IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

MOXCHANGE LLC, Plaintiff, v. **ALLIED TELESIS, INC.,** Defendant.	C.A. No. _____ **JURY TRIAL DEMANDED** **PATENT CASE**

ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Moxchange LLC files this Original Complaint for Patent Infringement against Allied Telesis, Inc., and would respectfully show the Court as follows:

I. THE PARTIES

1. Plaintiff Moxchange LLC ("Moxchange" or "Plaintiff") is a Texas limited liability company with its address at 15922 Eldorado Pkwy, Suite 500-1706, Frisco, TX 75035.

2. On information and belief, Defendant Allied Telesis, Inc. ("Defendant") is a corporation organized and existing under the laws of Delaware with a place of business at 19800 North Creek Parkway, Suite 100, Bothell, WA 98011. Defendant has a registered agent at The Prentice-Hall Corporation System, Inc., 251 Little Falls Dr., Wilmington, DE 19808.

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 Delaware Long-Arm Statute, due

at least to its business in this forum, including at least a portion of the infringements alleged herein.

5. Without limitation, on information and belief, within this state, Defendant has used the patented inventions thereby committing, and continuing to commit, acts of patent infringement alleged herein. In addition, on information and belief, Defendant has derived revenues from its infringing acts occurring within Delaware. Further, on information and belief, Defendant is subject to the Court's general jurisdiction, including from regularly doing or soliciting business and engaging in other persistent courses of conduct in Delaware. 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 Delaware and Defendant is a Delaware corporation. Defendant has committed such purposeful acts and/or transactions in Delaware 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 is incorporated in Delaware. Under the patent laws, because Defendant is incorporated in Delaware, Delaware is the only district in which it resides. 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. 7,860,254)

8. Plaintiff incorporates the above paragraphs herein by reference.

9. On December 28, 2010, United States Patent No. 7,860,254 ("the '254 Patent") was duly and legally issued by the United States Patent and Trademark Office. The '254 Patent is titled "Computer System Security Via Dynamic Encryption." A true and correct copy of the '254 Patent is attached hereto as Exhibit A and incorporated herein by reference.

10. Moxchange is the assignee of all right, title, and interest in the '254 patent, including all rights to enforce and prosecute actions for infringement and to collect damages for all relevant times against infringers of the '254 Patent. Accordingly, Moxchange possesses the exclusive right and standing to prosecute the present action for infringement of the '254 Patent by Defendant.

11. The application leading to the '254 patent was filed March 13, 2003. (Ex. A at cover).

12. The invention in the '254 Patent relates to the field of computer system security and more particularly to a dynamic data encryption and node authentication method and system that distributes the complexity of the encryption algorithm over the dynamics of data exchange and involves full synchronization of encryption key regeneration at system nodes, independent of the node clocks. (*Id.* at col. 1:8-13).

13. The objective of cryptography is to allow users to communicate securely through an insecure shared data communications channel while maintaining data integrity, privacy, and user authentication. (*Id.* at col. 1:15-18). For centuries, cryptographic systems have been developed that require a great deal of time to break, even when using large computational power. (*Id.* at col. 1:19-21). However, once an encryption key is obtained, the encryption mechanism and likely the entire system security is compromised and a new key is required. (*Id.* at col. 1:21-24). The two most common strategies for make an encryption system difficult to penetrate are:

(1) a long encryption key, and/or (2) a complex encryption function. (*Id.* at col. 1:25-28). For example, for an encryption key of length *n* bits, for large values of *n* a code breaker would need more than a lifetime to break the cipher. (*Id.* at col. 1:28-30). Simpler encryption functions, such as the logic XOR function, is easy to decipher no matter how long the key length is. (*Id.* at col. 1:28-33). For examples, a logic XOR operation is performed on one bit of data and its corresponding bit from the encryption key, one bit at a time: if the bits are the same then the result is 0 and if the bits are different then the result is 1. (*Id.* at col. 1:33-35). The simple linearity of the XOR function allows an intruder to decipher individual key fragments using a divide-and-conquer approach and then reconstruct the entire key once all the individual fragments are obtained. (*Id.* at col. 1:37-41). A non-linear exponential encryption function, such as Rivest-Sharmi-Adelman (RSA) system, is more difficult to apply a divide-and-conquer approach to break the key. (*Id.* at col. 1:41-44).

14. At the time the patent application was filed, there were two major cryptography system philosophies: 1) symmetric systems (static or semi-dynamic key), and 2) public key systems (static key). (*Id.* at col. 1:45-47). In symmetric systems, a key is exchanged between the users (the sender and receiver) and is used to encrypt and decrypt the data. (*Id.* at col. 1:47-50). There are three main problems with the symmetric system. (*Id.* at col. 1:20-21). First, the exchange of the key between the users introduces a security loophole, which can be alleviated through encrypting the exchanged key using a secure public key cryptography system. (*Id.* at col. 1:51-54). Second, using only one static encryption key makes it easier for an intruder to have sufficient time to break the key, which can be addressed using multiple session keys that are exchanged periodically. (*Id.* at col. 1:54-56). Third, and most important, is the susceptibility to an insider attack on the key where the time window between exchanging keys might be long

enough for a super user, who has super user privileges, to break in and steal the key. (*Id.* at col. 1:58-63).

15. In RSA public key cryptography system, a user generates two related keys, reveals one to the public ("public" key) to be used to encrypt any data sent and a second key that is private to the user ("private" key) that is used to decrypt received data by the user. (*Id.* at col. 1:64 – col. 2:2). The RSA cryptography system generates large random primes and multiplies them to get the public key and uses a complex encryption function such as mod and exponential operations, which makes the technique unbreakable in a lifetime for large keys (*e.g.*, higher than 256 bits) and eliminates the problem of insecure exchange of symmetric keys. (*Id.* at col. 2:2-8). However, the huge computational time required by RSA encryption and decryption, in addition to the time to generate the keys, is not appealing to users of the Internet and is therefore mainly used as one-shot solid protection of the symmetric cryptography key exchange. (*Id.* at col. 2:9-14). This one-shot protection, however, allows an internal super user with a helper to generate its own pair of encryption keys and replace the original keys. (*Id.* at col. 2:15-28). The sender then uses the super user's public key so the super user can decrypt the cipher text, store it, re-encrypt it using the original public key to continue the data to the original recipient for decrypting using the original private key without any knowledge of the break that occurred in the middle (a "super-user-in-the-middle" attack). (*Id.* at col. 2:15-28).

16. Even though both symmetric and public key cryptography systems are secure against outside attack, they are still vulnerable to insider attacks. (*Id.* at col. 2:29-31). A common way to protect a static encryption key is to save it under a file with restricted access but this cannot prevent a person with super user privileges from accessing the static key of the host file. (*Id.* at col. 2:37-45). Various attempts have been made to circumvent intrusion by outside

users, however, they are still prone to attack by super-user-in-the-middle attacks. (*Id.* at col. 2:46-56). The invention in the '254 patent alleviates these problems by providing continuous encryption key modification. (*Id.* at col. 2:58-59). New keys are generated from the previous key and data record, and are used to encrypt the subsequent data record. (*Id.* at col. 2:59-61).

17. There are several benefits to the claimed invention. The key lifetime is too small for an intruder to break and a super-user to copy. (*Id.* at col. 2:61-63). The invention also reduces the computations overhead by breaking the complexity of the encryption function and shifting it over the dynamics of data exchange. (*Id.* at col. 2:63-66). Speed is also improved by using a simple logic encryption function. (*Id.* at col. 2:66-67). Encryption is fully automated and all parties, the source user, destination user, and central authority, are clock-free synchronized and securely authenticated at all times. (*Id.* at col. 3:4-6). The invention also alleviates the super-user-in-the-middle attack because the intruder must obtain the entire set of keys at the right moment without being noticed to decrypt the entire ciphered message. (*Id.* at col. 3:7-10).

18. The novelty of generating new keys based on previous keys and data and using a logic operation, which resulted in the claimed benefits, was a point of novelty addressed during the prosecution history. During the prosecution in the USPTO of the application leading to the '254 patent, the examiner rejected the claims as obvious over two prior art references. (Ex. B at 3). The applicant appealed the decision and the Board agreed that the methods of the claims at issue here were not obvious. (Ex. B). The Board stated that even if it were assumed that the proposed modification by the examiner to combine the references was obvious and such a combination was operable, the prior art did not disclose the claimed invention. (Ex. B at 6). There was nothing in the prior art of record to suggest regenerating a new encryption key at a

source node as a function of a plaintext record and a previous encryption key by performing a logic operation on the previous encryption key and the plaintext as required by claim 1. (*Id.*)

19. **Direct Infringement.** Upon information and belief, Defendant has been directly infringing claim 1 of the '254 patent in Delaware, and elsewhere in the United States, by performing actions comprising at least using or performing the claimed method of providing a secure data stream between system nodes by using and testing the Allied Telesis TQm1402 ("Accused Instrumentality") (*e.g.*, https://www.alliedtelesis.com/en/products/wireless/tqm1402; https://www.alliedtelesis.com/sites/default/files/documents/manuals/ati-tq1402series-ug.pdf; https://www.alliedtelesis.com/sites/default/files/documents/datasheets/ati-tqm1402-ds.pdf).

20. For example, the Accused Instrumentality practices a method of providing a secure data stream (*e.g.*, secure data transmission over Wi-Fi) between system nodes (*e.g.*, the Accused Instrumentality and the accessories connected in a Wi-Fi network) using the IEEE 802.11i standard. Upon information and belief, the Accused Instrumentality performs the step of providing a previous encryption key (*e.g.*, a previous MIC key). For example, the Accused Instrumentality utilizes TKIP cipher suite to encrypt data blocks (*e.g.*, MSDUs). TKIP encrypt MSDU plaintext data with a keyed cryptographic message integrity code (MIC). A Michael key operation appends MSDU data with a MIC key. The Michael key operation also generates a new MIC Key for the next MSDU. A new MIC key is generated from the Michael key operation of a previous MIC key and a plaintext record.

21. Upon information and belief, the Accused Instrumentality performs the step of creating a data record (*e.g.*, MSDU) at a source node (*e.g.*, the Accused Instrumentality), the data record (*e.g.*, MSDU) including plaintext (*e.g.*, a plaintext MSDU) to be exchanged.

22. Upon information and belief, the Accused Instrumentality performs the step of regenerating a new encryption key (*e.g.*, a new MIC encryption key generated after N iterations with i=0 to i= N-1) at the source node (*e.g.*, the Accused Instrumentality) as a function of the data record and a previous encryption key by performing a logic operation (*e.g.*, a combination of logical operations) on the previous encryption key (*e.g.*, a previous MIC key) and the data record (*e.g.*, plaintext MSDU).

23. Upon information and belief, the Accused Instrumentality performs the step of performing a logic operation (*e.g.*, a combination of logical operations) on the previous encryption key (*e.g.*, a previous MIC key) and the data record (*e.g.*, MSDU) to form an expanded key (*e.g.*, a MIC encryption key generated after N-1 iterations with i=0 to i= N-2).

24. 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 '254 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.

25. On information and belief, Defendant has had at least constructive notice of the '254 patent by operation of law and, to the extent required, marking requirements have been complied with.

26. On information and belief, Defendant will continue its infringement of one or more claims of the '254 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.

IV. COUNT II
(PATENT INFRINGEMENT OF UNITED STATES PATENT NO. 7,233,664)

27. Plaintiff incorporates the above paragraphs herein by reference.

28. On June 19, 2007, United States Patent No. 7,233,664 ("the '664 Patent") was duly and legally issued by the United States Patent and Trademark Office. The '664 Patent is titled "Dynamic Security Authentication for Wireless Communication Networks." A true and correct copy of the '664 Patent is attached hereto as Exhibit C and incorporated herein by reference.

29. Moxchange is the assignee of all right, title, and interest in the '664 patent, including all rights to enforce and prosecute actions for infringement and to collect damages for all relevant times against infringers of the '664 Patent. Accordingly, Moxchange possesses the exclusive right and standing to prosecute the present action for infringement of the '664 Patent by Defendant.

30. The application leading to the '664 patent is a continuation-in-part to Application No. 10/387,711, which issued as the '254 patent. (Ex. C at cover). The '664 patent shares the same background of the invention as the '254 patent and therefore the background discussed above, Paragraphs 12-18, are incorporated by reference.

31. As a continuation-in-part application, the '664 patent adds a discussion in the specification of the need for security for wireless communications in networks, including allowing mobile communication devices to move between access ports or base stations while maintaining full, mutually secure authentication. (Ex. C at col. 3:4-12). In wireless local area networks, the Wired Equivalent Privacy (WEP) algorithm is used to protect wireless communication from eavesdropping. (*Id.* at col. 3:33-36). WEP relies on a secret encryption key that is shared between a supplicant, such as a wireless laptop personal computer, and an

access point. (*Id.* at col. 3:36-39). The secret key is used to encrypt data packets before they are transmitted, and an integrity check is used to ensure that packets are not modified in transit. (*Id.* at col. 3:39-41). The standard does not discuss how the shared key is established; however, in practice, most installations use a single key that is shared between all mobile stations and access points. (*Id.* at col. 3:41-44).

32. Ineffective WEP security lead to different types of attacks by outsiders. (*Id.* at col. 3:60-61). For example, a passive eavesdropper can intercept all wireless traffic and through known methodologies and educated guesses can narrow the field of the contents of a message and possibly determine the exact contents to of the message. (*Id.* at col. 3:45 – col. 4:6). Another type of attack when using a WEP algorithm is if an attacker knows the exact plaintext for one encrypted message, the attacker can use this knowledge to construct correct encrypted packet. (*Id.* at col. 4:7-17). Therefore, despite the WEP algorithm being part of the standard that describes communications in wireless local area networks, it fails to protect the wireless communications from eavesdropping and unauthorized access to wireless networks, primarily because it relies on a static secret key shared between the supplicant and the wireless network. (*Id.* at col. 4:18-24).

33. The claimed invention of the ‘664 patent provides the same benefits over the prior described above with respect to the ‘254 patent. (Ex. C at col. 4:25-54).

34. The prosecution history of the ‘664 patent further explains the unconventional features of the claimed invention. The examiner allowed the relevant claims without rejection because the prior art of record did not teach installing a node identifier at a first network node; sending the node identifier information from a first network node to a second network node, and

synchronously regenerating an authentication key at two network nodes based upon node identifier information. (Ex. D at 2).

35. **Direct Infringement.** Upon information and belief, Defendant has been directly infringing claim 1 of the '664 patent in Delaware, and elsewhere in the United States, by performing actions comprising using or performing the claimed method of providing secure authentication between wireless communication network nodes by using and/or testing the Allied Telesis TQm1402 ("Accused Instrumentality") (*e.g.*, https://www.alliedtelesis.com/en/products/wireless/tqm1402; https://www.alliedtelesis.com/sites/default/files/documents/manuals/ati-tq1402series-ug.pdf; https://www.alliedtelesis.com/sites/default/files/documents/datasheets/ati-tqm1402-ds.pdf).

36. For example, a system using the Accused Instrumentality practices a method of providing secure authentication between wireless communication (*e.g.*, Wi-Fi) network nodes (*e.g.*, the Accused Instrumentality and accessory devices such as a Wi-Fi enabled smartphone, etc.) using the IEEE 802.11i standard. Upon information and belief, the Accused Instrumentality provides wireless connection to accessory devices and allows them to join its Wi-Fi network and sets a password to secure the Wi-Fi network using WPA2 security, which is based on the IEEE 802.11i standard.

37. Upon information and belief, the Accused Instrumentality performs the step of providing a node identifier comprising an address (*e.g.*, MAC address) and an initial authentication key (*e.g.*, Pre-shared key or Pairwise master key).

38. Upon information and belief, the Accused Instrumentality performs the step of installing the node identifier (*e.g.*, MAC address and Pre-shared key or Pairwise master key) at a first network node (*e.g.*, accessory devices such as a Wi-Fi enabled smartphone, etc.). For

example, the accessory device enters or installs the Wi-Fi password as well as the MAC address in the Wi-Fi stack of the accessory device to initiate an association process with the Wi-Fi network of the Accused Instrumentality.

39. Upon information and belief, the Accused Instrumentality performs the step of storing the node identifier (*e.g.*, MAC address of an accessory device and Pre-shared key or Pairwise master key) at a second network node (*e.g.*, the Accused Instrumentality). For example, to join the Wi-Fi network of the Accused Instrumentality, an accessory device transmits a response for a beacon transmitted by the Accused Instrumentality or sends a probe request to the Accused Instrumentality. A Wi-Fi header comprises the MAC address of a sender. The Accused Instrumentality receives and stores the MAC address of the accessory device. Also, the Accused Instrumentality stores the Wi-Fi password, which is Pre-shared key or Pairwise master key (*e.g.*, initial authentication key) of its wireless personal network.

40. Upon information and belief, the Accused Instrumentality performs the step of sending node identifier information (*e.g.*, MAC address of an accessory device and Pre-shared key or Pairwise master key) from a first network node (*e.g.*, an accessory device such as a Wi-Fi enabled smartphone, etc.) to a second network node (*e.g.*, the Accused Instrumentality). The accessory device sends its MAC address (*e.g.*, address) as well as a key value derived from the Pre-shared key or Pairwise master key (*e.g.*, initial authentication key) to the Accused Instrumentality for authentication to connect to Wi-Fi network of the Accused Instrumentality. A Pairwise temporal key is derived from the Pre-shared key or Pairwise master key (*e.g.*, initial authentication key). The pairwise temporal key has two parts, KCK and KEK. In the authentication process, the accessory device acts as a supplicant. The accessory device transfers a key value derived from KCK in the EAPOL-message 2 to the Accused Instrumentality.

41. Upon information and belief, the Accused Instrumentality performs the step of synchronously regenerating an authentication key (*e.g.*, temporal keys) at two network nodes (*e.g.*, the Accused Instrumentality and an accessory device such as a Wi-Fi enabled smartphone, etc.) based upon node identifier information. The accessory device sends its MAC address (*e.g.*, address) as well as a key value derived from the Pre-shared key or Pairwise master key (*e.g.*, initial authentication key) to the Accused Instrumentality for authentication prior to connecting to the Wi-Fi network of the Accused Instrumentality. The Accused Instrumentality and the accessory device both regenerate temporal keys each time the devices get connected to each other. The Accused Instrumentality and the accessory device, both synchronously install temporal keys (*i.e.*, a Pairwise temporal key) with the help of a 4-way handshake message transfer having the node identifier information for establishing secured wireless communication.

42. 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 '664 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.

43. On information and belief, Defendant has had at least constructive notice of the '664 patent by operation of law and, to the extent required, marking requirements have been complied with.

44. On information and belief, Defendant will continue its infringement of one or more claims of the '664 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. COUNT III
(PATENT INFRINGEMENT OF UNITED STATES PATENT NO. 7,376,232)

45. Plaintiff incorporates the above paragraphs herein by reference.

46. On May 20, 2008, United States Patent No. 7,376,232 ("the '232 Patent") was duly and legally issued by the United States Patent and Trademark Office. The '232 Patent is titled "Computer System Security Via Dynamic Encryption." A true and correct copy of the '232 Patent is attached hereto as Exhibit E and incorporated herein by reference.

47. Moxchange is the assignee of all right, title, and interest in the '232 patent, including all rights to enforce and prosecute actions for infringement and to collect damages for all relevant times against infringers of the '232 Patent. Accordingly, Moxchange possesses the exclusive right and standing to prosecute the present action for infringement of the '232 Patent by Defendant.

48. The application leading to the '232 patent is also a continuation-in-part to Application No. 10/387,711, which issued as the '254 patent. (Ex. E at cover). The '232 patent shares the same background of the invention as the '254 patent and therefore the background discussed above, Paragraphs 12-18, are incorporated by reference.

49. The claimed invention of the '232 patent provides several benefits over the prior art. The invention provides fully automated security procedures with all system nodes synchronized and mutually authenticated. (Ex. E at col. 4:43-45). The claimed invention is also simple and fast but still secure against spying by an internal super-user or outside intruder due to the large number of dynamic keys (n) that would need to be broken or compromised—one key per ciphered data record, (n) parallel sessions of encryption, and zero entropy of the ciphered text. (*Id.* at col. 4:45-51). The invention also minimizes the exchange of keys between uses and/or the central authority. (*Id.* at col. 4:51-53). Another advantage is that an initial dynamic

authentication key (DAK) is securely exchanged between a user and central authority which is continuously regenerated during the entire life of the user, allowing the user and central authority to synchronize (realign DAKs) and authenticate to one another as needed for a communication session or when there is a disaster misalignment between a user and central authority. (*Id.* at col. 4:53-60).

50. The prosecution history of the '232 patent further explains the unconventional features of the claimed invention. The examiner contended that the relevant claims were invalid as anticipated. (*See* Ex. F at 5). Applicant filed an appeal brief to the Board of Patent Appeals. (Ex. F). Appliance argued that the prior art did not disclose providing a previous encryption key, selecting an old data record from the plurality of data record, and regenerating a new encryption key at a user node as a function of the previous encryption key and the old data record. (Ex. F at 6). In response to the appeal brief, the examiner dropped the rejection and issued a Notice of Allowability. (Ex. G).

51. **Direct Infringement.** Upon information and belief, Defendant has been directly infringing claim 1 of the '232 patent in Delaware, and elsewhere in the United States, by performing actions comprising using or performing the claimed method of providing a secure data stream between system nodes by using and/or testing the Allied Telesis TQm1402 ("Accused Instrumentality") (*e.g.*, https://www.alliedtelesis.com/en/products/wireless/tqm1402; https://www.alliedtelesis.com/sites/default/files/documents/manuals/ati-tq1402series-ug.pdf; https://www.alliedtelesis.com/sites/default/files/documents/datasheets/ati-tqm1402-ds.pdf).

52. For example, a system using the Accused Instrumentality practices a method of providing a secure data stream (*e.g.*, secure data transmission over Wi-Fi) between system nodes (*e.g.*, the Accused Instrumentality and the accessories connected over Wi-Fi network) using the

IEEE 802.11i standard. Upon information and belief, the Accused Instrumentality provides a data record block (*e.g.*, data payloads transferred between one node to other such an A-MSDU block) including a plurality of data records (*e.g.*, MSDUs) encrypted within a predetermined time interval (*e.g.*, a session). For example, the Accused Instrumentality provides wireless connection to accessory devices and allows them to join its Wi-Fi network and sets a password to secure the Wi-Fi network using WPA2 security, which is based on the IEEE 802.11i standard. The Accused Instrumentality exchanges data payloads with an associated device using an A-MSDU block. The block comprises multiple MSDUs data records. The Accused Instrumentality utilizes TKIP cipher suit to encrypt data records (*e.g.*, MSDUs). TKIP encrypts MSDU plaintext data with a keyed cryptographic message integrity code (MIC). A Michael key operation appends MSDU data with a MIC key. The Michael key operation also generates a new MIC Key for the next MSDU. An initial Michael key is generated from temporal keys such as PTK/GTK. These temporal keys are generated for a single session (*e.g.*, a predetermined time interval) only.

53. Upon information and belief, the Accused Instrumentality performs the steps of providing a previous encryption key, selecting an old data record (*e.g.*, a previous MSDU) from the plurality of data records (*e.g.*, a data file containing multiple MSDUs), and regenerating a new encryption key (*e.g.*, a new MIC encryption key) at a user node (*e.g.*, the Accused Instrumentality) as a function (*e.g.*, a combination of logical operations) of the previous encryption key (e *e.g.*, a previous MIC encryption key) and the old data record (e.g., a previous MSDU). For example, the Accused Instrumentality utilizes TKIP cipher suit to encrypt data records (*e.g.*, MSDUs). TKIP encrypt MSDU plaintext data with a keyed cryptographic message integrity code (MIC). A Michael key operation appends MSDU data with a MIC key. The

Michael key operation also generates a new MIC Key for the next MSDU. A new MIC key is generated from the Michael key operation of a previous MIC key and a previous plaintext record.

54. 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 '254 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.

55. On information and belief, Defendant has had at least constructive notice of the '254 patent by operation of law and, to the extent required, marking requirements have been complied with.

56. On information and belief, Defendant will continue its infringement of one or more claims of the '254 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.

IV. 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.

V. 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. 7,860,254 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. 7,233,664 have been infringed, either literally and/or under the doctrine of equivalents, by Defendant;

c. Judgment that one or more claims of United States Patent No. 7,376,232 have been infringed, either literally and/or under the doctrine of equivalents, by Defendant;

d. 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;

e. That Defendant be enjoined from future infringing activities;

f. 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; and

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

August 26, 2020

OF COUNSEL:

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

CHONG LAW FIRM, PA

/s/ Jimmy Chong

Jimmy Chong (#4839)
2961 Centerville Road, Suite 350
Wilmington, DE 19808
Telephone: (302) 999-9480
Facsimile: (877) 796-4627
Email: chong@chonglawfirm.com

Attorneys for Plaintiff Moxchange LLC