IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

CASSIOPEIA IP LLC, Plaintiff, v. **HISENSE USA CORPORATION,** Defendant.	Civil Action File No.: _____ **JURY TRIAL DEMANDED**

COMPLAINT FOR INFRINGEMENT OF PATENT

Now comes, Plaintiff Cassiopeia IP LLC ("Plaintiff" or "Cassiopeia"), by and through undersigned counsel, and respectfully alleges, states, and prays as follows:

NATURE OF THE ACTION

1. This is an action for patent infringement under the Patent Laws of the United States, Title 35 United States Code ("U.S.C.") to prevent and enjoin Defendant Hisense USA Corporation (hereinafter "Defendant"), from infringing and profiting, in an illegal and unauthorized manner, and without authorization and/or consent from Plaintiff from U.S. Patent No. 7,322,046 ("the '046 Patent" or the "Patent-in-Suit"), which is attached hereto as Exhibit A and incorporated

herein by reference, and pursuant to 35 U.S.C. §271, and to recover damages, attorney's fees, and costs.

THE PARTIES

2. Plaintiff is a Texas limited liability company with its principal place of business at 6205 Coit Road, Suite 300-1017, Plano, Texas 75024.

3. Upon information and belief, Defendant is a corporation organized under the laws of Georgia, having a principal place of business at 7310 McGinnis Ferry Road, Suwanee, GA, 30024. Upon information and belief, Defendant may be served with process c/o: Bryce Mowbray**,** 3559 Gus Way, Powder Springs, GA, 30127**.**

4. Plaintiff is further informed and believes, and on that basis alleges, that Defendant operates the website www.hisense-usa.com, which is in the business of providing smart TVs using secure network services. Defendant derives a portion of its revenue from sales and distribution via electronic transactions conducted on and using at least, but not limited to, its Internet website located at www.hisense-usa.com, and its incorporated and/or related systems or products (collectively the "Hisense Website"). Plaintiff is informed and believes, and on that basis alleges, that, at all times relevant hereto, Defendant has done and continues to do business in this judicial district, including, but not limited to,

providing products/services to customers located in this judicial district by way of the Hisense Website.

JURISDICTION AND VENUE

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

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

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

8. Defendant is subject to this Court's specific and general personal jurisdiction pursuant to its substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Georgia and in this judicial District; and (iii) being incorporated in this District.

9. Venue is proper in this judicial district pursuant to 28 U.S.C. §1400(b) because Defendant resides in this District under the Supreme Court's opinion in

TC Heartland v. Kraft Foods Group Brands LLC, 137 S. Ct. 1514 (2017) through its incorporation in this District, and/or through its having committed acts of infringement in this District together with its regular and established place of business in this District.

FACTUAL ALLEGATIONS

10. On January 22, 2008, the United States Patent and Trademark Office ("USPTO") duly and legally issued the '046 Patent, entitled "METHOD AND SYSTEM FOR THE SECURE USE OF A NETWORK SERVICE" after a full and fair examination. The '046 Patent is attached hereto as Exhibit A and incorporated herein as if fully rewritten.

11. Plaintiff is presently the owner of the '046 Patent, having received all right, title and interest in and to the '046 Patent from the previous assignee of record. Plaintiff possesses all rights of recovery under the '046 Patent, including the exclusive right to recover for past infringement.

12. The invention claimed in the '046 Patent comprises a method for the secure use of a network service using a blackboard on which all usable services are entered.

13. Claim 1 of the '046 Patent states:

> "1. A method for the secure use of a network service using a blackboard on which all usable services are entered, the method comprising the steps of: detecting a service which has not yet been entered on the blackboard; executing a first check to determine whether use of the service is allowed; entering the service in the blackboard only if it is determined that use of the service is allowed; loading an interface driver related to the service on the blackboard; extending the loaded interface driver on the blackboard with at least one security function to form a secured interface driver; loading the secured interface driver related to the service prior to the first use of the service; and executing a second check by a second security function prior to the use of the service to determine if use of the service is allowed by a user." *See* Exhibit A.

14. Defendant commercializes, inter alia, methods that perform all the steps recited in at least one claim of the '046 Patent. More particularly, Defendant commercializes, inter alia, methods that perform all the steps recited in Claim 1 of the '046 Patent. Specifically, Defendant makes, uses, sells, offers for sale, or imports a method that encompasses that which is covered by Claim 1 of the '046 Patent.

DEFENDANT'S PRODUCTS

15. Defendant offers solutions, such as the "120" Class – L10 Series TV" (the "Accused Instrumentality"), that enables a method for the secure use of a network service using a blackboard on which all usable services are entered. For example, the Accused Instrumentality performs the method for the secure use of a

network service using a blackboard on which all usable services are entered. A non-limiting and exemplary claim chart comparing the Accused Instrumentality to Claim 1 of the '046 Patent is attached hereto as Exhibit B and is incorporated herein as if fully rewritten.

16. As recited in Claim 1, upon information and belief, the Accused Instrumentality, practices a method for secure use of a network service (e.g., casting via DIAL onto various applications on the TV) using a blackboard (e.g., a software/hardware component that stores all available devices and applications you can cast to) on which all usable services (e.g., DIAL casting/streaming devices and applications) are entered. *See* Exhibit B.

17. As recited in one step of Claim 1, upon information and belief, the Accused Instrumentality supports casting from a smartphone via DIAL. The Accused Instrumentality comes preloaded with Netflix and YouTube which utilize DIAL for casting. The DIAL protocol allows a client (e.g. a smartphone) to discover DIAL servers (e.g. the Accused Instrumentality) and access DIAL services (e.g. ability to cast onto and activate applications on the Accused Instrumentality). Upon information and belief, the Accused Instrumentality must utilize a blackboard (e.g. database or lookup table) that stores services. *See* Exhibit B.

18. As recited in another step of Claim 1, upon information and belief, the Accused Instrumentality utilizes a system in which a service which has not yet been entered on a blackboard is detected. A DIAL client (e.g. a smartphone) will send out an M-SEARCH to discover DIAL enabled TVs/servers. In response, the DIAL enabled TV will send a response with a location header that includes an HTTP URL that hold an UPnP description of the TV. The DIAL client (e.g. a smartphone) will then send and HTTP GET message to the HTTP URL in the location header. If the HTTP GET is sent to the correct HTTP URL originally provided by the DIAL enabled TV, the TV will send the DIAL client (e.g. a smartphone) a DIAL REST SERVICE URL that identifies the services (e.g. applications that can be used such as Netflix or YouTube) a client can utilize. The applications will be represented as resources identified by URLs known as Application resource URLs. As such, the DIAL REST SERVICE will then be added to a list of available services that was previously not discovered. *See* Exhibit B.

19. As recited in another step of Claim 1, upon information and belief, the Accused Instrumentality utilizes a system in which a first check is executed to determine whether a user of the service is allowed. A DIAL client sends out an M-SEARCH that defines particular services that the client is looking for. A UPnP

device will only respond to this request if they provide services that the client is searching for. This serves as a first check that ensures that the services provided by a DIAL server responding to the client can in fact be used by the client. *See* Exhibit B.

20. As recited in another step of Claim 1, upon information and belief, the Accused Instrumentality will only enter the service (e.g. access to a DIAL server and its services) in the blackboard (e.g. a database or list of available servers/services) only if it is determined that the use of the service is allowed (e.g. the server/service responding to a client request matches the service defined in the request). *See* Exhibit B.

21. As recited in another step of Claim 1, upon information and belief, the Accused Instrumentality utilizes a system that loads an interface driver related to the service on the blackboard (e.g. the client's receipt of a DIAL REST SERVICE URL that identifies the services that can be provided by a DIAL server/TV and which further contains Application Resource URLs). The client's receipt of the DIAL REST SERVICE URL and the contained Application Resource URLs allows the client to interface with the DIAL server/TV in order to launch a service/application on the said DIAL server/TV, since operations related to an application are performed by HTTP request to said Application Resource URLs).

A DIAL client (e.g. a smartphone) will send out an M-SEARCH to discover DIAL enabled TVs/servers. In response, the DIAL enabled TV will send a response with a location header that includes an HTTP URL that holds an UPnP description of the TV. The DIAL client (e.g. a smartphone) will then send and HTTP GET message to the HTTP URL in the location header. If the HTTP GET is sent to the correct HTTP URL originally provided by the DIAL enabled TV, the TV will send the DIAL client (e.g. a smartphone) a DIAL REST SERVICE URL that identifies the services (e.g. applications that can be used such as Netflix or YouTube) a client can utilize. The applications will be represented as resources identified by URLs known as Application Resource URLs. *See* Exhibit B.

22. As recited in another step of Claim 1, upon information and belief, the Accused Instrumentality practices extending the loaded interface driver (e.g., the Application Resource URL that identifies an application will be used by the client to send an HTTP GET request) on the blackboard (e.g., a software/hardware component which logs services and service software) with at least one security function (e.g., a check to determine that an HTTP GET request is valid and that the Application Name included in the request is recognized) to form a secured interface driver (e.g., upon validation that an HTTP GET request is valid and that

an Application Name is recognized, the system will allow the client to load the desired application on the DIAL server/TV). *See* Exhibit B.

23. As recited in another step of Claim 1, upon information and belief, the Accused Instrumentality loads an interface driver by providing a DIAL REST Service that contains Application Resource URLs. The DIAL REST Service and its contained Application Resource URLs are considered an interface driver because they allow for the DIAL client to interface with the DIAL server/TV. The interface driver, in this case the DIAL REST Service and its contained Application Resource URLs, are extended with a security function when the Application Resource URL is further combined with an HTTP GET request which is then subject to a validation of the request itself and the Application Name it contains. If the validations are successful, the DIAL server will execute the desired application (e.g. Netflix or YouTube) and send a confirmation of the execution. *See* Exhibit B.

24. As recited in another step of Claim 1, upon information and belief, the Accused Instrumentality loads the secured interface driver related to the service prior to the first use of the service (e.g. upon validation of an HTTP GET request and its contained Application Name, the DIAL server/TV will launch a desired application (e.g. Netflix or YouTube) that will then allow a DIAL client (e.g. a smartphone) to cast a program onto the application (e.g. the Netflix or YouTube

application on a DIAL server/TV) using said client device) and executing a second check by a second security function prior to the use of the service to determine if use of the service is allowed by a user (e.g. before the application can be used on the DIAL server/TV, the user must be logged into their account on the DIAL server/TV's version of the application as well). The DIAL protocol outlines that an application, as it exists on a DIAL enabled TV, will be launched after the successful validation of an HTTP GET request and its contained Application Name. The TV version of the application must be launched before casting services can be used. *See* Exhibit B.

25. The elements described in paragraphs 15-24 are covered by at least Claim 1 of the '046 Patent. Thus, Defendant's use of the Accused Instrumentality is enabled by and infringes the method described in the '046 Patent.

INFRINGEMENT OF THE '046 PATENT

26. Plaintiff realleges and incorporates by reference all of the allegations set forth in the preceding Paragraphs.

27. In violation of 35 U.S.C. § 271, Defendant is now, and has been directly infringing the '046 Patent.

28. Defendant has had knowledge of infringement of the '046 Patent at least as of the service of the present Complaint.

29. Defendant has directly infringed and continues to directly infringe at least one claim of the '046 Patent by using, at least through internal testing or otherwise, the Accused Instrumentality without authority in the United States, and will continue to do so unless enjoined by this Court. As a direct and proximate result of Defendant's direct infringement of the '046 Patent, Plaintiff has been and continues to be damaged.

30. By engaging in the conduct described herein, Defendant has injured Plaintiff and is thus liable for infringement of the '046 Patent, pursuant to 35 U.S.C. § 271.

31. Defendant has committed these acts of infringement without license or authorization.

32. As a result of Defendant's infringement of the '046 Patent, Plaintiff has suffered monetary damages and is entitled to a monetary judgment in an amount adequate to compensate for Defendant's past infringement, together with interests and costs.

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

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

DEMAND FOR JURY TRIAL

35. Plaintiff demands a trial by jury of any and all causes of action.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for the following relief:

a. That Defendant be adjudged to have directly infringed the '046 Patent either literally or under the doctrine of equivalents;

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

c. That Defendant, its officers, directors, agents, servants, employees, attorneys, affiliates, divisions, branches, parents, and those persons in active concert or participation with any of them, be permanently restrained and enjoined from directly infringing the '046 Patent;

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

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

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

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

[signatures on next page]

Dated: July 29, 2019

Respectfully submitted,

/s/Daniel A. Kent

Daniel A. Kent
Georgia Bar No. 415110
dankent@kentrisley.com
Ph: (404) 585-4214
Fx: (404) 829-2412
KENT & RISLEY LLC
5755 N Point Pkwy, Suite 57
Alpharetta, GA 30022

Of Counsel:

Howard L. Wernow
(to be admitted pro hac vice)
Andrew S. Curfman
(to be admitted pro hac vice)
SAND, SEBOLT &WERNOW CO., LPA
Aegis Tower - Suite 1100
4940 Munson Street, N. W.
Canton, Ohio 44718
Ph: 330-244-1174
Fx: 330-244-1173
Howard.Wernow@sswip.com
Andrew.Curfman@sswip.com

Attorneys for Plaintiff