

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

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TEXAS
SHERMAN DIVISION

ANCORA TECHNOLOGIES, INC.,

Plaintiff,

v.

TCL CORP.,
TCL COMMUNICATION LTD., TCL
COMMUNICATION HOLDINGS
LTD. AND
TCL COMMUNICATION
TECHNOLOGY HOLDINGS LTD.

Defendants.

NO.

COMPLAINT

DEMAND FOR JURY TRIAL

COMPLAINT - 1
Case No.

1 1. Plaintiff, ANCORA TECHNOLOGIES, INC. (“Ancora”), for its Complaint
2 against TCL Corp., TCL Communication Ltd., TCL Communication Technology Holdings
3 Ltd., (collectively “TCL”) herein, states as follows:
4

5 **I. THE PARTIES**

6 2. Plaintiff Ancora Technologies, Inc. is a corporation organized and existing
7 under the laws of the State of Delaware and having a place of business at 23977 S.E. 10th
8 Street, Sammamish, Washington 98075.

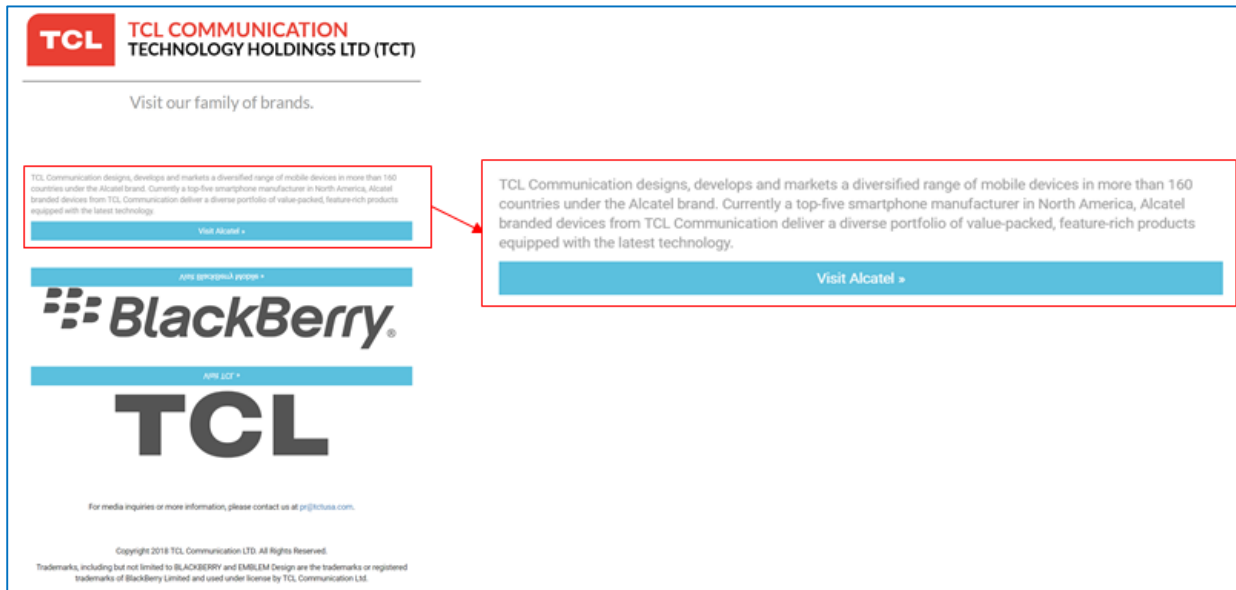
9 3. Upon information and belief, TCL Corp. is a corporation duly organized and
10 existing under the laws of the People’s Republic of China, having an address of No. 26, the
11 Third Road, Zhongkai Avenue, Huizhou City, Guangdong, P.R. China 516006.

12 4. Upon information and belief, TCL Communication Ltd. is a corporation duly
13 organized and existing under the laws of the People’s Republic of China, having an address of
14 7/F, Block F4, TCL International E City Zhong Shan Yuan Road, Nanshan District, Shenzhen
15 China.

16 5. Upon information and belief, TCL Communication Holdings Ltd. is a
17 corporation existing under the laws of China, with a principal place of business at TCL Tower,
18 15th floor, Gaoxin Nan Yi Road, Nanshan District, Shenzhen, Guangong, 518057 P.R. China.

19 6. Upon information and belief, TCL Communication Technology Holdings Ltd.
20 (“TCT”) is a corporation duly organized and existing under the laws of the People’s Republic
21 of China, having an address of Block F4, TCL Communication Technology Building, TCL
22 International E City, Zhong Shan Yuan Road, Nanshan District, Shenzhen, Guangdong, P.R.
23 China, 518052.

24 7. Upon information and belief, TCT is licensed to make, use, and sell Alcatel-
25 branded mobile devices in the United States.
26
27

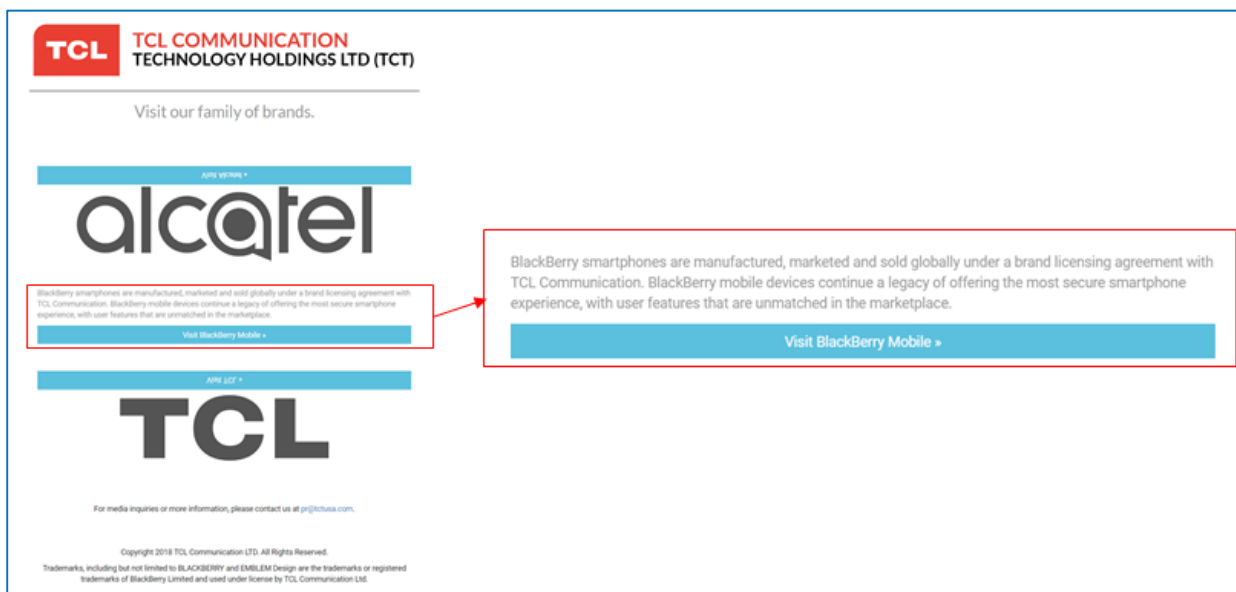


<http://www.tctusa.com/>



<https://us.alcatelmobile.com/about-us/>

8. Upon information and belief, TCT is licensed to make, use, and sell Blackberry-branded mobile devices in the United States.



<http://www.tctusa.com/>

About Us

BlackBerry smartphones are manufactured, marketed and sold globally under a brand licensing agreement with TCL Communication. As a top-5 smartphone manufacturer in North America, and a top manufacturer globally, TCL Communication's portfolio of products – which include Alcatel, BlackBerry and TCL branded devices – are currently sold in over 160 countries throughout North America, Latin America, Europe, the Middle East, Africa and Asia Pacifica.

TCL Communication operates nine R&D centers worldwide, employing thousands across the globe. For more information, please visit www.TCLCOM.com.

For media inquiries, please email us at PR@TCTUSA.com.

<https://blackberrymobile.com/us/about-us/>

9. The Defendants identified in paragraphs 2-5 above are an interrelated group of companies which together comprise a manufacturer and seller of Android mobile devices in the

1 United States, including Android mobile devices that are sold under the Alcatel and Blackberry
2 brands.

3 4 **II. JURISDICTION**

5 10. This is an action for infringement of United States patents arising under 35
6 U.S.C. §§ 271, 281, and 284–85, among others. This Court has subject matter jurisdiction of
7 the action under 28 U.S.C. § 1331 and § 1338(a).

8 11. This Court has personal jurisdiction over Defendants pursuant to due process
9 and/or the Texas Long Arm Statute because, *inter alia*, (i) Defendants have done and continue
10 to do business in Texas and (ii) Defendants have committed and continue to commit acts of
11 patent infringement in the State of Texas, including making, using, offering to sell, and/or
12 selling accused products in Texas, and/or importing accused products into Texas, including by
13 Internet sales and sales via retail and wholesale stores, inducing others to commit acts of patent
14 infringement in Texas, and/or committing a least a portion of any other infringements alleged
15 herein. In addition, or in the alternative, this Court has personal jurisdiction over Defendants
16 pursuant to Fed. R. Civ. P. 4(k)(2).

17 12. Venue is proper in this district pursuant to 28 U.S.C. §§ 1391(b), 1391(c), and
18 1400(b) because (i) Defendants have done and continue to do business in this district; (ii)
19 Defendants have committed and continue to commit acts of patent infringement in this district,
20 including making, using, offering to sell, and/or selling accused products in this district, and/or
21 importing accused products into this district, including by internet sales and sales via retail and
22 wholesale stores, and/or inducing others to commit acts of patent infringement in this district;
23 and (iii) Defendants are foreign entities.

24 13. Venue is proper as to Defendants, which are organized under the laws of the
25 People’s Republic of China, Hong Kong, and Canada. 28 U.S.C. § 1391(c)(3) provides that “a
26 defendant not resident in the United States may be sued in any judicial district, and the joinder
27

1 of such a defendant shall be disregarded in determining where the action may be brought with
2 respect to other defendants.”

3 4 **III. BACKGROUND**

5 14. On June 25, 2002, U.S. Patent No. 6,411,941 (“the ‘941 patent”) entitled
6 “Method Of Restricting Software Operation Within A License Limitation” was duly and legally
7 issued. (See Exhibit A, U.S. Patent No. 6,411,941.) A reexamination certificate also issued to
8 the ‘941 Patent on June 1, 2010 where the patentability of all claims was confirmed by the
9 United States Patent Office. (Exhibit B, Ex Parte Reexamination Certificate Issued Under 35
10 U.S.C. § 307.)

11 15. The ‘941 patent has been involved in litigation against Microsoft Corporation,
12 Dell Incorporated, Hewlett Packard Incorporated, and Toshiba America Information Systems.
13 (See 2009-cv-00270, Western District of Washington).

14 16. The ‘941 patent has also been involved in litigation against Apple Incorporated.
15 (See 2015-cv-03659, Northern District of California).

16 17. The ‘941 patent is currently involved in litigation against HTC America, Inc. and
17 HTC Corporation. (See 2016-cv-01919, Western District of Washington).

18 18. The ‘941 patent is currently involved in litigation against Samsung Electronics
19 America, Inc. and Samsung Electronics Co., Ltd. (See 2019-cv-00385, Western District of
20 Texas).

21 19. The ‘941 patent is currently involved in litigation against LG Electronics USA,
22 Inc. and LG Electronics, Inc. (See 2019-cv-00384, Western District of Texas).

23 20. The ‘941 patent was involved in a Covered Business Method proceeding before
24 the U.S. Patent and Trademark Office (See PTAB-CBM2017-00054). The U.S. Patent and
25 Trademark Office denied institution of the petition filed by HTC and found the ‘941 patent
26 recites a “technological improvement to problems arising in prior art software and hardware
27

1 methods of restricting an unauthorized software program's operation." (See PTAB-CBM2017-
2 00054, Paper No. 7 at pg. 9).

3
4 21. The U.S. Court of Appeals for the Federal Circuit further issued an order on
5 November 16, 2018 regarding the validity of the '941 patent. (See CAFC 18-1404, Dkt. # 39.)
6 In this appeal, the U.S. Court of Appeals for the Federal Circuit held:

7 [T]he claimed invention moves a software-verification structure to a BIOS
8 location not previously used for this computer-security purpose and alters how the
9 function is performed (in that the BIOS memory used for verification now
10 interacts with distinct computer memory to perform a software-verification
11 function), yielding a tangible technological benefit (by making the claimed system
12 less susceptible to hacking).

13 CAFC 18-1404, Dkt. # 39, pg. 13.

14
15 22. The U.S. Court of Appeals for the Federal Circuit further issued an order on
16 March 3, 2014 regarding claim construction and invalidity of the '941 Patent. (See CAFC 13-
17 1378, Dkt. # 57).

18 23. Ancora is the owner of all right, title and interest in the '941 patent.

19 **IV. COUNT I – PATENT INFRINGEMENT**

20 24. Ancora realleges the preceding paragraphs as though set forth fully herein.

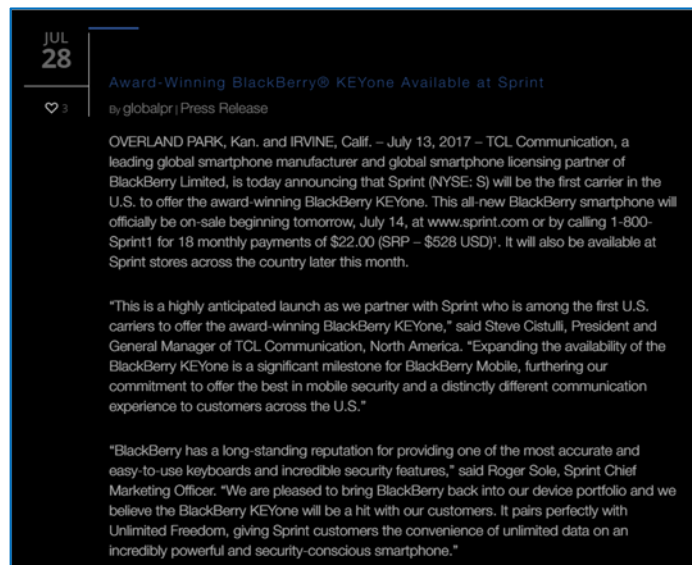
21 25. TCL has infringed the '941 patent in violation of 35 U.S.C. § 271(a) by, prior to
22 the expiration of the '941 patent, selling, and/or offering for sale in the United States, and/or
23 importing into the United States, without authorization, products that are capable of performing
24 at least Claim 1 of the '941 patent literally or under the doctrine of equivalents and/or, without
25 authorization, causing products to perform each step of at least Claim 1 of the '941 patent.

26 26. Accused Products include, but are not limited to, the Alcatel 3c/33x/3v/3L;
27 Alcatel 1c/1x/1/1t7/1T10; Alcatel A3/A3XL/A7XL/A7/A2XL/A3A; Alcatel A5; Alcatel IDOL

1 4/4S/5; Alcatel POP 4/4S/4PLUS; Alcatel PIXI 4(4)/4(5)/4(6); Blackberry KeyONE; and
2 Blackberry Key2 (“Accused Devices”).

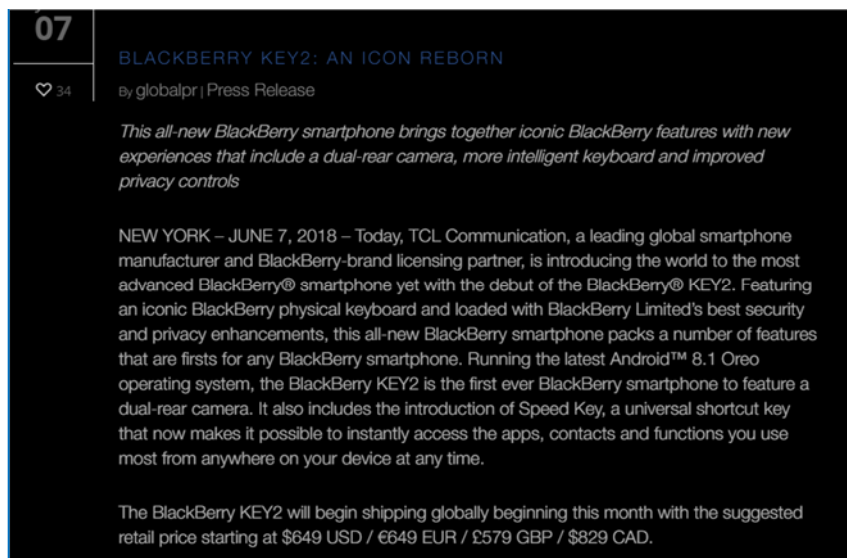
3
4 27. Upon information and belief, TCL began selling the accused Alcatel products
5 between 2016 - 2018.

6 28. Upon information and belief, TCL began selling the Blackberry KeyONE in
7 2017.



17 <https://blackberrymobile.com/press-room/>

19 29. Upon information and belief, TCL began selling the Blackberry Key2 in 2018.



<https://blackberrymobile.com/press-room/>

30. At a minimum, the Accused Products include servers/software utilized by TCL to transmit an over-the-air (“OTA”) software update, as well as those smartphones and other devices and technology that received from TCL, or received at TCL’s direction, an OTA update that caused such device to perform the method recited in Claim 1 prior to the expiration of the ’941 patent.

31. Such Accused Products are configured by TCL such that they are capable of performing each step of Claim 1 of the ’941 patent and to which TCL provided one or more OTA updates before the expiration of the ’941 patent that would cause a TCL device to perform each step of Claim 1 in order to upgrade its operating system. (See e.g., https://www.att.com/devicehowto/tutorial.html#!/stepbystep/id/stepbystep_KM1231051?make=BlackBerry&model=BBB100&gsi=mpo8f8; https://support.sprint.com/support/pages/printTemplate.jsp?articleId=WServiceAdvisory_542_GKB92134-dvc9760001prd.)

1 32. For example, Claim 1 of the '941 patent claims “a method of restricting software
2 operation within a license for use with a computer including an erasable, non-volatile memory
3 area of a BIOS of the computer, and a volatile memory area; the method comprising the steps
4 of: [1] selecting a program residing in the volatile memory, [2] using an agent to set up a
5 verification structure in the erasable, non-volatile memory of the BIOS, the verification
6 structure accommodating data that includes at least one license record, [3] verifying the
7 program using at least the verification structure from the erasable non-volatile memory of the
8 BIOS, and [4] acting on the program according to the verification.”

9 33. When TCL transmitted an OTA update, TCL performed and/or caused to be
10 performed each of these elements as part of what is described as “verified boot”:
11

Verified Boot

Verified Boot strives to ensure all executed code comes from a trusted source (usually device OEMs), rather than from an attacker or corruption. It establishes a full chain of trust, starting from a hardware-protected root of trust to the bootloader, to the boot partition and other verified partitions including `system`, `vendor`, and optionally `oem` partitions. During device boot up, each stage verifies the integrity and authenticity of the next stage before handing over execution.

In addition to ensuring that devices are running a safe version of Android, Verified Boot check for the correct version of Android with `rollback protection`. Rollback protection helps to prevent a possible exploit from becoming persistent by ensuring devices only update to newer versions of Android.

In addition to verifying the OS, Verified Boot also allows Android devices to communicate their state of integrity to the user.

12
13
14
15
16
17
18
19 <https://source.android.com/security/verifiedboot>
20

21 34. In particular, each mobile device contains both erasable, non-volatile memory in
22 the form of ROM and volatile memory in the form of RAM.

23 35. Further, each mobile device was configured by TCL to perform the below
24 described process (or one substantially like it) in order to install an OTA update:
25
26
27

Life of an OTA update

A typical OTA update contains the following steps:

1. Device performs regular check in with OTA servers and is notified of the availability of an update, including the URL of the update package and a description string to show the user.
2. Update downloads to a cache or data partition, and its cryptographic signature is verified against the certificates in `/system/etc/security/otacerts.zip`. User is prompted to install the update.
3. Device reboots into recovery mode, in which the kernel and system in the recovery partition are booted instead of the kernel in the boot partition.
4. Recovery binary is started by init. It finds command-line arguments in `/cache/recovery/command` that point it to the downloaded package.
5. Recovery verifies the cryptographic signature of the package against the public keys in `/res/keys` (part of the RAM disk contained in the recovery partition).
6. Data is pulled from the package and used to update the boot, system, and/or vendor partitions as necessary. One of the new files left on the system partition contains the contents of the new recovery partition.
7. Device reboots normally.
 - a. The newly updated boot partition is loaded, and it mounts and starts executing binaries in the newly updated system partition.
 - b. As part of normal startup, the system checks the contents of the recovery partition against the desired contents (which were previously stored as a file in `/system`). They are different, so the recovery partition is reflashed with the desired contents. (On subsequent boots, the recovery partition already contains the new contents, so no reflash is necessary.)

The system update is complete! The update logs can be found in `/cache/recovery/last_log.#`.

<https://source.android.com/devices/tech/ota/nonab>

36. For example, during this process, a program running on one or more OTA servers owned and/or controlled by TCL set up a verification structure in the erasable, non-volatile memory of the BIOS of the Accused Products by transmitting to the device an OTA update. The Accused Products are then configured by TCL to save to a partition (*e.g.*, the “cache” or “A/B” partitions) of the erasable, non-volatile memory of its BIOS.

37. The OTA update contains a verification structure that include data accommodating at least one license record. Examples of such a license record include a cryptographic signature or key:

Signing Builds for Release

Android OS images use cryptographic signatures in two places:

1. Each .apk file inside the image must be signed. Android's Package Manager uses an .apk signature in two ways:
 - When an application is replaced, it must be signed by the same key as the old application in order to get access to the old application's data. This holds true both for updating user apps by overwriting the .apk, and for overriding a system app with a newer version installed under /data.
 - If two or more applications want to share a user ID (so they can share data, etc.), they must be signed with the same key.
2. OTA update packages must be signed with one of the keys expected by the system or the installation process will reject them.

https://source.android.com/devices/tech/ota/sign_builds

38. Such license record also may comprise a cryptographic hash or hash tree:

Verifying Boot

Verified boot requires cryptographically verifying all executable code and data that is part of the Android version being booted before it is used. This includes the kernel (loaded from the `boot` partition), the device tree (loaded from the `dtbo` partition), `system` partition, `vendor` partition, and so on.

Small partitions, such as `boot` and `dtbo`, that are read only once are typically verified by loading the entire contents into memory and then calculating its hash. This calculated hash value is then compared to the *expected hash value*. If the value doesn't match, Android won't load. For more details, see [Boot Flow](#).

Larger partitions that won't fit into memory (such as, file systems) may use a hash tree where verification is a continuous process happening as data is loaded into memory. In this case, the root hash of the hash tree is calculated during run time and is checked against the *expected root hash value*. Android includes the `dm-verity` driver to verify larger partitions. If at some point the calculated root hash doesn't match the *expected root hash value*, the data is not used and Android enters an error state. For more details, see [dm-verity corruption](#).

The *expected hashes* are typically stored at either the end or beginning of each verified partition, in a dedicated partition, or both. Crucially, these hashes are signed (either directly or indirectly) by the root of trust. As an example, the AVB implementation supports both approaches, see [Android Verified Boot](#) for details.

<https://source.android.com/security/verifiedboot/verified-boot>.

39. Once the verification structure has been set up in the BIOS, the Accused Products are configured by TCL to reboot into recovery mode, load the OTA update into its volatile memory (e.g., RAM), and use the at least one license record from the BIOS to verify the OTA update.

1 40. If the OTA update is verified, the Accused Products are configured to load and
2 execute the update.

3 41. In sum, as described above, once TCL has set up the verification structure by
4 transmitting to a device an OTA update, each Accused Product is configured to automatically
5 perform each of the remaining Claim 1 steps.

6 42. Further, on information and belief, when TCL provided OTA updates, TCL
7 performed or caused to be performed each of the Claim 1 steps.

8 43. Further, TCL conditions participation in the OTA update process and the receipt
9 of the benefit of a software update on the performance of each of the above steps.

10 44. Primarily, as described above, TCL pre-configures/programs each Accused
11 Product to perform the above described steps upon receiving an OTA update from TCL.

12 45. Further, TCL takes steps to ensure that each Accused Product cannot install an
13 OTA update except by performing each of the above described steps.

14 46. Further, TCL emphasizes the benefits associated with updating the software of
15 its Accused Products.

16 47. Further, TCL controlled the manner of the performance of such method. As set
17 forth above, TCL configured each Accused Product such that, upon receiving an OTA update,
18 it would automatically perform each remaining step of the claimed method.

19 48. TCL also controlled the timing of the performance of such method by
20 determining when to utilize its OTA servers/software to set up a verification structure in each
21 Accused Product.

22 49. TCL also had the right and ability to stop or limit infringement simply by not
23 performing the initial step of using its OTA servers/software to set up a verification structure in
24 each Accused Product. Absent this action by TCL, the infringement at issue would not have
25 occurred.
26
27

1 50. TCL's infringement has caused damage to Ancora, and Ancora is entitled to
2 recover from TCL those damages Ancora has sustained as a result of TCL's infringement.
3

4 **V. DEMAND FOR RELIEF**

5 WHEREFORE, Plaintiff prays for judgment as follows:

6 A. Declaring that TCL has infringed United States Patent No. 6,411,941 in violation
7 of 35 U.S.C. § 271;

8 B. Awarding damages to Ancora arising out of this infringement, including enhanced
9 damages pursuant to 35 U.S.C. § 284 and prejudgment and post-judgment interest, in an amount
10 according to proof;

11 C. Awarding such other costs and relief the Court deems just and proper, including
12 any relief that the Court may deem appropriate under 35 U.S.C. § 285.
13

14 **VI. DEMAND FOR JURY TRIAL**

15 Ancora respectfully demands a trial by jury of any and all issues triable of right by a
16 jury in the above-captioned action.
17

18 DATED: August 27, 2019

SIEBMAN FORREST BURG
& SMITH, LLP
Federal Courthouse Square
300 N. Travis
Sherman, TX 75090
(903) 870-0070
(903) 870-0066 Telefax
Clyde M. Siebman
Texas State Bar #18341600
clydesiebman@siebman.com
Elizabeth S. Forrest
Texas State Bar #24086207
elizabethforrest@siebman.com

25 By: /s/ Clyde M. Siebman
26 Clyde M. Siebman
27

BROOKS KUSHMAN P.C.

John P. Rondini (pending admission *pro hac vice*)

Mark A Cantor (pending admission *pro hac vice*)

John S. LeRoy (pending admission *pro hac vice*)

Marc Lorelli (pending admission *pro hac vice*)

1000 Town Center, 22nd Floor

Southfield, Michigan 48075-1238

Tel.: (248) 358-4400

Fax: (248) 358-3351

Email: jrondini@brookskushman.com

mcantor@brookskushman.com

jleroy@brookskushman.com

mlorelli@brookskushman.com

Attorneys for Plaintiff Ancora Technologies, Inc.