second mode) calling modes. The Accused Instrumentality has an operating system (*e.g.*, mode manager) to manage switching between cellular and Wi-Fi modes. By utilizing hardware, software, or both, the Accused Instrumentality's operating system routes communication information to one of the cellular network mode or Wi-Fi network mode. The

Accused Instrumentality supports Portable Hotspot functionality that would also utilize a mode manager (*e.g.*, operating system) for managing the switching between a first mode (*e.g.*, sending and receiving data via a cellular connection) and a second mode (*e.g.*, sending and receiving information via a Wi-Fi connection).

23. The Accused Instrumentality further comprises a user interface for communicating information and commands between the first protocol stack and a user and between the second protocol stack and the user for controlling the mobile telephone. On information and belief, the Accused Instrumentality comprises a user interface (*e.g.*, touchscreen of the Accused Instrumentality) for communicating information and commands (*e.g.*, Network information, network selection, calls, messaging, etc.) between the first protocol stack (*e.g.*, LTE protocol stack) and a user and between the second protocol stack (*e.g.*, IEEE 802.11 protocol stack) and the user for controlling the mobile telephone (*e.g.*, enabling and/or disabling the air interfaces, general mobile function controlling, calling, sending messages, etc.).

24. The Accused Instrumentality further comprises a bridge for providing communication of information between the first protocol stack and the second protocol stack. For example, on information and belief, the Accused Instrumentality comprises a bridge (*e.g.*, AXI Interconnect) for providing communication of information between the first protocol stack (*e.g.*, LTE protocol stack) and the second protocol stack (*e.g.*, IEEE 802.11 protocol stack). The bridge will enable communication between both protocol stacks (*e.g.*, Wi-Fi & LTE) to enable switching between Cellular and Wi-Fi calling modes. While utilizing hotspot tethering to enable communication between Wi-Fi and LTE, the Accused Instrumentality must also utilize a bridge which provides communication of information from LTE protocol to Wi-Fi protocol stack. The

bridge will enable communication between both protocol stacks (*e.g.*, Wi-Fi & LTE) so that data sent/received by cellular can be passed to tethered devices connected via Wi-Fi.

25. The Accused Instrumentality further comprises a system wherein control of the mobile telephone is provided via a single man machine interface that is substantially consistent across the first and second modes. For example, on information and belief, the Accused Instrumentality functions such that control of the mobile telephone (*e.g.*, the Accused Instrumentality) is provided via a single man machine interface (*e.g.*, touchscreen display of the Accused Instrumentality) that is substantially consistent across the first (*e.g.*, cellular call mode) and second modes (*e.g.*, Wi-Fi calling mode). Whether a phone is currently using a cellular connection, or a Wi-Fi based connection, the OS and GUI will remain the same.

26. The Accused Instrumentality further comprises a common database for storage of user data utilized by the first and second protocol stacks, the user data including at least one of an address book entry, a phonebook entry, a short message, an email, a ringing tone, and a picture. For example, on information and belief, the Accused Instrumentality comprises a common database for contact information for use by the first and second protocol stacks.

27. The Accused Instrumentality comprises a mobile telephone system comprising a first protocol stack for supporting a first air interface standard providing a first functionality, the first protocol stack being supported by a first chipset of the mobile telephone. For example, on information and belief, the Accused Instrumentality comprises a first protocol stack (*e.g.*, LTE protocol stack) for supporting a first air interface (*e.g.*, LTE interface) standard providing a first functionality (*e.g.*, sending/receiving data via cellular in a tethering scheme, or calling through cellular interface), the first protocol stack (*e.g.*, LTE protocol stack) being supported by a first chipset (*e.g.*, the processor of the Accused Instrumentality) of the mobile telephone.

28. The Accused Instrumentality further comprises a second protocol stack for supporting a second air interface standard providing a second functionality, to second protocol stack being supported concurrently with the first protocol stack by one of the first chipset and a second chipset of the mobile telephone. For example, on information and belief, the Accused Instrumentality comprises a second protocol stack (*e.g.*, Wi-Fi protocol stack) for supporting a second air interface (*e.g.*, Wi-Fi interface) standard providing a second functionality (sending/receiving data to and from a tethered device via Wi-Fi, or calling through Wi-Fi interface), to second protocol stack (*e.g.*, Wi-Fi protocol stack) being supported concurrently with the first protocol stack by the first chipset (*e.g.*, the processor of the Accused Instrumentality) of the mobile telephone.

29. The Accused Instrumentality further comprises a mode manager for managing switching of the system between a first mode utilizing the first air interface standard and a second mode utilizing the second air interface standard, the mode manager including a router for routing information to one of the first protocol stack and the second protocol stack. For example, on information and belief, the Accused Instrumentality comprises a mode manager (*e.g.*, the operating system of the Accused Instrumentality) for managing switching of the system (e.g. switching between Wi-Fi and LTE during tethering/hotspot functionality or Wi-Fi calling) between a first mode (*e.g.*, cellular call mode) utilizing a first air interface standard (*e.g.*, LTE interface) supported by a first protocol stack (*e.g.*, LTE protocol stack) and a second mode (*e.g.*, Wi-Fi calling mode) utilizing a second air interface standard (*e.g.*, IEEE 802.11 a/b/g/n interface) supported by a second protocol stack (*e.g.*, IEEE 802.11 protocol stack), the first protocol stack (*e.g.*, LTE protocol stack) and the second protocol stack (*e.g.*, IEEE 802.11 protocol stack) being supported concurrently by at least one chipset of the mobile telephone (*e.g.*, processor of the

Accused Instrumentality), the mode manager including a router for routing information (*e.g.*, data, call information, contact information, etc.) to one of the first protocol stack and the second protocol stack. The Accused Instrumentality supports both LTE and Wi-Fi connectivity. It can be switched between cellular call mode (i.e., a first mode) and wireless data network mode (i.e., a second mode) by utilizing user interface of the Accused Instrumentality. The Accused Instrumentality has an operating system (*e.g.*, mode manager) to manage switching between cellular and wireless data network modes. By utilizing hardware, software, or both, the Accused Instrumentality's operating system routes communication information to one of the cellular data network mode or wireless data network mode.

30. The Accused Instrumentality further comprises a user interface for communicating information and commands between the first protocol stack and a user and between the second protocol stack and the user for controlling the mobile telephone. For example, on information and belief, the Accused Instrumentality comprises a user interface (*e.g.*, touch screen of the Accused Instrumentality) for communicating information and commands (*e.g.*, network information, network selection, calls, messages, etc.) between the first protocol stack (*e.g.*, LTE protocol stack) and a user and between the second protocol stack (*e.g.*, IEEE 802.11 protocol stack) and the user for controlling the mobile telephone (*e.g.*, enabling and/or disabling the interfaces, calls, messages, etc.).

31. The Accused Instrumentality further comprises a bridge for providing communication of information between the first protocol stack and the second protocol stack. For example, on information and belief, the Accused Instrumentality comprises a bridge (*e.g.*, AXI Interconnect) for providing communication of information between the first protocol stack (*e.g.*, LTE protocol stack) and the second protocol stack (*e.g.*, IEEE 802.11 protocol stack). The

Accused Instrumentality must utilize a bridge which provides a communication interlink between the LTE protocol and the Wi-Fi protocol stack. The bridge will enable communication between both protocol stacks (*e.g.*, Wi-Fi & LTE) to enable switching between Cellular and Wi-Fi calling modes. While utilizing hotspot tethering to enable communication between Wi-Fi and LTE, the Accused Instrumentality must also utilize a bridge which provides communication of information from LTE protocol to Wi-Fi protocol stack. The bridge will enable communication between both protocol stacks (*e.g.*, Wi-Fi & LTE) so that data sent/received by cellular can be passed to tethered devices connected via Wi-Fi.

32. The Accused Instrumentality further comprises a system wherein control of the first and second functionalities is provided via a single man machine interface that is substantially consistent across the first and second modes. For example, on information and belief, the Accused Instrumentality comprises a system wherein control of the mobile telephone (*e.g.*, the Accused Instrumentality) is provided via a single man machine interface (*e.g.*, touchscreen display of the Accused Instrumentality) that is substantially consistent across the first (*e.g.*, cellular call/data mode) and second modes (*e.g.*, Wi-Fi call/data mode). When tethering the Accused Instrumentality's interface will remain the same whether it is currently sending/receiving data via cellular or Wi-Fi. Likewise, the Accused Instrumentality's interface will stay the same whether a call is being made via cellular or Wi-Fi.

33. The Accused Instrumentality further comprises a database for storage of data by the first and second protocol stacks. For example, on information and belief, the Accused Instrumentality comprises a common database (*e.g.*, internal memory's database) for storage of data utilized by the first and second protocol stacks, including but not limited to contact information.

## IV. COUNT II
## (PATENT INFRINGEMENT OF UNITED STATES PATENT NO. 8,843,641)

34. Plaintiff incorporates the above paragraphs herein by reference.

35. On September 23, 2014, United States Patent No. 8,843,641 ("the '641 Patent") was duly and legally issued by the United States Patent and Trademark Office. The '641 Patent is titled "Plug-In Connector System for Protected Establishment of a Network Connection." A true and correct copy of the '641 Patent is attached hereto as Exhibit B and incorporated herein by reference.

36. Bunker IP is the assignee of all right, title and interest in the '641 patent, including all rights to enforce and prosecute actions for infringement and to collect damages for all relevant times against infringers of the '641 Patent. Accordingly, Bunker IP possesses the exclusive right and standing to prosecute the present action for infringement of the '641 Patent by Defendant.

37. The invention in the '641 patent relates to a plug-in connector system, and a network plug and a network socket for protected establishment of a network connection, which is especially suitable for granting previously defined maintenance companies or maintenance technicians access to a system that is to be maintained. (Ex. B at col. 1:8-13).

38. Technical devices require maintenance which should only be undertaken by authorized personnel. (*Id.* at col. 1:16-19). This requires ensuring that only the appropriately authorized personnel access the maintenance functionality of a machine or system. (*Id.* at col. 1:19-21). Furthermore, mobile maintenance devices, such as laptop computers or mobile phones, are normally used, which obtain maintenance access by a locally accessible interface to a specific electronic device, such as another computer. (*Id.* at col. 1:28-33). The connection to the locally accessible interface is made by wire or wirelessly. (*Id.* at col. 1:33-34).

39. To grant access rights, an authentication check is usually performed in which a claimed identity is verified and thus the authorization for accessing the respective maintenance interface is checked. (*Id.* at col. 1:38-41). If the authentication check is successful, the access rights previously allocated to the respective user are granted. (*Id.* at col. 1:41-43).

40. Most known authentication methods are based on the entity to be authorized having to prove, in relation to a checking entity, that it is in possession of a secret and/or of an object. (*Id.* at col. 1:44-46). The best-known authentication method is the transmission of a password in which the authenticating entity transmits a secret password directly to a checking entity. (*Id.* at col. 1:47-49). The checking entity or the authentication checking unit respectively then check the correctness of the transmitted password. (*Id.* at col. 1:49-51). For administration of maintenance accesses in large systems, however, such a method involves a significant administrative overhead. (*Id.* at col. 1:52-54).

41. A further known option for secure administration of maintenance accesses is to provide the respective network sockets for maintenance access in an area to which access is physically protected. (*Id.* at col. 1:60-63). Such a method is, however, associated with uncertainties because a physical access protection can be overcome with little effort in most cases. (*Id.* at col. 1:65-67). In addition, this type of solution also demands significant administrative outlay, for example, for distributing and collecting the mechanical keys. (*Id.* at col. 1:67 – col. 2:2).

42. The inventors therefore created a system for administering and implementing access rights to maintenance functionalities that is operable securely and with little effort. (*Id.* at col. 2:6-9). The objects and advantages of the invention are achieved in accordance with the invention by a plug-in connector system, a network plug and a network socket, wherein the

inventive plug-in connector system for protected establishment of a network connection comprises a network plug featuring an authentication unit and a network socket featuring an authentication checking unit and an enabling unit. (*Id.* at col. 2:10-16). Generally, a checking command is transferred by the authentication checking unit to the authentication unit. (*Id.* at col. 2:19-20). Based the checking command, a checking response is determined by the authentication unit and transferred to the authentication checking unit. (*Id.* at col. 2:20-23). The checking response is checked by the authentication checking unit. (*Id.* at col. 2:23-24). In the event of a successful check of the checking response, a physical connection is enabled between the network plug and network socket for protected establishment of the network connection by the enabling device. (*Id.* at col. 2:24-27).

43. **Direct Infringement.** Upon information and belief, Defendant has been directly infringing at least claim 7 of the '641 patent in Illinois, and elsewhere in the United States, by making, using, selling and/or offering to sell the ZTE Blade 10 ("Accused Instrumentality") (*E.g.*, https://www.zteusa.com/blade-10.html).

44. The Accused Instrumentality has a network socket having an authentication checking unit and an enabling unit. For example, on information and belief, the Accused Instrumentality has a USB Type-C connection system, which is an authentication checking unit (*e.g.*, an Authentication Initiator in a USB Type-C authentication sequence), and an enabling unit that enables protected establishment of a network communication (*e.g.*, an Internet connection through USB tethering) subsequent to successful authorization of the computing device (*e.g.*, a Computer, Laptop, etc.). *E.g.*, https://www.zteusa.com/blade-10.html; https://www.usb.org/sites/default/files/documents/usb_authentication_20180904.zip (*e.g.*, Fig. B.1)).

45. The Accused Instrumentality has a network socket configured for implementation in a plug-in connection system for protected establishment of a network connection. For example, on information and belief, the Accused Instrumentality is configured for implementation in a plug-in connection system (*e.g.*, USB Type-C based connector system) for protected establishment of a network connection (*e.g.*, an Internet connection through USB tethering). https://www.zteusa.com/blade-10.html; https://www.usb.org/sites/default/files/documents/usb_authentication_20180904.zip).

46. The Accused Instrumentality has a network socket with an authentication checking unit configured to transfer a checking command to an authentication unit and to check a transferred checking response from the authentication unit, checking the transferred checking response comprising performing a cryptographic computation utilizing a stored cryptographic key. For example, on information and belief, the authentication checking unit (*e.g.*, an Authentication Initiator) of the Accused Instrumentality is configured to transfer a checking command (*e.g.*, a CHALLENGE Req) to the authentication unit (*e.g.*, the component of the Computer/Laptop which responds to the authentication requests/challenges) and to check a transferred checking response from the authentication unit, checking the transferred checking response comprising performing a cryptographic computation utilizing a stored cryptographic key. (*E.g.*, https://www.zteusa.com/blade-10.html; https://www.usb.org/sites/default/files/documents/usb_authentication_20180904.zip (*e.g.*, sections 2.2.1, 2.3, 2.3.2, Fig. B.1)).

47. The Accused Instrumentality has a network socket with an enabling unit being configured to enable a physical connection between a network connector and the network socket for protected establishment of the network connection in an event of a successful check of the

checking response transferred from the authentication unit. For example, on information and belief, the enabling unit is configured to enable a physical connection between the network connector (*e.g.*, a Computer, Laptop, etc.) and the network socket (*e.g.*, the Accused Instrumentality) for protected establishment of the network connection (*e.g.*, an Internet connection) in an event of a successful check of the checking response (*e.g.*, a CHALLENGE_AUTH Resp) by the authentication checking unit (*e.g.*, the Authentication Initiator is inherent in the Accused Instrumentality). The Accused Instrumentality verifies the checking response (*e.g.*, a CHALLENGE_AUTH Resp) and completes an authorization process in the event of a successful signature verification within the CHALLENGE_AUTH Resp. (*E.g.*, https://www.zteusa.com/blade-10.html; https://www.usb.org/sites/default/files/documents/usb_authentication_20180904.zip (*e.g.*, Fig. B.1)).

48. The Accused Instrumentality has a network socket that includes a communication unit for wired transfer of the checking command and the checking response between the authentication unit and the authentication checking unit. For example, on information and belief, the network socket (*e.g.*, the USB/Network Interface of the Accused Instrumentality) includes a communication unit (*e.g.*, USB communication unit) for wired transfer of the checking command (*e.g.*, a CHALLENGE Req) and the checking response (*e.g.*, a CHALLENGE_AUTH Resp) between the authentication unit (*e.g.*, the component of the Computer/Laptop which responds to the authentication requests/challenges) and the authentication checking unit (*e.g.*, Authentication Initiator is inherent in the Accused Instrumentality).

49. Plaintiff has been damaged as a result of Defendant's infringing conduct. Defendant is thus liable to Plaintiff for damages in an amount that adequately compensates

Plaintiff for such Defendant's infringement of the '237 patent and '641 patent, *i.e.*, in an amount that by law cannot be less than would constitute a reasonable royalty for the use of the patented technology, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

50. On information and belief, Defendant has had at least constructive notice of the '237 patent and '641 patent by operation of law and marking requirements have been complied with.

51. On information and belief, Defendant will continue its infringement of one or more claims of the '237 patent and '641 patent unless enjoined by the Court. Defendant's infringing conduct thus causes Plaintiff irreparable harm and will continue to cause such harm without the issuance of an injunction.

## V. JURY DEMAND

Plaintiff, under Rule 38 of the Federal Rules of Civil Procedure, requests a trial by jury of any issues so triable by right.

## VI. PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that the Court find in its favor and against Defendant, and that the Court grant Plaintiff the following relief:

a. Judgment that one or more claims of United States Patent No. 7,181,237 have been infringed, either literally and/or under the doctrine of equivalents, by Defendant;

b. Judgment that one or more claims of United States Patent No. 8,843,641 have been infringed, either literally and/or under the doctrine of equivalents, by Defendant;

c. Judgment that Defendant account for and pay to Plaintiff all damages to and costs incurred by Plaintiff because of Defendant's infringing activities and other conduct complained of herein, including any continuing or future infringement through the date such judgment is entered, including interest, costs, expenses, and an accounting of all infringing acts including, but not limited to, those future acts not presented at trial;

d. That Plaintiff be granted a permanent injunction pursuant to 35 U.S.C. § 283, enjoining Defendant, and all persons, including its officers, directors, agents, servants, affiliates, employees, divisions, branches, subsidiaries, parents, and all others acting in active concert or participation therewith, from making, using, offering to sell, or selling in the United States, or importing into the United States, any systems and/or devices that infringe any claim of the patents-in-suit, or contributing to, or inducing, the same by others, from further acts of infringement with respect to the claims of the '237 patent and '641 patent;

d. That Plaintiff be granted pre-judgment and post-judgment interest on the damages caused by Defendant's infringing activities and other conduct complained of herein;

e. That Plaintiff be granted such other and further relief as the Court may deem just and proper under the circumstances.

January 27, 2021

Respectfully Submitted,

*/s/ David R. Bennett*

David R. Bennett
Direction IP Law
P.O. Box 14184
Chicago, IL 60614-0184
(312) 291-1667
dbennett@directionip.com

*Attorneys for Plaintiff Bunker IP LLC*