UNITED STATES DISTRICT COURT
DISTRICT OF DELAWARE

BLUE SPIKE, LLC, *Plaintiff*, v. ROKU, INC., *Defendant*.	§ § § § § § § § § § § § § §	C.A. No. 17-928 (LPS) JURY TRIAL DEMANDED

AMENDED COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Blue Spike, LLC files this amended complaint against Defendant Roku, Inc. (“Roku” or “Defendant”), alleging five (5) counts of infringement of the following Patents-in-Suit, separated for convenience into two groups: Blue Spike’s Secure Server Patents; and Blue Spike’s Trusted Transaction Patents:

Blue Spike’s Secure Server Patents:

1. U.S. Patent No. 7,475,246, titled “Secure Personal Content Server” (the ’246 Patent);

2. U.S. Patent No. 8,171,561, titled "Secure Personal Content Server" (the '561 Patent);

3. U.S. Patent No. 8,739,295, titled "Secure Personal Content Server" (the '295 Patent, and collectively with U.S. Patent Nos. 7,475,246 and 8,171,561, the "Secure Server Patents");

Blue Spike's Trusted Transactions Patents:

4. U.S. Patent No. 7,159,116, titled "Systems, Methods and Devices for Trusted Transactions" (the '116 Patent); and

5. U.S. Patent No. 8,538,011, titled "Systems, Methods and Devices for Trusted Transactions" (the '011 Patent, and collectively with U.S. Patent No. 7,159,116, the "Trusted Transactions Patents").

NATURE OF THE SUIT

1. This is a claim for patent infringement arising under the patent laws of the United States, Title 35 of the United States Code.

PARTIES

2. Plaintiff Blue Spike, LLC is a Texas limited liability company and has its headquarters and principal place of business at 1820 Shiloh Road, Suite 1201-C, Tyler, Texas 75703. Blue Spike, LLC is the assignee of the Patents-in-Suit, and has ownership of all substantial rights in the Patents-in-Suit, including the rights to grant sublicenses, to exclude others from using it, and to sue and obtain damages and other relief for past and future acts of patent infringement.

3. On information and belief, Roku, Inc. is a company organized and existing under the laws of Delaware, with a principal place of business at 12980 Saratoga Ave., Ste. D,

Saratoga, California 95070. Roku, Inc. may be served through its registered agent, Registered Agents, LTD., 1013 Centre Rd. Ste. 403-A, Wilmington, DE 19805.

JURISDICTION AND VENUE

4. This lawsuit is a civil action for patent infringement arising under the patent laws of the United States, 35 U.S.C. § 101 *et seq.* The Court has subject-matter jurisdiction pursuant to 28 U.S.C. §§ 1331, 1332, 1338(a), and 1367.

5. The Court has personal jurisdiction over Defendant for at least five reasons: (1) Defendant is a company organized and existing under the laws of Delaware; (2) Defendant has committed acts of patent infringement and contributed to and induced acts of patent infringement by others in this District; (3) Defendant regularly does business or solicits business in this District; (4) Defendant engages in other persistent courses of conduct and derives substantial revenue from products and/or services provided to individuals in this District; and (5) Defendant has purposefully established substantial, systematic, and continuous contacts with this District and should reasonably expect to be haled into court here.

6. Defendant operates a website that solicits sales of the Accused Products by consumers in this District and Delaware (*see* Exhibits A & B); has partnered with numerous resellers and distributors to sell and offer for sale the Accused Products to consumers in this District and in Delaware, both online and in stores (*see*, *e.g.*, Exhibits C & D), offers support service to customers in this District and Delaware (*see* Exhibit E), and sells its products through retailers throughout Delaware (*see* Exhibit F). Given these extensive contacts, the Court's exercise of jurisdiction over Defendant will not offend traditional notions of fair play and substantial justice.

7. Venue is proper in this judicial district under 28 U.S.C. §§ 1391(b)-(c) and 1400(b) because Defendant is incorporated in this state. *See*, 28 U.S.C § 1400 (b); *TC Heartland LLC v. Kraft Foods Group Brands LLC*, 137 S. Ct. 1514, 1521 (2017).

PROCEDURAL BACKGROUND

8. Blue Spike first filed suit against Roku for infringement of the same Patents-in-Suit in the Eastern District of Texas on February 17, 2017. *See* Case 6:17-cv-0100, Dkt. 1. In May of 2017, Blue Spike filed an amended complaint in the same district. *See* Case 6:17-cv-0100, Dkt. 13. Both cases provided Roku with more notice than what the Eastern District of Texas required. *See* Blue Spike's Original Complaint, Case 6:17-cv-0100, Dkt. 1, at ¶ 21 ("Although Blue Spike is not obligated to identify specific claims or claim elements in its complaint, it does so below for Defendant's benefit."); *Rmail Ltd. v. Right Signature, LLC*, 2:11-cv-300-JRG, 2012 WL 2595305, at *2 (E.D. Tex. July 5, 2012) ("Plaintiffs are not required to identify specific claims or claim elements at this stage of the litigation.").

9. Instead of filing an answer, Roku filed a Rule 12(b)(3) motion to dismiss (Case 6:17-cv-0100, Dkt. 14). In July of 2017, just post *TC Heartland,* the Court granted it "without prejudice to their [Blue Spike] refiling in a District in which venue is proper." *See* Case 6:17-cv-0100, Dkt. 17. Blue Spike then filed suit in this District where Roku agreed venue is proper. *See* Dkt. 1. Blue Spike's original complaint in this District provided Roku with sufficient notice of infringement. *Princeton Digital Image Corp. v. Ubisoft Ent. SA,* Case 13-cv-335-LPS-CJB, 2017 WL 6337188, at *2 (D. Del. Dec. 12, 2017) (noting the plaintiff's "complaint need not describe precisely how each element of the asserted claims are practiced") (internal marks omitted).

10. Although Roku had the benefit of reviewing Blue Spike's complaint and infringement theories well in advance as filed in the Eastern District of Texas, Roku declined to file a Rule 12(b)(6) motion in this case. Instead, Roku filed an Answer in August of 2017. *See* Dkt. 8 at 8. On January 24, 2018, Roku filed a Rule 12(c) Motion to Dismiss "for failure to state a claim upon which relief can be granted."

FACTUAL BACKGROUND

11. Protection of intellectual property is a prime concern for creators and publishers of digitized copies of copyrightable works, such as musical recordings, movies, video games, and computer software. Blue Spike founder Scott Moskowitz pioneered—and continues to invent—technology that makes such protection possible.

12. Blue Spike is a company focused on innovation with research and development. Blue Spike does not make a product that competes directly with Roku, but other companies have licensed Blue Spike's pioneering patents. Many of those companies are Roku's competitors that licensed Blue Spike's technology and avoided litigation.

13. Blue Spike is a practicing entity, just not in the same field as Roku. For instance, Blue Spike provides pre-release tracking technology for audio, like new music artists' singles, that may be sent to various radio stations for promotional purposes. This type of tracking helps an artist know whether a radio station improperly posts the song for sale rather than simply playing it as a "demo only." Blue Spike also has other product offerings at www.bluespike.com. Blue Spike objects to Roku's statement of Blue Spike as anything else. Derogatory attorney argument such as unfounded classifications as an "NPE" have no place in the United States District Court for the District of Delaware.

14. Moskowitz is a senior member of the Institute of Electrical and Electronics Engineers (IEEE), a member of the Association for Computing Machinery, and the International Society for Optics and Photonics (SPIE). As a senior member of the IEEE, Moskowitz has peer-reviewed numerous conference papers and has submitted his own publications.

15. Moskowitz is an inventor on more than 100 patents, including forensic watermarking, signal abstracts, data security, software watermarks, product license keys, deep packet inspection, license code for authorized software and bandwidth securitization.

16. The National Security Agency (NSA) even took interest in his work after he filed one of his early patent applications. The NSA marked the application "classified" under a "secrecy order" while it investigated his pioneering innovations and their impact on national security.

17. As an industry trailblazer, Moskowitz has been a public figure and an active author on technologies related to protecting and identifying software and multimedia content. A 1995 *New York Times* article—titled "TECHNOLOGY: DIGITAL COMMERCE; 2 plans for watermarks, which can bind proof of authorship to electronic works"—recognized Moskowitz's company as one of two leading software start-ups in this newly created field. *Forbes* also interviewed Moskowitz as an expert for "Cops Versus Robbers in Cyberspace," a September 9, 1996 article about the emergence of digital watermarking and rights-management technology. He has also testified before the Library of Congress regarding the Digital Millennium Copyright Act.

18. Moskowitz has spoken to the RSA Data Security Conference, the International Financial Cryptography Association, Digital Distribution of the Music Industry, and many other organizations about the business opportunities that digital watermarking creates. Moskowitz also authored *So This Is Convergence?*, the first book of its kind about secure digital-content management. This book has been downloaded over a million times online and has sold thousands of copies in Japan, where Shogakukan published it under the name *Denshi Skashi*, literally "electronic watermark." Moskowitz was asked to author the introduction to *Multimedia Security Technologies for Digital Rights Management*, a 2006 book explaining digital-rights management. Moskowitz authored a paper for the 2002 International Symposium on Information Technology, titled "What is Acceptable Quality in the Application of Digital Watermarking: Trade-offs of Security, Robustness and Quality." He also wrote an invited 2003 article titled "Bandwidth as Currency" for the *IEEE Journal*, among other publications.

19. Moskowitz and Blue Spike continue to invent technologies that protect intellectual property from unintended use or unauthorized copying.

THE ACCUSED PRODUCTS

20. Defendant makes, uses, offers for sale and/or imports into the U.S. products, systems, and/or services that infringe the Patents-in-Suit, including, but not limited to, its Roku, Roku Express, Roku Express+, Roku Premiere, Roku Premiere+, and Roku Ultra (collectively, the "Accused Products").

21. Defendant's Accused Products allow playback of streaming video services such as Netflix, Amazon, and HBO, as well as audio streaming services such as Pandora,

Rdio, Rhapsody, and Spotify. The Accused Products also receive and transmit sensitive information and authorize users to view and listen to secured content.

22. Defendant's Accused Products are therefore using methods, devices, and systems taught by the Patents-in-Suit.

23. Yet Defendant has not sought or obtained a license for any of Blue Spike's patented technologies. This creates a competitive disadvantage to other Companies, like Apple, IBM, Samsung, Dell, and Sony to name some large companies, who recognized the value and novelty Blue Spike's patents provides to society.

24. Each count of patent infringement contained herein is accompanied by a representative claim. *See*, *Atlas IP LLC v. P. Gas and Electric Co*., 15-CV-05469-EDL, 2016 WL 1719545, at *5 (N.D. Cal. Mar. 9, 2016) ("*Iqbal* and *Twombly* only require Plaintiff to state a plausible claim for relief, which can be satisfied by adequately pleading infringement of one claim.").

COUNT 1: INFRINGEMENT OF U.S. PATENT 7,475,246

25. Blue Spike incorporates by reference the allegations in the paragraphs above.

26. The '246 Patent is valid, enforceable, and was duly and legally issued by the United States Patent and Trademark Office.

27. Without a license or permission from Blue Spike, Defendant has infringed and continue to infringe on one or more claims of the '246 Patent—directly, contributorily, or by inducement—by importing, making, using, offering for sale, or selling products and devices that embody the patented invention, including, without limitation, one or more of the Accused Products, in violation of 35 U.S.C. § 271.

28. Defendant has been and now is directly infringing by, among other things, practicing all the steps of the ’246 Patent and/or directing, controlling, and obtaining benefits from its subsidiaries, partners, distributors, and retailers practicing all the steps of the ’246 Patent. Specifically, Defendant imports the Accused Products into the United States; offers for sale and sells the Accused Products via its own online store (*see* Exhibits A & B), has partnered with numerous resellers to offer for sale and sell the Accused Products in the United States (*see*, *e.g.*, Exhibits C & D), generates revenue from sales of the Accused Products to U.S. customers via such outlets (*see id.*), and has attended trade shows in the United States where it has demonstrated the Accused Products (*see*, *e.g.*, Exhibit G).

29. For instance, the Accused Products infringe claim 17 of the ’246 Patent which teaches

> A method for creating a secure environment for digital content for a consumer, comprising the following steps:
>
> sending a message indicating that a user is requesting a copy of a content data set;
>
> retrieving a copy of the requested content data set;
>
> embedding at least one robust open watermark into the copy of the requested content data set, said watermark indicating that the copy is authenticated;
>
> embedding a second watermark into the copy of the requested content data set, said second watermark being created based upon information transmitted by the requesting user;
>
> transmitting the watermarked content data set to the requesting consumer via an electronic network;
>
> receiving the transmitted watermarked content data set into a Local Content Server (LCS) of the user;
>
> extracting at least one watermark from the transmitted watermarked content data set;
>
> permitting use of the content data set if the LCS determines that use is authorized; and
>
> permitting use of the content data set at a predetermined quality level, said predetermined quality level

> having been set for legacy content if the LCS determines that use is not authorized.

Defendant's Accused Products allow playback, upon request and proper authorization, of secured content via Netflix, HBO Go, Pandora, Spotify and other streaming services (*method for creating a secure environment for digital content for a consumer*). *See* Exhibit A.

30. A Roku user uses an Accused Product to select a movie on Netflix, for example (*sending a message indicating that a user is requesting a copy of a content data set*) and Netflix retrieves the movie from its content servers (*retrieving a copy of the requested content data set*). *See* Exhibits H & J.

31. Netflix employs a digital rights management system called PlayReady. The PlayReady encoder encrypts the media content and embeds a PlayReady header including at least a license acquisition service URL into the copy of the requested content (*embedding at least one robust open watermark into the copy of the requested content data set, said watermark indicating that the copy is authenticated;*). The PlayReady client on the Roku device determines that the media content file is authenticated by examining the PlayReady header. *See* Exhibit K ("Netflix has selected Microsoft PlayReady technology"); Exhibit J ("[PlayReady] Adds a PlayReady header to the media file. The PlayReady header is a rights management header that enables a PlayReady client to decrypt and acquire a license for the file. … Attempts to play back the media file and finds the PlayReady header in the file. Because the file contains this header, the client determines that the file is encrypted and a license must be acquired to play back the file.").

32. The PlayReady encoder embeds another watermark (*i.e.*, Key ID(s) of a content key) into the copy of the requested content set. The content key is created based upon the information transmitted between the PlayReady license server and the Netflix subscriber (*embedding a second watermark into the copy of the requested content data set, said second watermark being created based upon information transmitted by the requesting user*). *See* Exhibit J ("[PlayReady] Encrypts the resulting media file by using a content key, which it shares with PlayReady license services. PlayReady uses AES-128 CTR encryption.").

33. The PlayReady encoder transmits the watermarked content data to the requested user over the Internet (*transmitting the watermarked content data set to the requesting consumer via an electronic network*). *See* Exhibit J ("The encoder packages the media file and sends it to a content distribution network for delivery to PlayReady clients. … The content distribution network sends the media file to a PlayReady client in response to a request from the client.").

34. The Accused Device receives the content from Netflix (*receiving the transmitted watermarked content data set into a Local Content Server (LCS) of the user*) and finds the PlayReady header in it (*extracting at least one watermark from the transmitted watermarked content data set*). *See* Exhibit J ("The client does the following: Attempts to play back the media file and finds the PlayReady header in the file. Because the file contains this header, the client determines that the file is encrypted and a license must be acquired to play back the file.")

35. The PlayReady license server authenticates the client on the Accused Device and issues a license back to the client. The device uses the policies specified in the license to

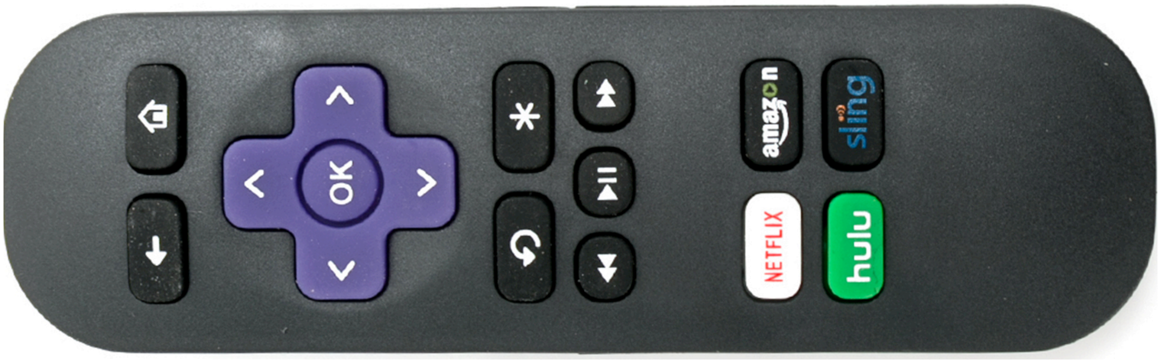
safeguard the media content against copying. If it determines that the user is authorized to receive 4K video, that quality is received, otherwise a lower resolution is received (*permitting use of the content data set if the LCS determines that use is authorized; and permitting use of the content data set at a predetermined quality level, said predetermined quality level having been set for legacy content if the LCS determines that use is not authorized*). *See* Exhibit H ("The PlayReady license server authenticates the client and issues a license back to the client. … As the client uses the license key to unencrypt the content, it plays back the content according to the policies specified in the license. Some of the common policies utilized are time based restrictions and output protections …"); Exhibit L.

36. Defendant has been and now is indirectly infringing by way of inducing infringement by others and/or contributing to the infringement by others of the '246 Patent in the State of Delaware, in this judicial district, and elsewhere in the United States, by, among other things, making, using, importing, offering for sale, and/or selling, without license or authority, products for use in systems that fall within the scope of one or more claims of the '246 Patent. Such products include, without limitation, one or more of the Accused Products. Such products have no substantial non-infringing uses and are for use in systems that infringe the '246 Patent. By making, using, importing offering for sale, and/or selling such products, Defendant injured Blue Spike and is thus liable to Blue Spike for infringement of the '246 Patent under 35 U.S.C. § 271. It is not necessary for Plaintiff to indicate specific customers directly infringing the Patents-in-Suit through the use of Defendant's Accused Products. *See In re Bill of Lading Transmission and Processing System Pat. Litig*., 681 F.3d 1323, 1336 (Fed. Cir. 2012). Defendant induces

and contributes to the infringement of its customers, who use the infringing functionality, and its partners and resellers, who offer for sale and sell the Accused Products (*see*, *e.g*., Exhibits C & D). Each of these groups of direct infringers is sufficient to justify an inference of direct infringement. *See Aeritas, LLC v. Alaska Air Group, Inc*., 893 F. Supp. 2d 680, 683 (D. Del. 2012) (noting the Federal Circuit Court in *In re Bill of Lading* "concluded that plaintiffs alleging indirect infringement need not name a specific customer to adequately plead the predicate direct infringement, so long as plaintiffs have pled facts sufficient to allow an inference that at least one direct infringer exists") (internal marks omitted). Those whom Defendant induces to infringe and/or to whose infringement Defendant contributes are the end users of the Accused Products.

37. Defendant had knowledge of the '246 Patent at least as early as the service of Blue Spike's complaint against Defendant in the Eastern District of Texas, filed on February 17, 2017 (Case No. 6:17-cv-00100, Dkt. No. 1). That complaint also notified Defendant that the Accused Products infringe the Patents-in-Suit, are especially made and adapted to infringe the Patents-in-Suit, cannot be used without infringing the technology claimed by the Patents-in-Suit, and have no alternative non-infringing uses. Thus, Defendant is liable for infringement of one or more claims of the '246 Patent by actively inducing infringement and/or is liable as contributory infringer of one or more claims of the '246 Patent under 35 U.S.C. § 271.

38. Defendant induces its customers to infringe at the very least by providing information on how to access infringing streaming content (*see, e.g.,* Ex. U) and by creating remote controls that encourage customers to use infringing services such as Netflix, Pandora, and Amazon.



(Figure 1: Showing buttons for specific infringing services.)

Defendant also provides customers other incentives to use the infringing services, such as through discounted offers. *See*, Ex. V.

39. The Accused Products have no substantial non-infringing uses and are for use in systems that infringe the Patents-in-Suit. *See, e.g., Lucent Techs., Inc. v. Gateway, Inc.*, 580 F.3d 1301 (Fed. Cir. (Cal.) 2009) (holding that the substantial non-infringing uses element of a contributory infringement claim applies to an infringing feature or component). An "infringing feature" of a product does not escape liability simply because the product as a whole has other non-infringing uses. *See id*. at 1321.

40. Defendant's acts of infringement of the '246 Patent have caused damage to Blue Spike, and Blue Spike is entitled to recover from Defendant the damages sustained as a result of Defendant's wrongful acts in an amount subject to proof at trial pursuant to 35 U.S.C. § 271. Defendant's infringement of Blue Spike's exclusive rights under the '246 Patent will continue to damage Blue Spike, causing it irreparable harm, for which there is no adequate remedy at law, warranting an injunction from the Court.

41. On information and belief, the infringement of the '246 Patent by Defendant has been willful and continues to be willful. Defendant had knowledge of the '246 Patent, including but not limited to at least one or more of the following:

a. The filing of Blue Spike's complaint against Defendant in the Eastern District of Texas on February 17, 2017 (Case No. 6:17-cv-00100, Dkt. No. 1).

b. In the course of its due diligence and freedom to operate analyses.

On information and belief, Defendant has had at least had constructive notice of the '246 Patent by operation of law. Plaintiff believes the evidence provided shows Defendant's willful infringement is egregious. Even so, Plaintiff is not required to prove egregiousness in its pleadings. "Even after Halo, broader allegations of willfulness, without a specific showing of egregiousness, are sufficient to withstand a motion to dismiss." *Shire ViroPharma Inc. v. CSL Behring LLC*, CV 17-414, 2018 WL 326406, at *3 (D. Del. Jan. 8, 2018) (denying a defendant's motion to dismiss and noting "Defendants' argument seems to conflate the standards for pleading willful infringement with the standards for proving willful infringement.").

COUNT 2:
INFRINGEMENT OF U.S. PATENT 8,171,561

42. Blue Spike incorporates by reference the allegations in the paragraphs above.

43. The '561 Patent is valid, enforceable, and was duly and legally issued by the United States Patent and Trademark Office.

44. Without a license or permission from Blue Spike, Defendant has infringed and continue to infringe on one or more claims of the '561 Patent—directly, contributorily, or by inducement—by importing, making, using, offering for sale, or selling products and devices that embody the patented invention, including, without limitation, one or more of the Accused Products, in violation of 35 U.S.C. § 271.

45. Defendant has been and now is directly infringing by, among other things, practicing all the steps of the ’561 Patent and/or directing, controlling, and obtaining benefits from its subsidiaries, partners, distributors, and retailers practicing all the steps of the ’561 Patent. Specifically, Defendant imports the Accused Products into the United States; offers for sale and sells the Accused Products via its own online store (*see* Exhibits A & B), has partnered with numerous resellers to offer for sale and sell the Accused Products in the United States (*see*, *e.g.*, Exhibits C & D), generates revenue from sales of the Accused Products to U.S. customers via such outlets (*see id.*), and has attended trade shows in the United States where it has demonstrated the Accused Products (*see*, *e.g.*, Exhibit G).

46. For instance, the Accused Products infringe claim 9 of the ’561 Patent which teaches

> A method for using a local content server (LCS), said LCS comprising an LCS communications port; an LCS storage unit for storing digital data; an LCS domain processor for processing digital data; and an LCS identification code uniquely associated with said LCS, said method comprising:
>
> said LCS storing in said LCS storage unit a plurality of rules for processing a data set;
>
> said LCS receiving via said communications port a first data set that includes data defining first content;
>
> said LCS using said domain processor to determine from inspection of said first data set for a watermark, a first data set status value of said first data set to be at least one of unsecure, secure, and legacy;
>
> said LCS using said first data set status value to determine which of a set of rules to apply to process said first data set prior to storage of a processed second data set resulting from processing of said first data set, in said LCS storage unit;
>
> said LCS determining, at least in part, from rights associated with a user identification associated with

> a prompt received by said LCS for said first content, a quality level at which to transmit said first content, wherein said quality level is one of at least unsecure, secure, and legacy; and
>
> wherein a quality level of legacy means that said first content does not include said watermark.

Defendant's Accused Products allow playback, upon request and proper authorization, of secured content via Netflix, HBO Go, Pandora, Spotify and other streaming services (*method for using a local content server (LCS)*). An Accused Device such as a Roku Ultra has Internet connectivity, memory, a processor for enforcing content rights, and a unique ID (*said LCS comprising an LCS communications port; an LCS storage unit for storing digital data; an LCS domain processor for processing digital data; and an LCS identification code uniquely associated with said LCS; said LCS storing in said LCS storage unit a plurality of rules for processing a data set*). *See* Exhibits B & M; Exhibit N ("The service confirms the code is correct and issues a token to the Roku device…").

47. Netflix, for example, employs a digital rights management system called PlayReady. PlayReady sets policies and rules for media content (*said LCS storing in said LCS storage unit a plurality of rules for processing a data set*). See Exhibit K ("Netflix has selected Microsoft PlayReady technology"); Exhibit J ("In PlayReady, policies support several types of usage rules, most commonly: time-based restrictions, which specify a time frame that a license is valid for; output-protection levels, which indicate whether playback is restricted to specific types of output ports on devices; and, allowable-export restrictions, which specify restrictions for moving or exporting content to a different content protection scheme.")

48. PlayReady secures content by encrypting media content and embeds a PlayReady header including at least a license acquisition service URL and one or more Key IDs

corresponding to the encryption key used for encrypting the media content. The encrypted file is streamed to the Roku device. The Roku device extracts the PlayReady header from the media content or media file, then it process the header to acquire a license from the license acquisition service and thereon the content decryption key for decrypting the content, hence determining the status of the content as secure (licensed) or unsecure content (*said LCS using said domain processor to determine from inspection of said first data set for a watermark, a first data set status value of said first data set to be at least one of unsecure, secure, and legacy*). *See* Exhibit J ("PlayReady secures content by encrypting data files. … The key is contained within a *license*. … PlayReady client finds and extracts the PlayReady rights management header from a media or media manifest file when it begins parsing the file. The client then processes the header data to acquire a license for and ultimately decrypt the content with the content key in the acquired license. In most cases, this includes sending the header to the appropriate license service, which in turn processes the header data, verifies that the license request is from a valid client (client authentication), and then issues a license to the client."). If the media content does not contain a PlayReady header (for example, if the content provider does not use digital rights management, such as PlayReady, the media content is determined to be legacy content.

49. For streaming secure content received from the PlayReady server, the Roku device must obey the output protection rule. The HDCP protocol determines the content rights and then if it does not match the protection criteria, a prompt is displayed. Quality level is determined to transmit content through output port (HDMI) (i.e., if the HDCP protection criteria is not matched, then the content is transmitted in low quality 720p or

1080p instead of 4K) (*said LCS using said first data set status value to determine which of a set of rules to apply to process said first data set prior to storage of a processed second data set resulting from processing of said first data set, in said LCS storage unit; said LCS determining, at least in part, from rights associated with a user identification associated with a prompt received by said LCS for said first content, a quality level at which to transmit said first content, wherein said quality level is one of at least unsecure, secure, and legacy; and wherein a quality level of legacy means that said first content does not include said watermark.*) *See* Exhibit H ("The PlayReady license server authenticates the client and issues a license back to the client. … As the client uses the license key to unencrypt the content, it plays back the content according to the policies specified in the license. Some of the common policies utilized are time based restrictions and output protections …"); Exhibit L ("If even one device does not support HDCP 2.2, then the 4K or 4K HDR movie or TV show can only be viewed in a lower resolution, such as 720p or 1080p.").

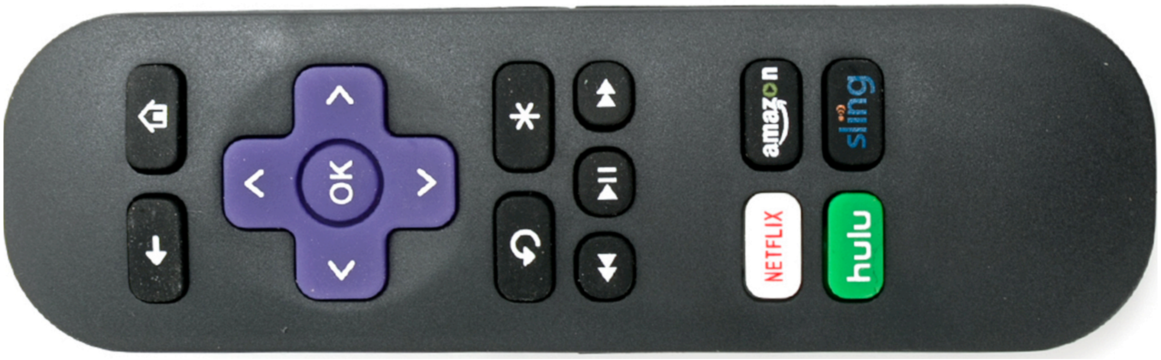
50. Defendant has been and now is indirectly infringing by way of inducing infringement by others and/or contributing to the infringement by others of the '561 Patent in the State of Delaware, in this judicial district, and elsewhere in the United States, by, among other things, making, using, importing, offering for sale, and/or selling, without license or authority, products for use in systems that fall within the scope of one or more claims of the '561 Patent. Such products include, without limitation, one or more of the Accused Products. Such products have no substantial non-infringing uses and are for use in systems that infringe the '561 Patent. By making, using, importing offering for sale, and/or selling such products, Defendant injured Blue Spike and is thus liable to Blue

Spike for infringement of the ’561 Patent under 35 U.S.C. § 271. It is not necessary for Plaintiff to indicate specific customers directly infringing the Patents-in-Suit through the use of Defendant’s Accused Products. *See In re Bill of Lading Transmission and Processing System Pat. Litig*., 681 F.3d 1323, 1336 (Fed. Cir. 2012). Even so, Defendant induces and contributes to the infringement of its customers. Defendant also induces and contributes to the infringement of its partners and resellers who use, test, and demonstrate the infringing functionality (*see*, *e.g*., Exhibits C & D). Each of these groups of direct infringers is sufficient to justify an inference of direct infringement. *See Aeritas, LLC v. Alaska Air Group, Inc*., 893 F. Supp. 2d 680, 683 (D. Del. 2012) (noting the Federal Circuit Court in *In re Bill of Lading* “concluded that plaintiffs alleging indirect infringement need not name a specific customer to adequately plead the predicate direct infringement, so long as plaintiffs have pled facts sufficient to allow an inference that at least one direct infringer exists”) (internal marks omitted). Those whom Defendant induces to infringe and/or to whose infringement Defendant contributes are the end users of the Accused Products.

51. Defendant had knowledge of the ’561 Patent at least as early as the service of Blue Spike’s complaint against Defendant in the Eastern District of Texas, filed on February 17, 2017 (Case No. 6:17-cv-00100, Dkt. No. 1). That complaint also notified Defendant that the Accused Products infringe the Patents-in-Suit, are especially made and adapted to infringe the Patents-in-Suit, cannot be used without infringing the technology claimed by the Patents-in-Suit, and have no alternative non-infringing uses. Thus, Defendant is liable for infringement of one or more claims of the ’561 Patent by actively inducing

infringement and/or is liable as contributory infringer of one or more claims of the ’561 Patent under 35 U.S.C. § 271.

52. Defendant induces its customers to infringe at the very least by providing information on how to access infringing streaming content (*see, e.g.,* Ex. U) and by creating remote controls that encourage customers to use infringing services such as Netflix, Pandora, and Amazon.



(Figure 1: Showing buttons for specific infringing services.)

Defendant also provides customers other incentives to use the infringing services, such as through discounted offers. *See*, Ex. V.

53. The Accused Products have no substantial non-infringing uses and are for use in systems that infringe the Patents-in-Suit. *See, e.g., Lucent Techs., Inc. v. Gateway, Inc.*, 580 F.3d 1301 (Fed. Cir. (Cal.) 2009) (holding that the substantial non-infringing uses element of a contributory infringement claim applies to an infringing feature or component). An “infringing feature” of a product does not escape liability simply because the product as a whole has other non-infringing uses. *See id*. at 1321.

54. Defendant’s acts of infringement of the ’561 Patent have caused damage to Blue Spike, and Blue Spike is entitled to recover from Defendant the damages sustained as a result of Defendant’s wrongful acts in an amount subject to proof at trial pursuant to

35 U.S.C. § 271. Defendant's infringement of Blue Spike's exclusive rights under the '561 Patent will continue to damage Blue Spike, causing it irreparable harm, for which there is no adequate remedy at law, warranting an injunction from the Court.

55. On information and belief, the infringement of the '561 Patent by Defendant has been willful and continues to be willful. Defendant had knowledge of the '561 Patent, including but not limited to at least one or more of the following:

a. The filing of Blue Spike's complaint against Defendant in the Eastern District of Texas on February 17, 2017 (Case No. 6:17-cv-00100, Dkt. No. 1).

b. In the course of its due diligence and freedom to operate analyses.

On information and belief, Defendant has had at least had constructive notice of the '561 Patent by operation of law. Plaintiff believes the evidence provided shows Defendant's willful infringement is egregious. Even so, Plaintiff is not required to prove egregiousness in its pleadings. "Even after Halo, broader allegations of willfulness, without a specific showing of egregiousness, are sufficient to withstand a motion to dismiss." *Shire ViroPharma Inc. v. CSL Behring LLC*, CV 17-414, 2018 WL 326406, at *3 (D. Del. Jan. 8, 2018) (denying a defendant's motion to dismiss and noting "Defendants' argument seems to conflate the standards for pleading willful infringement with the standards for proving willful infringement.").

COUNT 3:
INFRINGEMENT OF U.S. PATENT 8,739,295

56. Blue Spike incorporates by reference the allegations in the paragraphs above.

57. The ’295 Patent is valid, enforceable, and was duly and legally issued by the United States Patent and Trademark Office.

58. Without a license or permission from Blue Spike, Defendant has infringed and continue to infringe on one or more claims of the ’295 Patent—directly, contributorily, or by inducement—by importing, making, using, offering for sale, or selling products and devices that embody the patented invention, including, without limitation, one or more of the Accused Products, in violation of 35 U.S.C. § 271.

59. Defendant has been and now is directly infringing by, among other things, practicing all the steps of the ’295 Patent and/or directing, controlling, and obtaining benefits from its subsidiaries, partners, distributors, and retailers practicing all the steps of the ’295 Patent. Specifically, Defendant imports the Accused Products into the United States; offers for sale and sells the Accused Products via its own online store (*see* Exhibits A & B), has partnered with numerous resellers to offer for sale and sell the Accused Products in the United States (*see*, *e.g.*, Exhibits C & D), generates revenue from sales of the Accused Products to U.S. customers via such outlets (*see id.*), and has attended trade shows in the United States where it has demonstrated the Accused Products (*see*, *e.g.*, Exhibit G).

60. For instance, the Accused Products infringe claim 13 of the ’295 Patent which teaches

> A method for using a local content server system (LCS), said LCS comprising an LCS communications port; an LCS storage unit for storing digital data in non-transitory form; an LCS domain processor that imposes a plurality of rules and procedures for content being transferred between said LCS and devices outside said LCS, thereby defining a first LCS domain; and a programmable address module

> programmed with an LCS identification code uniquely associated with said LCS domain processor; comprising:
>
> storing, in said LCS storage unit, a plurality of rules for processing a data set;
>
> receiving, via said LCS communications port, a first data set that includes data defining first content;
>
> said LCS determining whether said first content belongs to a different LCS domain than said first LCS domain;
>
> said LCS excluding from said first LCS domain said first content when said LCS determines that said first content belongs to said different LCS domain;
>
> said LCS domain processor determining, from said first data set, a first data set status value of said first data set to be at least one of unsecure, secure, and legacy;
>
> said LCS determining, using said first data set status value, which of a set of rules to apply to process said first data set; and
>
> said LCS determining, at least in part from rights associated with an identification associated with a prompt received by said LCS for said first content, a quality level at which to transmit said first content, wherein said quality level is one of at least unsecure, secure, and legacy;
>
> said LCS transmitting said first content at the determined quality level.

Defendant's Accused Products allow playback, upon request and proper authorization, of secured content via Netflix, HBO Go, Pandora, Spotify and other streaming services (*method for using a local content server system (LCS)*). An Accused Device such as a Roku Ultra has Internet connectivity, memory, a processor for enforcing content rights, and a unique ID (*said LCS comprising an LCS communications port; an LCS storage unit for storing digital data in non-transitory form; an LCS domain processor that imposes a plurality of rules and procedures for content being transferred between said LCS and devices outside said LCS, thereby defining a first LCS domain; and a programmable address module programmed with an LCS identification code uniquely associated with* *said LCS domain processor*). *See* Exhibits B & M; Exhibit N ("The service confirms the code is correct and issues a token to the Roku device…").

61. Netflix, for example, employs a digital rights management system called PlayReady. PlayReady sets policies and rules for the playback of media content (*storing, in said LCS storage unit, a plurality of rules for processing a data set*). See Exhibit K ("Netflix has selected Microsoft PlayReady technology"); Exhibit J ("In PlayReady, policies support several types of usage rules, most commonly: time-based restrictions, which specify a time frame that a license is valid for; output-protection levels, which indicate whether playback is restricted to specific types of output ports on devices; and, allowable-export restrictions, which specify restrictions for moving or exporting content to a different content protection scheme.")

62. PlayReady secures content by encrypting media content and embeds a PlayReady header including at least a license acquisition service URL and one or more Key IDs corresponding to the encryption key used for encrypting the media content. The encrypted file is streamed to the Accused Device. The Accused Device receives the content from Netflix (*receiving, via said LCS communications port, a first data set that includes data defining first content*) and finds the PlayReady header in it to determine if the content can be played back (*said LCS determining whether said first content belongs to a different LCS domain than said first LCS domain; said LCS excluding from said first LCS domain said first content when said LCS determines that said first content belongs to said different LCS domain*). *See* Exhibit J ("The client does the following: Attempts to play back the media file and finds the PlayReady header in the file. Because the file

contains this header, the client determines that the file is encrypted and a license must be acquired to play back the file.")

63. In order to decrypt these data files, the Roku device extracts the header from the media content or media file, then it processes the header to acquire a license from the license acquisition service and thereon the content decryption key for decrypting the content, hence determining the status of the content as secure (licensed) or unsecure content (*said LCS domain processor determining, from said first data set, a first data set status value of said first data set to be at least one of unsecure, secure, and legacy*). *See* Exhibit J ("PlayReady secures content by encrypting data files. … The key is contained within a *license*. … PlayReady client finds and extracts the PlayReady rights management header from a media or media manifest file when it begins parsing the file. The client then processes the header data to acquire a license for and ultimately decrypt the content with the content key in the acquired license. In most cases, this includes sending the header to the appropriate license service, which in turn processes the header data, verifies that the license request is from a valid client (client authentication), and then issues a license to the client."). If the media content does not contain a PlayReady header (for example, if the content provider does not use digital rights management, such as PlayReady, the media content is determined to be legacy content.

64. For streaming secure content received from the PlayReady server, the Roku device must obey the output protection rule. The HDCP protocol determines the content rights and then if it does not match the protection criteria, a prompt is displayed. Quality level is determined to transmit content through output port (HDMI) (i.e., if the HDCP protection criteria is not matched, then the content is transmitted in low quality 720p or

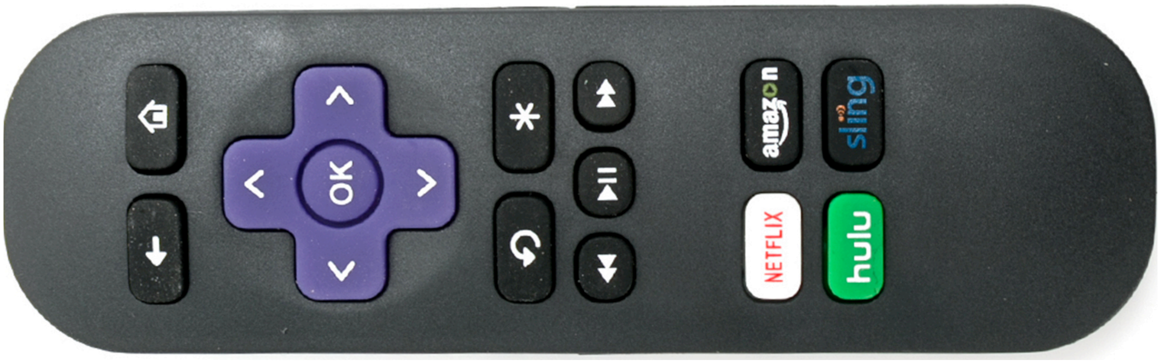
1080p instead of 4K) (*said LCS determining, using said first data set status value, which of a set of rules to apply to process said first data set; and said LCS determining, at least in part from rights associated with an identification associated with a prompt received by said LCS for said first content, a quality level at which to transmit said first content, wherein said quality level is one of at least unsecure, secure, and legacy; said LCS transmitting said first content at the determined quality level.*) *See* Exhibit H ("The PlayReady license server authenticates the client and issues a license back to the client. … As the client uses the license key to unencrypt the content, it plays back the content according to the policies specified in the license. Some of the common policies utilized are time based restrictions and output protections …"); Exhibit L ("If even one device does not support HDCP 2.2, then the 4K or 4K HDR movie or TV show can only be viewed in a lower resolution, such as 720p or 1080p.").

65. Defendant has been and now is indirectly infringing by way of inducing infringement by others and/or contributing to the infringement by others of the '295 Patent in the State of Delaware, in this judicial district, and elsewhere in the United States, by, among other things, making, using, importing, offering for sale, and/or selling, without license or authority, products for use in systems that fall within the scope of one or more claims of the '295 Patent. Such products include, without limitation, one or more of the Accused Products. Such products have no substantial non-infringing uses and are for use in systems that infringe the '295 Patent. By making, using, importing offering for sale, and/or selling such products, Defendant injured Blue Spike and is thus liable to Blue Spike for infringement of the '295 Patent under 35 U.S.C. § 271. It is not necessary for Plaintiff to indicate specific customers directly infringing the Patents-in-Suit through the

use of Defendant's Accused Products. *See In re Bill of Lading Transmission and Processing System Pat. Litig.*, 681 F.3d 1323, 1336 (Fed. Cir. 2012). Even so, Defendant induces and contributes to the infringement of its customers. Defendant also induces and contributes to the infringement of its partners and resellers who use, test, and demonstrate the infringing functionality (*see*, *e.g.*, Exhibits C & D). Each of these groups of direct infringers is sufficient to justify an inference of direct infringement. *See Aeritas, LLC v. Alaska Air Group, Inc.*, 893 F. Supp. 2d 680, 683 (D. Del. 2012) (noting the Federal Circuit Court in *In re Bill of Lading* "concluded that plaintiffs alleging indirect infringement need not name a specific customer to adequately plead the predicate direct infringement, so long as plaintiffs have pled facts sufficient to allow an inference that at least one direct infringer exists") (internal marks omitted). Those whom Defendant induces to infringe and/or to whose infringement Defendant contributes are the end users of the Accused Products.

66. Defendant had knowledge of the '295 Patent at least as early as the service of Blue Spike's complaint against Defendant in the Eastern District of Texas, filed on February 17, 2017 (Case No. 6:17-cv-00100, Dkt. No. 1). That complaint also notified Defendant that the Accused Products infringe the Patents-in-Suit, are especially made and adapted to infringe the Patents-in-Suit, cannot be used without infringing the technology claimed by the Patents-in-Suit, and have no alternative non-infringing uses. Thus, Defendant is liable for infringement of one or more claims of the '295 Patent by actively inducing infringement and/or is liable as contributory infringer of one or more claims of the '295 Patent under 35 U.S.C. § 271.

67. Defendant induces its customers to infringe at the very least by providing information on how to access infringing streaming content (*see, e.g.,* Ex. U) and by creating remote controls that encourage customers to use infringing services such as Netflix, Pandora, and Amazon.



(Figure 1: Showing buttons for specific infringing services.)

Defendant also provides customers other incentives to use the infringing services, such as through discounted offers. *See*, Ex. V.

68. The Accused Products have no substantial non-infringing uses and are for use in systems that infringe the Patents-in-Suit. *See, e.g., Lucent Techs., Inc. v. Gateway, Inc.*, 580 F.3d 1301 (Fed. Cir. (Cal.) 2009) (holding that the substantial non-infringing uses element of a contributory infringement claim applies to an infringing feature or component). An "infringing feature" of a product does not escape liability simply because the product as a whole has other non-infringing uses. *See id.* at 1321.

69. Defendant's acts of infringement of the '295 Patent have caused damage to Blue Spike, and Blue Spike is entitled to recover from Defendant the damages sustained as a result of Defendant's wrongful acts in an amount subject to proof at trial pursuant to 35 U.S.C. § 271. Defendant's infringement of Blue Spike's exclusive rights under the

’295 Patent will continue to damage Blue Spike, causing it irreparable harm, for which there is no adequate remedy at law, warranting an injunction from the Court.

70. On information and belief, the infringement of the ’295 Patent by Defendant has been willful and continues to be willful. Defendant had knowledge of the ’295 Patent, including but not limited to at least one or more of the following:

a. The filing of Blue Spike’s complaint against Defendant in the Eastern District of Texas on February 17, 2017 (Case No. 6:17-cv-00100, Dkt. No. 1).

b. In the course of its due diligence and freedom to operate analyses.

On information and belief, Defendant has had at least had constructive notice of the ’295 Patent by operation of law. Plaintiff believes the evidence provided shows Defendant’s willful infringement is egregious. Even so, Plaintiff is not required to prove egregiousness in its pleadings. “Even after Halo, broader allegations of willfulness, without a specific showing of egregiousness, are sufficient to withstand a motion to dismiss.” *Shire ViroPharma Inc. v. CSL Behring LLC*, CV 17-414, 2018 WL 326406, at *3 (D. Del. Jan. 8, 2018) (denying a defendant’s motion to dismiss and noting “Defendants' argument seems to conflate the standards for pleading willful infringement with the standards for proving willful infringement.”).

COUNT 4:
INFRINGEMENT OF U.S. PATENT 7,159,116

71. Blue Spike incorporates by reference the allegations in the paragraphs above.

72. The ’116 Patent is valid, enforceable, and was duly and legally issued by the United States Patent and Trademark Office.

73. Without a license or permission from Blue Spike, Defendant has infringed and continue to infringe on one or more claims of the ’116 Patent—directly, contributorily, or by inducement—by importing, making, using, offering for sale, or selling products and devices that embody the patented invention, including, without limitation, one or more of the Accused Products, in violation of 35 U.S.C. § 271.

74. Defendant has been and now is directly infringing by, among other things, practicing all the steps of the ’116 Patent and/or directing, controlling, and obtaining benefits from its subsidiaries, partners, distributors, and retailers practicing all the steps of the ’116 Patent. Specifically, Defendant imports the Accused Products into the United States; offers for sale and sells the Accused Products via its own online store (*see* Exhibits A & B), has partnered with numerous resellers to offer for sale and sell the Accused Products in the United States (*see*, *e.g.*, Exhibits C & D), generates revenue from sales of the Accused Products to U.S. customers via such outlets (*see id.*), and has attended trade shows in the United States where it has demonstrated the Accused Products (*see*, *e.g.*, Exhibit G).

75. The Accused Products infringe claims of the ’116 Patent, such as Claim 14 which teaches

> A device for conducting a trusted transaction between at least two parties who have agreed to transact, comprising:
>
> means for uniquely identifying information selected from the group consisting of a unique identification of one of the parties, a unique identification of the transaction, a unique identification of value added information to be transacted, a unique identification of a value adding component;
>
> a steganographic cipher for generating said unique identification information, wherein the

> steganographic cipher is governed by at least the following elements: a predetermined key, a predetermined message, and a predetermined carrier signal; and
>
> a means for verifying an agreement to transact between the parties.

Defendant's Accused Products allow playback of Netflix, Hulu+, HBO Go, Pandora, Spotify and other paid streaming services (*device[s] for conducting a trusted transaction between at least two parties who have agreed to transact*). *See* Exhibit A; Exhibit O ("Before you can start streaming media content, channels must be downloaded and installed on your Roku streaming device. To accomplish this, your Roku device must be linked to a Roku account. With a Roku account, not only can you add channels from the Roku Channel Store, but you can also manage your subscriptions and linked devices…").

76. An Accused Product such as a Roku Express has a unique device ID, and if the device is linked with an authentication service, a token is generated. The token is sent back to Roku devices and written into the channel registry. This token is used to uniquely identify the subscriber and the device on the server. In order to stream media on Roku devices, a Roku account must be set up which gives a unique identification of the subscriber (*means for uniquely identifying information selected from the group consisting of a unique identification of one of the parties…*) See Exhibit N ("All subsequent API requests use this token to identify the customer and device").

77. An Accused Product allows playback of streaming content via Netflix. Netflix employs a digital rights management system called PlayReady. Netflix through the PlayReady DRM uses Advanced Encryption Standard (AES) cipher in Galois/Counter Mode (GCM) for trusted transmission to devices. A client license request from a Roku device includes a content identifier and/or Key ID corresponding to the encryption key

used by Netflix to encrypt the content, which uniquely identifies the media file, and the public key. The licensing server receives the content identifier and/or Key ID, retrieves an appropriate license and encrypts the license using public key. The encrypted license is received by the Roku device where it is decrypted by Roku's AES cipher using a private key for generating a unique license to decrypt the media file for playback (*a steganographic cipher for generating said unique identification information ... governed by ... a predetermined key*). *See* Exhibit K ("Netflix has selected Microsoft PlayReady technology"); Exhibit H ("PlayReady secures content by encrypting data files. … In order to decrypt these data files, a digital key is required."); Exhibit I ("We evaluated available and applicable ciphers and decided to primarily use the Advanced Encryption Standard (AES) cipher … The AES-GCM cipher algorithm encrypts and authenticates the message simultaneously—as opposed to AES-CBC, which requires an additional pass over the data to generate keyed-hash message authentication code (HMAC)").

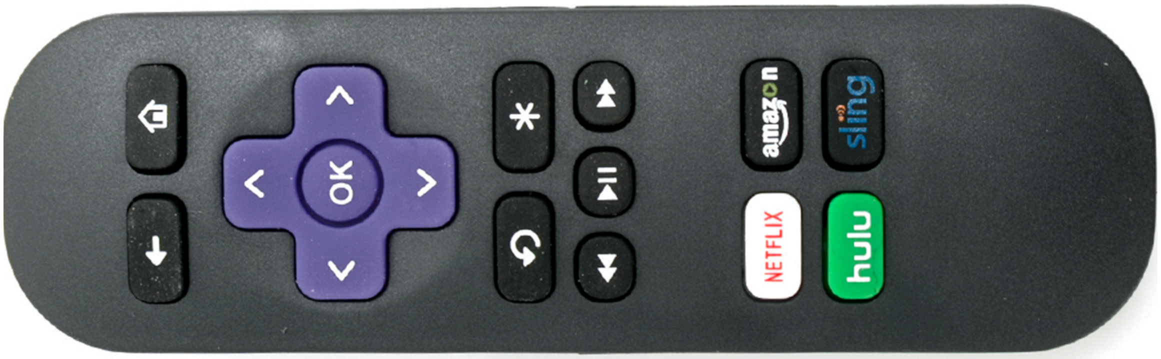
78. An Accused Device such as a Roku Express is associated with a Roku account to automatically sign a Roku customer to a partner channel application such as Netflix. The channel application determines if the Roku device is linked to the partner content service by locating a proprietary credential in the local registry (*a means for verifying an agreement to transact between the parties*). *See* Exhibit P ("The Channel Application securely passes the roku_pucid up to the Partner service and if there is a Partner customer account with the matching roku_pucid, the local registry is updated and the user is automatically signed in.").

79. Defendant has been and now is indirectly infringing by way of inducing infringement by others and/or contributing to the infringement by others of the '116

Patent in the State of Delaware, in this judicial district, and elsewhere in the United States, by, among other things, making, using, importing, offering for sale, and/or selling, without license or authority, products for use in systems that fall within the scope of one or more claims of the ’116 Patent. Such products include, without limitation, one or more of the Accused Products. Such products have no substantial non-infringing uses and are for use in systems that infringe the ’116 Patent. By making, using, importing offering for sale, and/or selling such products, Defendant injured Blue Spike and is thus liable to Blue Spike for infringement of the ’116 Patent under 35 U.S.C. § 271. It is not necessary for Plaintiff to indicate specific customers directly infringing the Patents-in-Suit through the use of Defendant’s Accused Products. *See In re Bill of Lading Transmission and Processing System Pat. Litig*., 681 F.3d 1323, 1336 (Fed. Cir. 2012) . Even so, Defendant induces and contributes to the infringement of its customers. Defendant also induces and contributes to the infringement of its partners and resellers who use, test, and demonstrate the infringing functionality (*see*, *e.g*., Exhibits C & D). Each of these groups of direct infringers is sufficient to justify an inference of direct infringement. *See Aeritas, LLC v. Alaska Air Group, Inc*., 893 F. Supp. 2d 680, 683 (D. Del. 2012) (noting the Federal Circuit Court in *In re Bill of Lading* “concluded that plaintiffs alleging indirect infringement need not name a specific customer to adequately plead the predicate direct infringement, so long as plaintiffs have pled facts sufficient to allow an inference that at least one direct infringer exists”) (internal marks omitted). Those whom Defendant induces to infringe and/or to whose infringement Defendant contributes are the end users of the Accused Products.

80. Defendant had knowledge of the ’116 Patent at least as early as the service of Blue Spike’s complaint against Defendant in the Eastern District of Texas, filed on February 17, 2017 (Case No. 6:17-cv-00100, Dkt. No. 1). That complaint also notified Defendant that the Accused Products infringe the Patents-in-Suit, are especially made and adapted to infringe the Patents-in-Suit, cannot be used without infringing the technology claimed by the Patents-in-Suit, and have no alternative non-infringing uses. Thus, Defendant is liable for infringement of one or more claims of the ’116 Patent by actively inducing infringement and/or is liable as contributory infringer of one or more claims of the ’116 Patent under 35 U.S.C. § 271.

81. Defendant induces its customers to infringe at the very least by providing information on how to access infringing streaming content (*see, e.g.,* Ex. U) and by creating remote controls that encourage customers to use infringing services such as Netflix, Pandora, and Amazon.



(Figure 1: Showing buttons for specific infringing services.)

Defendant also provides customers other incentives to use the infringing services, such as through discounted offers. *See*, Ex. V.

82. The Accused Products have no substantial non-infringing uses and are for use in systems that infringe the Patents-in-Suit. *See, e.g., Lucent Techs., Inc. v. Gateway, Inc.*,

580 F.3d 1301 (Fed. Cir. (Cal.) 2009) (holding that the substantial non-infringing uses element of a contributory infringement claim applies to an infringing feature or component). An "infringing feature" of a product does not escape liability simply because the product as a whole has other non-infringing uses. *See id*. at 1321.

83. Defendant's acts of infringement of the '116 Patent have caused damage to Blue Spike, and Blue Spike is entitled to recover from Defendant the damages sustained as a result of Defendant's wrongful acts in an amount subject to proof at trial pursuant to 35 U.S.C. § 271. Defendant's infringement of Blue Spike's exclusive rights under the '116 Patent will continue to damage Blue Spike, causing it irreparable harm, for which there is no adequate remedy at law, warranting an injunction from the Court.

84. On information and belief, the infringement of the '116 Patent by Defendant has been willful and continues to be willful. Defendant had knowledge of the '116 Patent, including but not limited to at least one or more of the following:

a. The filing of Blue Spike's complaint against Defendant in the Eastern District of Texas on February 17, 2017 (Case No. 6:17-cv-00100, Dkt. No. 1).

b. In the course of its due diligence and freedom to operate analyses.

On information and belief, Defendant has had at least had constructive notice of the '116 Patent by operation of law. Plaintiff believes the evidence provided shows Defendant's willful infringement is egregious. Even so, Plaintiff is not required to prove egregiousness in its pleadings. "Even after Halo, broader allegations of willfulness, without a specific showing of egregiousness, are sufficient to withstand a motion to dismiss." *Shire ViroPharma Inc. v. CSL Behring LLC*, CV 17-414, 2018 WL 326406, at

*3 (D. Del. Jan. 8, 2018) (denying a defendant's motion to dismiss and noting "Defendants' argument seems to conflate the standards for pleading willful infringement with the standards for proving willful infringement.").

COUNT 5:
INFRINGEMENT OF U.S. PATENT 8,538,011

85. Blue Spike incorporates by reference the allegations in the paragraphs above.

86. The '011 Patent is valid, enforceable, and was duly and legally issued by the United States Patent and Trademark Office.

87. Without a license or permission from Blue Spike, Defendant has infringed and continue to infringe on one or more claims of the '011 Patent—directly, contributorily, or by inducement—by importing, making, using, offering for sale, or selling products and devices that embody the patented invention, including, without limitation, one or more of the Accused Products, in violation of 35 U.S.C. § 271.

88. Defendant has been and now is directly infringing by, among other things, practicing all the steps of the '011 Patent and/or directing, controlling, and obtaining benefits from its subsidiaries, partners, distributors, and retailers practicing all the steps of the '011 Patent. Specifically, Defendant imports the Accused Products into the United States; offers for sale and sells the Accused Products via its own online store (*see* Exhibits A & B), has partnered with numerous resellers to offer for sale and sell the Accused Products in the United States (*see*, *e.g.*, Exhibits C & D), generates revenue from sales of the Accused Products to U.S. customers via such outlets (*see id.*), and has attended trade shows in the United States where it has demonstrated the Accused Products (*see*, *e.g.*, Exhibit G).

89. The Accused Products infringe claims of the ’011 Patent, such as Claim 36 which teaches

> A device for conducting trusted transactions between at least two parties, comprising:
> a steganographic cipher;
> a controller for receiving input data or outputting output data; and
> at least one input/output connection,
> wherein the device has a device identification code stored in the device;
> a steganographically ciphered software application;
> wherein said steganographically ciphered software application has been subject to a steganographic cipher for serialization;
> wherein said device is configured to steganographically cipher both value-added information and at least one value-added component associated with said value-added information;
> wherein said steganographic cipher receives said output data, steganographically ciphers said output data using a key, to define steganographically ciphered output data, and transmits said steganographically ciphered output data to said at least one input/output connection.

Defendant’s Accused Products allow playback of Netflix, Hulu+, HBO Go, Pandora, Spotify and other paid streaming services (*device[s] for conducting a trusted transaction between at least two parties who have agreed to transact*). *See* Exhibit A; Exhibit O (“Before you can start streaming media content, channels must be downloaded and installed on your Roku streaming device. To accomplish this, your Roku device must be linked to a Roku account. With a Roku account, not only can you add channels from the Roku Channel Store, but you can also manage your subscriptions and linked devices…”).

90. An Accused Product such as a Roku Express includes a processor in combination with an OS platform. Collectively the processor and the OS provide a feature of receiving

and streaming media contents (*a controller for receiving input data or outputting output data*). *See*, *e.g.*, Exhibit Q.

91. An Accused Product includes a Wi-Fi connection for connecting to the Internet and an HDMI port for connecting to a television or monitor (s input/output connections (*at least one input/output connection*). *See*, *e.g.*, Exhibits R & S.

92. An Accused Product such as a Roku Express has a unique device ID (*wherein the device has a device identification code stored in the device*). See Exhibit T ("channel providers and advertisers can collect information about your device (including unique identifiers)").

93. An Accused Product allows playback of streaming content via Netflix. Netflix employs a digital rights management system called PlayReady. Netflix through the PlayReady DRM uses Advanced Encryption Standard (AES) cipher in Galois/Counter Mode (GCM) for trusted transmission to devices. A client license request from a Roku device includes a content identifier and/or Key ID corresponding to the encryption key used by Netflix to encrypt the content (*a steganographic cipher;)*, which uniquely identifies the media file, and the public key. The licensing server receives the content identifier and/or Key ID, retrieves an appropriate license and encrypts the license using public key. The encrypted license is received by the Roku device where it is decrypted by Roku's AES cipher using a private key for generating a unique license to decrypt the media file for playback. Each PlayReady license acquisition operation has a unique session ID which introduces individualization or serialization of trusted transaction of media license (*a steganographically ciphered software application; wherein said steganographically ciphered software application has been subject to a steganographic*

cipher for serialization;). *See* Exhibit K ("Netflix has selected Microsoft PlayReady technology"); Exhibit H ("PlayReady secures content by encrypting data files. … In order to decrypt these data files, a digital key is required."); Exhibit I ("We evaluated available and applicable ciphers and decided to primarily use the Advanced Encryption Standard (AES) cipher … The AES-GCM cipher algorithm encrypts and authenticates the message simultaneously—as opposed to AES-CBC, which requires an additional pass over the data to generate keyed-hash message authentication code (HMAC)"); *see also* Exhibit U.

94. The Roku Express System includes a PlayReady digital rights management header which is used by PlayReady clients to acquire licenses and decrypt media file for playback. Each PlayReady header includes a standard set of metadata, which includes content identifiers and/or Key IDs (*wherein said device is configured to steganographically cipher both value-added information and at least one value-added component associated with said value-added information*). *See* Exhibit J ("The PlayReady header object is a placeholder to store PlayReady digital rights management header that enables PlayReady clients to acquire a license for and decrypt the content in a media file. It can also store an embedded license directly in a media file. The header is added to and subsequently stored in a media file or, for streaming content, a media manifest file when the file is packaged for distribution.").

95. An Accused Device, using the PlayReady DRM system, allows the client device to receive a license and decrypt it using the private key from the key pair. A license contains a content key (corresponding to the content identifier and/or Key ID embedded in the PlayReady header), which is a symmetric cryptographic key used to decrypt

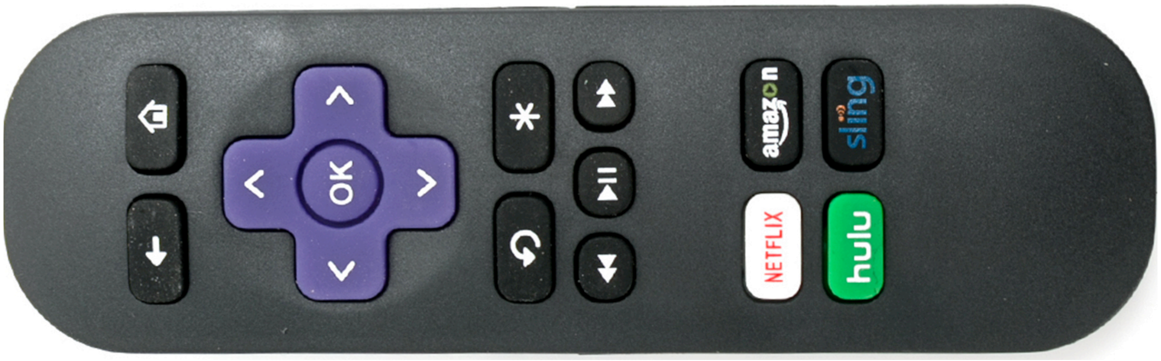
media files for further playback. (*wherein said steganographic cipher receives said output data, steganographically ciphers said output data using a key, to define steganographically ciphered output data, and transmits said steganographically ciphered output data to said at least one input/output connection*). *See* Exhibit J ("PlayReady media files are encrypted by AES encryption algorithm, so those can be moved, archived, copied, and distributed but their content cannot be consumed without a license. A license contains a content key, which is a symmetric cryptographic key that is used to decrypt a media file, and it specifies policies that define how and under what conditions a file's content may be used. … The client receives the license and decrypts it by using the private key from the key pair that is unique to the client device (device private key). The client then uses the license to securely decrypt and play back the media file in accordance with the policies specified in the license.").

96. Defendant has been and now is indirectly infringing by way of inducing infringement by others and/or contributing to the infringement by others of the '011 Patent in the State of Delaware, in this judicial district, and elsewhere in the United States, by, among other things, making, using, importing, offering for sale, and/or selling, without license or authority, products for use in systems that fall within the scope of one or more claims of the '011 Patent. Such products include, without limitation, one or more of the Accused Products. Such products have no substantial non-infringing uses and are for use in systems that infringe the '011 Patent. By making, using, importing offering for sale, and/or selling such products, Defendant injured Blue Spike and is thus liable to Blue Spike for infringement of the '011 Patent under 35 U.S.C. § 271. It is not necessary for Plaintiff to indicate specific customers directly infringing the Patents-in-Suit through the

use of Defendant's Accused Products. *See In re Bill of Lading Transmission and Processing System Pat. Litig.*, 681 F.3d 1323, 1336 (Fed. Cir. 2012). Even so, Defendant induces and contributes to the infringement of its customers. Defendant also induces and contributes to the infringement of its partners and resellers who use, test, and demonstrate the infringing functionality (*see*, *e.g.*, Exhibits C & D). Each of these groups of direct infringers is sufficient to justify an inference of direct infringement. *See Aeritas, LLC v. Alaska Air Group, Inc.*, 893 F. Supp. 2d 680, 683 (D. Del. 2012) (noting the Federal Circuit Court in *In re Bill of Lading* "concluded that plaintiffs alleging indirect infringement need not name a specific customer to adequately plead the predicate direct infringement, so long as plaintiffs have pled facts sufficient to allow an inference that at least one direct infringer exists") (internal marks omitted). Those whom Defendant induces to infringe and/or to whose infringement Defendant contributes are the end users of the Accused Products.

97. Defendant had knowledge of the '011 Patent at least as early as the service of Blue Spike's complaint against Defendant in the Eastern District of Texas, filed on February 17, 2017 (Case No. 6:17-cv-00100, Dkt. No. 1). That complaint also notified Defendant that the Accused Products infringe the Patents-in-Suit, are especially made and adapted to infringe the Patents-in-Suit, cannot be used without infringing the technology claimed by the Patents-in-Suit, and have no alternative non-infringing uses. Thus, Defendant is liable for infringement of one or more claims of the '011 Patent by actively inducing infringement and/or is liable as contributory infringer of one or more claims of the '011 Patent under 35 U.S.C. § 271.

98. Defendant induces its customers to infringe at the very least by providing information on how to access infringing streaming content (*see, e.g.,* Ex. U) and by creating remote controls that encourage customers to use infringing services such as Netflix, Pandora, and Amazon.



(Figure 1: Showing buttons for specific infringing services.)

Defendant also provides customers other incentives to use the infringing services, such as through discounted offers. *See*, Ex. V.

99. The Accused Products have no substantial non-infringing uses and are for use in systems that infringe the Patents-in-Suit. *See, e.g., Lucent Techs., Inc. v. Gateway, Inc.*, 580 F.3d 1301 (Fed. Cir. (Cal.) 2009) (holding that the substantial non-infringing uses element of a contributory infringement claim applies to an infringing feature or component). An "infringing feature" of a product does not escape liability simply because the product as a whole has other non-infringing uses. *See id.* at 1321.

100. Defendant's acts of infringement of the '011 Patent have caused damage to Blue Spike, and Blue Spike is entitled to recover from Defendant the damages sustained as a result of Defendant's wrongful acts in an amount subject to proof at trial pursuant to 35 U.S.C. § 271. Defendant's infringement of Blue Spike's exclusive rights under the

’011 Patent will continue to damage Blue Spike, causing it irreparable harm, for which there is no adequate remedy at law, warranting an injunction from the Court.

101. On information and belief, the infringement of the ’011 Patent by Defendant has been willful and continues to be willful. Defendant had knowledge of the ’011 Patent, including but not limited to at least one or more of the following:

a. The filing of Blue Spike’s complaint against Defendant in the Eastern District of Texas on February 17, 2017 (Case No. 6:17-cv-00100, Dkt. No. 1).

b. In the course of its due diligence and freedom to operate analyses.

On information and belief, Defendant has had at least had constructive notice of the ’011 Patent by operation of law. Plaintiff believes the evidence provided shows Defendant’s willful infringement is egregious. Even so, Plaintiff is not required to prove egregiousness in its pleadings. “Even after Halo, broader allegations of willfulness, without a specific showing of egregiousness, are sufficient to withstand a motion to dismiss.” *Shire ViroPharma Inc. v. CSL Behring LLC*, CV 17-414, 2018 WL 326406, at *3 (D. Del. Jan. 8, 2018) (denying a defendant’s motion to dismiss and noting “Defendants' argument seems to conflate the standards for pleading willful infringement with the standards for proving willful infringement.”).

REQUEST FOR RELIEF

Blue Spike incorporates each of the allegations in the paragraphs above and respectfully asks the Court to:

(a) enter a judgment that Defendant has directly infringed, contributorily infringed, and/or induced infringement of one or more claims of each of the Patents-in-Suit with a finding of over $50 million in damages based on statements made in Roku's Form S-1 that it submitted to the Securities Exchange Commission; and separately $150 million in willful infringement damages as Roku knew of the Blue Spike's patents and the value of this case as part of its due diligence it performed to submit its S-1 Form to the SEC, among other ways Roku willfully infringed.

(b) enter a judgment awarding Blue Spike all damages adequate to compensate it for Defendant's infringement of, direct or contributory, or inducement to infringe, the Patents-in-Suit, including all pre-judgment and post-judgment interest at the maximum rate permitted by law;

(c) enter a judgment awarding treble damages pursuant to 35 U.S.C. § 284 for Defendant's willful infringement of one or more of the Patents-in-Suit;

(d) issue a preliminary injunction and thereafter a permanent injunction enjoining and restraining Defendant, its directors, officers, agents, servants, employees, and those acting in privity or in concert with them, and their subsidiaries, divisions, successors, and assigns, from further acts of infringement, contributory infringement, or inducement of infringement of the Patents-in-Suit;

(e) enter a judgment requiring Defendant to pay the costs of this action, including all disbursements, and attorneys' fees as provided by 35 U.S.C. § 285, together with prejudgment interest; and

(f) award Blue Spike all other relief that the Court may deem just and proper.

DEMAND FOR JURY TRIAL

Blue Spike demands a jury trial on all issues that may be determined by a jury.

Respectfully submitted,

/s/ Stamatios Stamoulis
Stamatios Stamoulis #4606
stamoulis@swdelaw.com
Stamoulis & Weinblatt LLC
Two Fox Point Centre
6 Denny Road, Suite 307
Wilmington, DE 19809
(302) 999-1540

Randall T. Garteiser
Texas Bar No. 24038912
rgarteiser@ghiplaw.com
Christopher A. Honea
Texas Bar No. 24059967
chonea@ghiplaw.com
GARTEISER HONEA
119 W. Ferguson Street
Tyler, Texas 75702
Telephone: (903) 705-7420
Facsimile: (888) 908-4400

Ian Ramage
California Bar No. 224881
iramage@ghiplaw.com
GARTEISER HONEA
795 Folsom Street, Floor 1
San Francisco, California 94107
Telephone: (415) 785-3762
Facsimile: (888) 908-4400

Counsel for Blue Spike, LLC

CERTIFICATE OF SERVICE

I hereby certify that on April 18, 2018, I electronically filed the above document(s) with the Clerk of Court using CM/ECF which will send electronic notification of such filing(s) to all registered counsel.

/s/ Stamatios Stamoulis
Stamatios Stamoulis #4606