BRADFORD J. BLACK (SBN 252031)
bblack@bradfordblack.com
BRADFORD BLACK P.C.
4 Embarcadero Ctr., Suite 1400
San Francisco, CA 94111
Telephone: (415) 813-6211
Facsimile: (415) 813-6222

DAVID C. RADULESCU (*pro hac vice to be submitted*)
david@radip.com
TIGRAN VARDANIAN (*pro hac vice to be submitted*)
tigran@radip.com
DANIEL KESACK (*pro hac vice to be submitted*)
dan@radip.com
RADULESCU LLP
The Empire State Building
350 Fifth Avenue, Suite 6910
New York, NY 10118
Telephone: (646) 502-5950
Facsimile: (646) 502-5959

Attorneys for Plaintiff
UPF INNOVATIONS, LLC

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

UPF INNOVATIONS, LLC, a Texas limited liability company,

Plaintiff,

v.

REDPINE SIGNALS, INC., a California corporation,

Defendant.

Case No. 3:18-cv-814

COMPLAINT FOR PATENT INFRINGEMENT

JURY TRIAL DEMANDED

Plaintiff UPF Innovations, LLC ("UPF"), by and through its attorneys, brings this action and makes the following allegations of patent infringement relating to U.S. Patent No. RE40,188 ("the '188 Patent" or "the patent-in-suit"). Defendant Redpine Signals, Inc. ("Redpine") infringes the patent-in-suit in violation of the patent laws of the United States of America, 35 U.S.C. § 1 *et seq*., and UPF seeks compensation for this infringement.

PARTIES

1. Plaintiff UPF Innovations, LLC is a Texas Limited Liability Company with its principal place of business located at 3800 N. Lamar Blvd., Suite 200, Austin, TX 78756.

2. On information and belief, Defendant Redpine Signals, Inc. is a California corporation with its principal place of business at 2107 North First Street, Suite 540, San Jose, CA, 95131. Redpine can be served through its registered agent, Jose Palma, 111 Race St, San Jose, CA 95126.

3. On information and belief, Redpine was founded in 2001, and is headquartered in San Jose, California.[1]

4. On information and belief, Redpine conducts engineering, research and development, sales and administration activities at its headquarters in San Jose, California.[2]

5. On information and belief, Redpine offers infringing products for sale throughout the United States, including in the Northern District of California.

JURISDICTION AND VENUE

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

7. Upon information and belief, this Court has personal jurisdiction over Redpine in this action because Redpine has committed acts within the Northern District of California giving rise to this action and has established minimum contacts with this forum such that the exercise of

[1] REDPINE WEBPAGE, available at http://www.redpinesignals.com/Contact_Us/ (accessed January 31, 2018).

[2] REDPINE WEBPAGE, available at http://www.redpinesignals.com/About_Us/culture_of_innovation.php (accessed January 31, 2018)

jurisdiction over Redpine would not offend traditional notions of fair play and substantial justice. Redpine, directly and/or through subsidiaries or intermediaries (including distributors, retailers, and others), has committed and continues to commit acts of infringement in this District by, among other things, offering to sell and selling products and/or services that infringe the patent-in-suit. Moreover, Redpine maintains its headquarters and principle place of business in San Jose, California[3]; is registered to do business in the State of California[4]; and has appointed Jose Palma, 111 Race St, San Jose, CA 95126, as its agent for service of process.

8. Venue is proper in this district under 28 U.S.C. § 1400(b). Redpine resides in California because California is its state of incorporation. Further, Redpine has a regular and established place of business in the Northern District of California, in San Jose, California, at 2107 North First Street, Suite 540, San Jose, CA. Consistent with its physical presence in San Jose, California, Redpine advertises its presence in the Northern District of California on its website.[5] Further, upon information and belief, Redpine has transacted business in the Northern District of California and has committed acts of direct infringement in the Northern District of California.

INTRADISTRICT ASSIGNMENT

9. Pursuant to Civil L.R. 3-2(c), this case is appropriate for assignment on a district-wide basis because this is an Intellectual Property Action.

TECHNOLOGY OVERVIEW

10. Integrated circuits have become ubiquitous in today's world and continue to become smaller, more powerful, and more complex. Modern integrated circuits, such as processors, systems on a chip ("SoCs"), digital memory, application-specific integrated circuits ("ASICs"), and field-programmable gate arrays ("FPGAs"), are used in virtually all of today's electronic devices.

---

[3] *See* note 1, *supra*.
[4] *See* CALIFORNIA SECRETARY OF STATE WEBPAGE, California Corporate Number: C2012127, Statement of Information FF18353, Filed Aug. 8, 2016, available at https://businesssearch.sos.ca.gov/ (last accessed January 31, 2018)
[5] *See* note 1, *supra* (Redpine office located at "2107 North First Street, Suite 540, San Jose, CA, 95131")

11. Integrated circuits are often manufactured in batch processes intended to make all integrated circuit chips identical, thereby lowering manufacturing costs and improving quality. However, it is useful to be able to distinguish each individual integrated circuit from all others, for example, to track its source of manufacture, or to identify a system employing the integrated circuit, which are both useful strategies for avoiding counterfeiting.

12. While it takes incredible ingenuity to design advanced integrated circuits, and the electronic devices that run by them, such circuitry is nevertheless susceptible to counterfeit.

13. In general, a counterfeit electronic part is any unlawful or unauthorized reproduction, substitution, or alteration that has been knowingly mismarked, misidentified, or otherwise misrepresented to be an authentic, unmodified electronic part from the original manufacturer, or a source with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer. Unlawful or unauthorized substitution may include used electronic parts represented as new, or the false identification of grade, serial number, lot number, date code, or performance characteristics.[6]

14. Counterfeit electronic parts cost American companies billions of dollars a year.[7] But economic risk is not the only risk of counterfeit parts; rather, counterfeit parts create significant health and safety risks as well due to their ubiquity in electronic devices of all sorts, including health and safety equipment.

15. As a result of the risks posed by counterfeit electronic parts, the U.S. government has enacted many laws to eliminate the introduction of counterfeit parts into the stream of commerce—especially where government contracts are concerned. For example, in 2012 the U.S. Government enacted laws requiring regulations for contractor responsibilities for detection and avoidance of the use of counterfeit electronic parts.[8]

---

[6] *See*, *e.g.*, U.S. Defense Federal Acquisition Regulation 202.101; SAE Int'l AS5553A and AS6081A

[7] *See*, *e.g.*, The 'Ticking Time Bomb' of Counterfeit Electronic Parts, available at http://www.industryweek.com/procurement/ticking-time-bomb-counterfeit-electronic-parts (last accessed January 31, 2018).

[8] *See* 48 CFR 252.246-7007 "Contractor Counterfeit Electronic Part Detection and Avoidance System" available at https://www.gpo.gov/fdsys/pkg/CFR-2014-title48-vol3/pdf/CFR-2014-title48-vol3-sec252-246-7007.pdf (last accessed January 31, 2018).

16. Many technological solutions for preventing and detecting counterfeit parts have been developed, including, for example, integrating RFID tags into electronic parts, creating hardware "fingerprints," "watermarking" electronic parts, and others. Many of these technologies are referred to as "intrinsic security" measures because they are built into the electronic parts.

17. One intrinsic security technique is based on Physical Unclonable Functions (PUFs). PUFs allow an electronic part to be uniquely identified based on the unique properties of its microstructure, which depends on random physical factors introduced during manufacturing. PUFs are extremely useful for electronic devices because they are easy to produce, often requiring no special manufacturing steps, but very difficult if not impossible to duplicate, even if the exact manufacturing process that produced the PUF is known. PUFs are frequently implemented in electronic parts with high security requirements.

OVERVIEW OF U.S. PATENT NO. RE40,188

18. U.S. Patent Application No. 09/251,692 ('692 Application) was filed on February 17, 1999 and subsequently issued as U.S. Patent No. 6,161,213 ('213 Patent), entitled "System and Method for Providing Integrated Circuit with a Unique Identification," on December 12, 2000.

19. On December 12, 2002, the assignee of the '213 Patent filed U.S. Patent Reissue Application 10/318,583 ('583 Application), entitled "System and Method for Providing Integrated Circuit with a Unique Identification," based on the '213 Patent. The '583 Application was subsequently reissued as RE40,188 ('188 Patent) on March 25, 2008. The '188 Patent includes 164 claims total, of which 10 are independent claims.

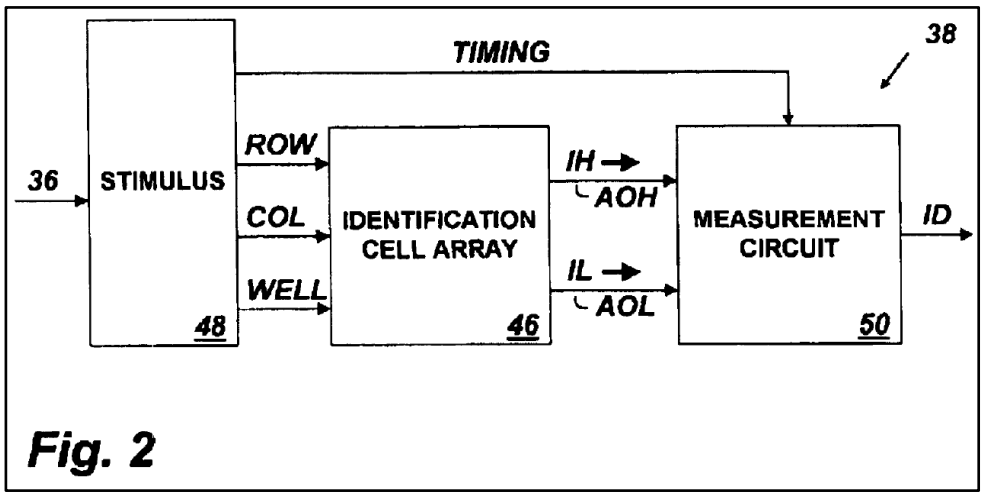
20. The '188 Patent recognizes that while many methods exist for uniquely identifying an electronic part, those existing methods require special steps during the manufacturing process that add cost and time to the manufacturing process. To solve this problem, the '188 Patent teaches a novel method for reliably and easily identifying and authenticating individual integrated circuits that does not require any additional manufacturing steps or equipment. Ex. 1 ['188 Patent] at 2:36-44.

21. In particular, the '188 Patent teaches a method of producing integrated circuit identification (ICID) circuits, which produces a unique identification number or record (ID) for each chip in which the ICID is included, even though the ICID circuit is fabricated on all chips using identical masks. Ex. 1 ['188 Patent] at 2:46-50.

22. Embodiments of ICID circuits include a set of cells that produce an output ID based on measurements of outputs of those cells, and the outputs of those cells are functions of random parametric variations that naturally occur when fabricating the ICID circuit. Ex. 1 ['188 Patent] at 2:50-54. Embodiments of ICID circuits include arrays of cells and a circuit for selecting each cell of the array, measuring that cell's output, and producing the chip ID based on the pattern of measured outputs of all cells in the array. Ex. 1 ['188 Patent] at 2:57-62. The chip ID is thus a unique "fingerprint" for the chip. Ex. 1 ['188 Patent] at 3:1-4.

23. The '188 Patent teaches that when the number of ICID circuit cells is sufficiently large, then millions of chips can be provided with a unique identifying ID without having to customize each chip using costly and time-consuming additional processing steps during or after chip fabrication. Ex. 1 ['188 Patent] at 2:54-56; 3:13:17.

24. Figure 2 of the '188 Patent depicts a functional block diagram of an embodiment of an ICID device:



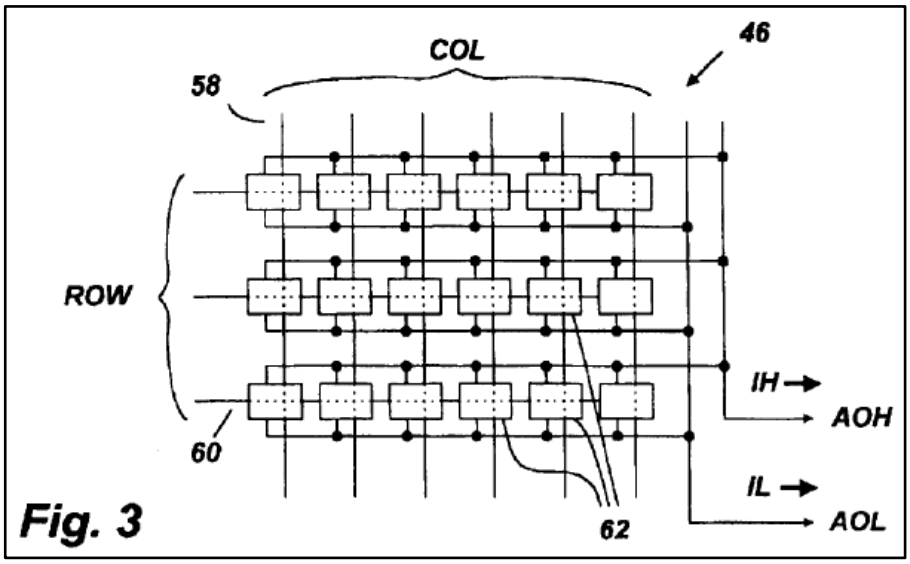
Ex. 1 ['188 Patent] at Fig. 2.

25. Referring to Figure 2, the specification explains: "ICID circuit **38** includes an array **46** of rows and columns of cells. Each cell of array **46**, when selected produces a pair of

output currents IH and IL on array output lines AOH and AOL. The IH and IL currents are produced by similar transistors within the selected cell and are nearly equal. But due to differences in the transistors resulting from random parametric variations, the IH and IL currents will not exactly match. The difference between the IH and IL currents will vary from cell to cell. A stimulus circuit **48** responds to the control input **36** by supplying row select data (ROW) and a column select data (COL) to array **46** to individually select and stimulate each of its cells in turn. As it selects a cell, stimulus circuit **48** sends timing signals (TIMING) to a measurement circuit **50** telling it when to measure a difference between the currents IH and IL of the selected cell." Ex. 1 ['188 Patent] at 5:22-37.

26. The specification further explains that: "[m]easurement circuit **50**, sequenced by TIMING strobes from stimulus circuit **48**, measures the current difference between IH and IL for each cell and … produces a serial output ID having a value that is base[d] on the particular pattern of measured current differences for all cells of array **46**." Ex. 1 ['188 Patent] at 5:51-56.

27. Figure 3 of the '188 Patent depicts more detail regarding an embodiment of an identification cell array:



Ex. 1 ['188 Patent] at Fig. 3.

28. Notably, Figure 3 is merely one example of a structure of such an array. As the specification teaches: "the number of cells 62 that should be included in array **46** is largely a function of the number of ICs to be uniquely identified." Ex. 1 ['188 Patent] at 12:13-20.

29. The cells themselves may be formed in some embodiments from transistors, such as shown in basic form with respect to Figure 6:

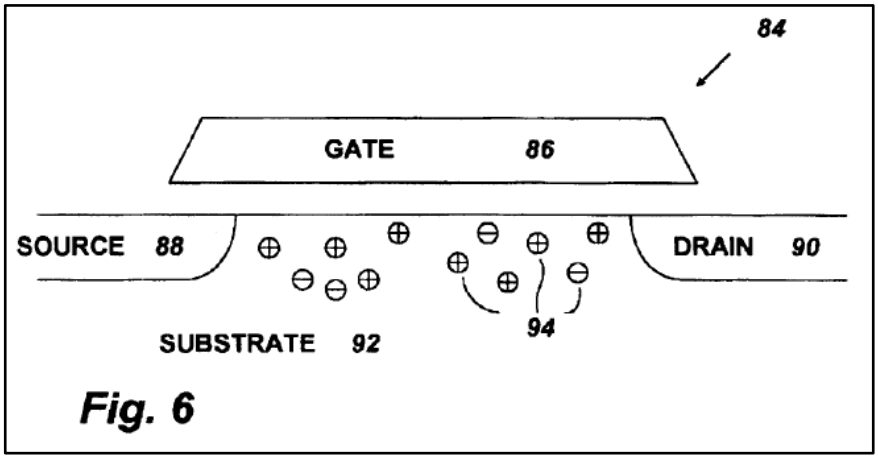


Fig. 6

Ex. 1 ['188 Patent] at Fig. 6.

30. As further described in the specification: ICID **38** (Figure 2) "may be adapted to provide an output ID that not only uniquely identifies an IC in which it is installed but also includes a 'type code' indicating aspects of the IC that is has in common with other ICs sharing the same photomask, such as its type, source of manufacture, etc. Thus, an output ID of ICID 38 would include one field having a value that is unique to the IC in which it is installed and another field having a value that is common to all similar ICs." Ex. 1 ['188 Patent] at 5:62-64.

31. Further, the specification explains that the output ID can be stored in a database and used to later identify the specific part. Ex. 1 ['188 Patent] at 14:55-15:8. Similarly, if a part is tested and found not to be in the database, then it may be determined to be a counterfeit. Ex. 1 ['188 Patent] at 15:12-13.

32. Additionally, an output ID "may be stored on the chip itself as a sequence of values in an on-chip Random Access Memory (RAM) which may be non-nonvolatile. The RAM may be part of a microprocessor on-board cache, and available to software executed by that

microprocessor. This arrangement allows fast access to the ID during use ….” Ex. 1 [‘188 Patent] at 16:5-10.

33. The innovativeness of the solutions taught in the ‘188 Patent are clear from the industry’s myriad of references to it and its predecessor patent.[9] By way of example, the ‘213 Patent (predecessor to ‘188 Patent) has been cited in patent documents all over the world more than 260 times by the likes of Advanced Micro Devices[10], Analog Devices Inc.[11], Fujitsu[12], Hewlett Packard[13], Hitachi[14], IBM[15], Intel[16], Intrinsic ID[17], MIT[18], National Semiconductor[19], Nokia[20], Panasonic[21], Philips[22], Samsung[23], STMicroelectronics[24], Synaptics[25], Texas Instruments[26], and Verayo[27]. And despite the ‘188 Patent issuing more than eight years after the ‘213 Patent, and almost a decade after the original filing date, it continues to be cited in contemporary patents and patent applications.[28]

---

[9] *See*, *e.g.*, Finding the Best Patents – Forward Citation Analysis Still Wins, available at http://www.ipwatchdog.com/2016/03/24/finding-best-patents-forward-citation-analysis-still-wins/id=67192/ (last accessed January 31, 2018) (“We’ve identified five primary factors for consideration in patent ranking (in order of weighting): Forward citations (45%) Age of patent from priority date (19%) Independent claim count (adjusted by number of means claims) (14%) Claim 1 word count (12%) Family size and international filings (10%) **We were surprised to discover that forward citations dominate the analysis. We evaluated millions of patents – and consistently forward citations were the biggest predictor of a higher value patent**.”) (emphasis added)

[10] *See*, *e.g.*, US6968303
[11] *See*, *e.g.*, US6480136
[12] *See*, *e.g.*, US6862725 and US7062346
[13] *See*, *e.g.*, US6960753 and US6889305
[14] *See*, *e.g.*, US6941536 and US7665049
[15] *See*, *e.g.*, US8214169 and US8619979
[16] *See*, *e.g.*, US7813507 and US7102358
[17] *See*, *e.g.*, US20030204743
[18] *See*, *e.g.*, US7681103 and US7757083
[19] *See*, *e.g.*, US7602666 and US7482657
[20] *See*, *e.g.*, US7356627
[21] *See*, *e.g.*, US7655483 and US8510608
[22] *See*, *e.g.*, WO/2004/017408 and WO/2004/105125
[23] *See*, *e.g.*, US6600686
[24] *See*, *e.g.*, US8745107 and US7334131
[25] *See*, *e.g.*, US8698594 and US9697411
[26] *See*, *e.g.*, US6952623
[27] *See*, *e.g.*, US8782396 and US8683210
[28] *See*, *e.g.*, US9506983 and US9568540

34. UPF is the owner and assignee of the patent-in-suit as recorded by the USPTO at Reel/Frame: 042956/0213.

COUNT I

(INFRINGEMENT OF U.S. PATENT NO. RE40,188 AGAINST REDPINE)

35. UPF restates and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

36. UPF is the owner by assignment of the '188 Patent. A true and correct copy of the '188 Patent is attached hereto as Exhibit 1.

37. On information and belief, Redpine makes, uses, sells, offers to sell, and/or imports the Wyzbee IoT Platform, WiSeMCU family of products and M2MCombo RS9113 family of products (collectively, the "Redpine Accused Products").

38. On information and belief, to the extent the preamble of claim 21 of the '188 Patent is limiting, the Redpine Accused Products comprise an apparatus in an integrated circuit (IC) for generating an identification number (ID) identifying the IC. For example, the Redpine Accused Products contain design security systems that bind the device's firmware to a specific device. Among these design security features are physically unclonable functions ("PUFs").

> The WyzBee platform is supported by the WyzBee IoT Cloud – a Redpine hosted cloud framework that offers flexible and customizable connectivity, analytics, and user interfaces. The RS9113 chipset integrates PUF-based hardware security block that provides for unique, individual device entities – ensuring that each IoT device can be individually authenticated and software delivered to it that cannot run on any other device.

Redpine Signals Launches WyzBee – World's First Comprehensive IoT Platform for Device Makers, (2015), http://www.redpinesignals.com/News_&_Events/PressReleases/Redpine_Signals_Launches_WyzBee_Worlds_First_Comprehensive_IoT_Platform_for_Device_Makers.php (last visited Jan 31, 2018).

> For networking and security, the chip integrates ThreadArch, a proprietary Redpine CPU with four threads. The ThreadArch subsystem comprises a trusted execution environment (TEE), which works with a set of integrated Suite-B crypto accelerators. The processor comes with a random-number generator and CRC functions, and a physically unclonable function (PUF) provides a unique device ID and key storage.

Redpine Scores IoT Triple Play, (2018), http://www.linleygroup.com/newsletters/newsletter_detail.php?num=5806 (last visited Jan 31, 2018).

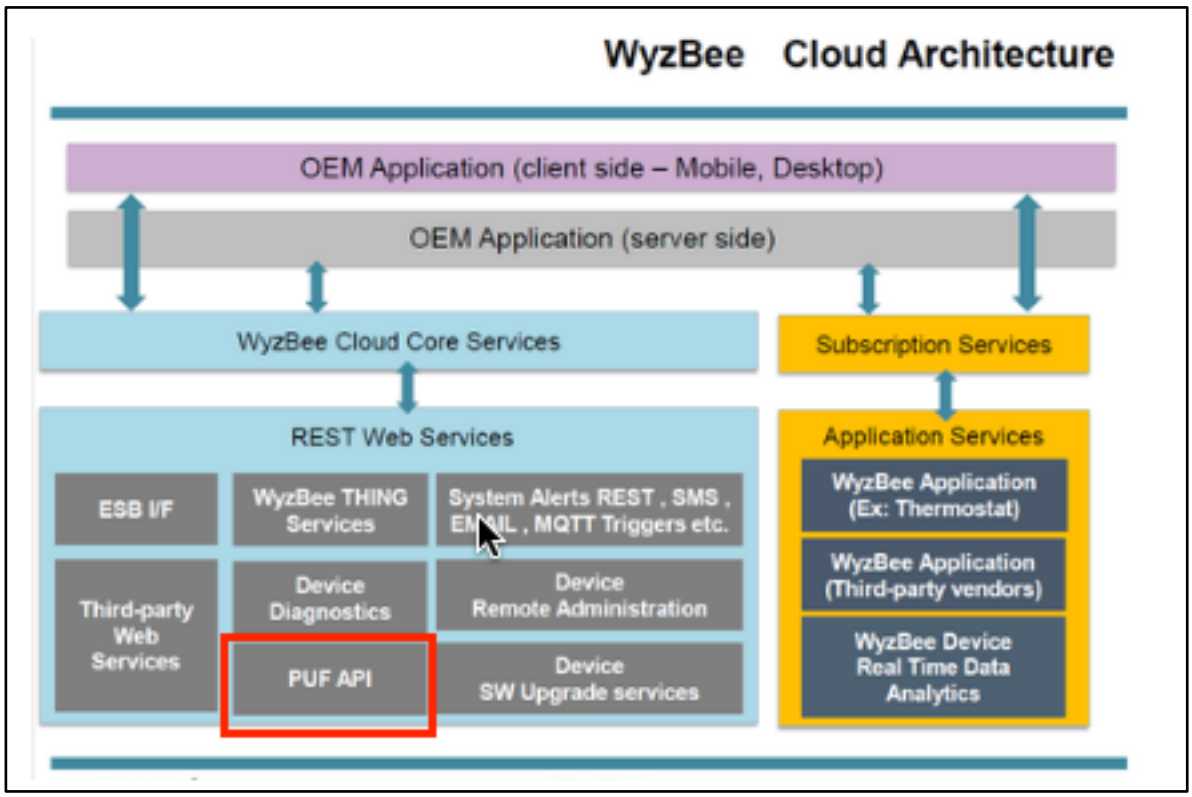
> Network nodes can communicate using CoAP, MQTT, email, and texts. Security is bolstered by a hardwa PUF: a physically unclonable function that establishes the device ID for binding purposes as well as supporting key generation for encryption and authentication.

Redpine Gives Makers a "Future-Proof" IoT Platform, Electronic Engineering Journal (2015). http://www.eejournal.com/2015/09/29/redpine-gives-makers-a-future-proof-iot-platform/ (last visited Jan 31, 2018).

> wireless space for the IoT market. Essentially, the chipset expertise is the key part of our play in the IoT space, without which, we will not be a credible sustainable player." The RS9113 chipset integrates PUF (Physical Unclonable Function)-based hardware security block, thereby providing unique, individual device entities, thus ensuring that each IoT device can be individually authenticated.

Redpine Signals: Introducing a Simpler Way to Create an IoT Device, SiliconIndia (2015), http://www.redpinesignals.com/News_&_Events/PressReleases/Siliconindia-cover-story-2015.pdf (last visited Jan 31, 2018).

> The platform's security features include not only SSL for the device-to-cloud connection, it includes the ability to bind the device's firmware to a specific device. Called physically unclonable function (PUF) security, the platform uses device-specific information to authenticate firmware before it will execute, preventing the cloning of devices that could intrude into a deployed network. With PUF, Mattela noted, firmware can only run on the specific device to which it has been bound.



IoT Dev Platform a One-Stop-Shop for Device Developers, EETimes, (2015), https://www.eetimes.com/document.asp?doc_id=1327466 (last visited Jan 31, 2018) (red box added).

39. On information and belief, the Redpine Accused Products comprise an identification circuit formed within the IC, the identification circuit outputting signals that are a substantial function of random parametric variations in the IC. For example, the Redpine Accused Products use a physically unclonable function that establishes the device ID for binding purposes, and this device ID is based on device-specific information. On information and belief, the "hardware PUF" used in the Redpine Accused Products establishes a device ID based on "device-specific information" that generates a response to a challenge based on unique device-specific physical properties of the IC containing the PUF, i.e. random parametric variations in the IC.

> Network nodes can communicate using CoAP, MQTT, email, and texts. Security is bolstered by a hardwa
> PUF: a physically unclonable function that establishes the device ID for binding purposes as well as supporting key generation for encryption and authentication.

Redpine Gives Makers a "Future-Proof" IoT Platform, Electronic Engineering Journal (2015), http://www.eejournal.com/2015/09/29/redpine-gives-makers-a-future-proof-iot-platform/ (last visited Jan 31, 2018).

> The platform's security features include not only SSL for the device-to-cloud connection, it includes the ability to bind the device's firmware to a specific device. Called physically unclonable function (PUF) security, the platform uses device-specific information to authenticate firmware before it will execute, preventing the cloning of devices that could intrude into a deployed network. With PUF, Mattela noted, firmware can only run on the specific device to which it has been bound.

IoT Dev Platform a One-Stop-Shop for Device Developers, EETimes, (2015), https://www.eetimes.com/document.asp?doc_id=1327466 (last visited Jan 31, 2018)

40. On information and belief, the Redpine Accused Products comprise a measurement circuit, the measurement circuit receiving the signals that are a substantial function of random parametric variations in the IC, wherein the measurement circuit generates the ID, wherein the ID is a substantial function of the random parametric variations. On information and belief, the Redpine Accused Products make use of a "PUF API" which supplies or causes to be supplied the challenge to the identification circuit, and uses the response to authenticate firmware, for binding purposes, and to generate keys for encryption and authentication, i.e. a measurement circuit that generates the ID substantially based on the specific physical properties of the IC containing the PUF.

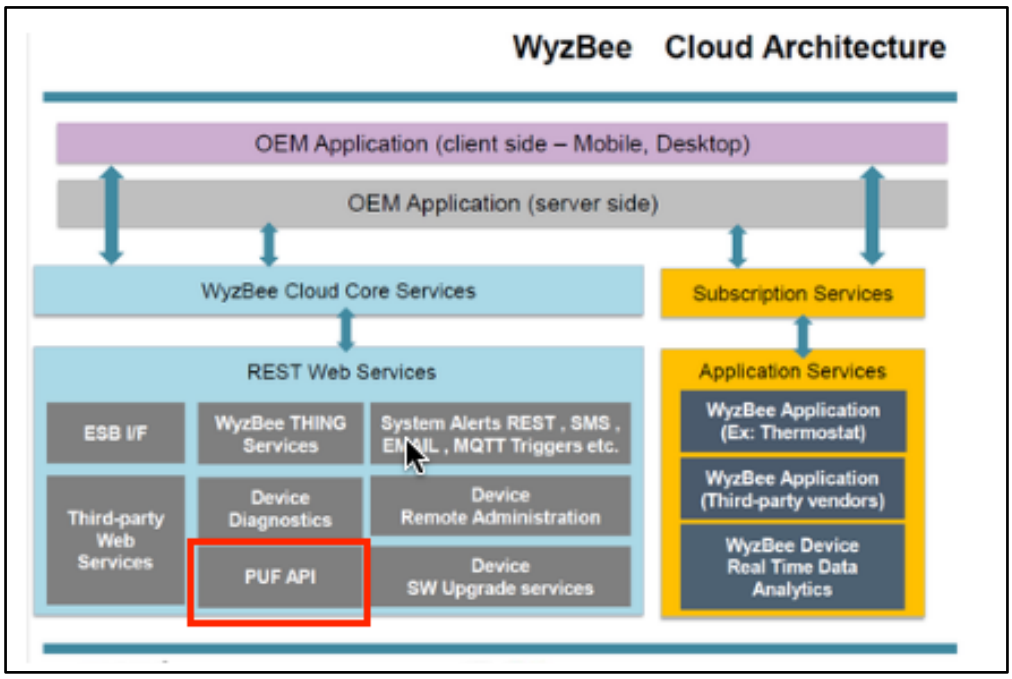
> wireless space for the IoT market. Essentially, the chipset expertise is the key part of our play in the IoT space, without which, we will not be a credible sustainable player." The RS9113 chipset integrates PUF (Physical Unclonable Function)-based hardware security block, thereby providing unique, individual device entities, thus ensuring that each IoT device can be individually authenticated.

Redpine Signals: Introducing a Simpler Way to Create an IoT Device, SiliconIndia (2015), http://www.redpinesignals.com/News_&_Events/PressReleases/Siliconindia-cover-story-2015.pdf (last visited Jan 31, 2018).

> Network nodes can communicate using CoAP, MQTT, email, and texts. Security is bolstered by a hardwa PUF: a physically unclonable function that establishes the device ID for binding purposes as well as supporting key generation for encryption and authentication.

Redpine Gives Makers a "Future-Proof" IoT Platform, Electronic Engineering Journal (2015), http://www.eejournal.com/2015/09/29/redpine-gives-makers-a-future-proof-iot-platform/ (last visited Jan 31, 2018).

> The platform's security features include not only SSL for the device-to-cloud connection, it includes the ability to bind the device's firmware to a specific device. Called physically unclonable function (PUF) security, the platform uses device-specific information to authenticate firmware before it will execute, preventing the cloning of devices that could intrude into a deployed network. With PUF, Mattela noted, firmware can only run on the specific device to which it has been bound.



IoT Dev Platform a One-Stop-Shop for Device Developers, EETimes, (2015), https://www.eetimes.com/document.asp?doc_id=1327466 (last visited Jan 31, 2018) (red box added).

41. By making, using, testing, offering for sale, selling, and/or importing integrated circuits and devices incorporating those integrated circuits, including but not limited to the Redpine Accused Products, Redpine has injured UPF Innovations and is liable to UPF Innovations for directly infringing one or more claims of the '188 Patent, including at least Claim 21, pursuant to 35 U.S.C. § 271(a).

42. Redpine has had knowledge of the '188 Patent since at least September 25, 2017, when it was given notice of the '188 Patent and of Redpine's need to obtain a patent license from UPF. Redpine has also had knowledge of the '188 Patent since the date of service of this Complaint or shortly thereafter, and on information and belief, Redpine knew of the '188 Patent and knew of its infringement, including by way of this lawsuit.

43. On information and belief, Redpine intended to induce patent infringement by third-party customers and users of the Redpine Accused Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Redpine specifically intended and was aware that the normal and

customary use of the accused products would infringe the '188 Patent. Redpine performed the acts that constitute induced infringement, and would induce actual infringement, with the knowledge of the '188 Patent and with the knowledge that the induced acts would constitute infringement. For example, Redpine provides the Redpine Accused Products, which are capable of operating in a manner that infringes one or more claims of the '188 Patent, including at least claim 21, and Redpine further provides advertising, documentation and training materials that cause customers of the Redpine Accused Products to utilize the products and services in a manner that directly infringes one or more claims of the '188 Patent. By advertising to and providing instruction and training to customers on how to use the Redpine Accused Products, Redpine specifically intended to induce infringement of the '188 Patent, including at least claim 21. On information and belief, Redpine engaged in such inducement to promote the sales of the Redpine Accused Products and to actively induce its customers to infringe the '188 Patent. Accordingly, Redpine has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '188 Patent, knowing that such use constitutes infringement of the '188 Patent.

44. As a result of Redpine's infringement of the '188 Patent, UPF has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Redpine's infringement, but in no event less than a reasonable royalty for the use made of the invention by Redpine together with interest and costs as fixed by the Court.

45. Upon information and belief, Redpine's infringing activities have continued and are continuing with knowledge of the '188 Patent, and with knowledge of their infringement of the '188 Patent. These infringing activities are, at a minimum, done with reckless disregard and/or willful blindness of UPF's rights under the '188 Patent. Redpine's acts of infringement have therefore been intentional, deliberate, and willful.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff UPF respectfully requests that this Court enter:

(a) A judgment in favor of Plaintiff UPF that Redpine has infringed the '188 Patent, either literally and/or under the doctrine of equivalents;

(b) An award of damages resulting from Redpine's acts of infringement in accordance with 35 U.S.C. § 284;

(c) A judgment and order requiring Redpine to provide accountings and to pay supplemental damages to UPF, including, without limitation, prejudgment and post-judgment interest; and

(d) A finding of willful infringement by Redpine and an award to UPF of enhanced damages pursuant to 35 U.S.C. § 284;

(e) Any and all other relief to which UPF may show itself to be entitled.

JURY TRIAL DEMANDED

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

Dated: February 7, 2018

Respectfully Submitted,

/s/ *Bradford Black*
Bradford J. Black

BRADFORD J. BLACK (SBN 252031)
bblack@bradfordblack.com
BRADFORD BLACK P.C.
4 Embarcadero Ctr., Suite 1400
San Francisco, CA 94111
Telephone: (415) 813-6211
Facsimile: (415) 813-6222
Attorneys for Plaintiff
UPF INNOVATIONS, LLC

Of Counsel:
DAVID C. RADULESCU (*pro hac vice to be submitted*)
david@radip.com
TIGRAN VARDANIAN (*pro hac vice to be submitted*)
tigran@radip.com
DANIEL KESACK (*pro hac vice to be submitted*)
dan@radip.com
RADULESCU LLP
The Empire State Building
350 Fifth Avenue, Suite 6910
New York, NY 10118
Telephone: (646) 502-5950
Facsimile: (646) 502-5959