IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

BLUE SPIKE LLC;
BLUE SPIKE INTERNATIONAL LTD.;
WISTARIA TRADING LTD.,

Plaintiffs,

v.

SOUNDCLOUD LTD.,

Defendant.

Civil Action No. ______________

JURY TRIAL DEMANDED

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Blue Spike LLC ("Blue Spike LLC"), Plaintiff Blue Spike International Ltd. ("Blue Spike Int."), and Plaintiff Wistaria Trading Ltd. ("Wistaria") (collectively, "Plaintiffs"), for their Complaint against Defendant SoundCloud Ltd., (referred to herein as "SoundCloud" or "Defendant"), allege the following:

NATURE OF THE ACTION

1. This is an action for patent infringement arising under the Patent Laws of the United States, 35 U.S.C. § 1 *et seq*.

THE PARTIES

2. Plaintiff Blue Spike LLC is a limited liability company organized under the laws of the State of Texas with a place of business at 1820 Shiloh Road, Suite 1201-C, Tyler, Texas 75703.

3. Plaintiff Blue Spike Int. is a limited liability company established in Ireland with a place of business at Unit 6, Bond House, Bridge Street, Dublin 8, Ireland. Blue Spike Int. was recently acquired by Blue Spike Inc., a Florida corporation. Blue Spike Inc. has no right, title, or

interest in the patents in suit, nor any licensing rights to the patents in suit, nor any enforcement rights in the patents in suit.

4. Plaintiff Wistaria Trading Ltd. is a Bermuda corporation with a place of business at Clarendon House, 2 Church St., Hamilton HM 11, Bermuda.

5. On information and belief, Defendant is a company organized under the law of Germany, with its principal place of business at Rheinberger Str. 76/77, 10115 Berlin, Germany. Defendant can be served through its general manager and wholly-owned subsidiary, SoundCloud Inc. On information and belief, SoundCloud Inc. is a corporation established under the laws of the State of Delaware, with its place of business at 5th Floor, 71 W 5th Avenue, New York, NY 10003. SoundCloud Inc. and SoundCloud Ltd. can be served through its registered agent, The Corporation Service Company, located at 251 Little Falls Drive, Wilmington, DE 19808.

JURISDICTION AND VENUE

6. This is an action for patent infringement arising under the Patent Laws of the United States, Title 35 of the United States Code.

7. This Court has subject matter jurisdiction under 28 U.S.C. §§ 1331 and 1338(a).

8. Venue is proper in this judicial district under 28 U.S.C. § 1400(b).

9. Venue is proper as to SoundCloud in this judicial district under 28 U.S.C. §1391(c)(3). On information and belief, SoundCloud is not resident in the United States and may be sued in any judicial district.

10. Further, this Court has personal jurisdiction over SoundCloud under the laws of the State of Delaware, due at least to their substantial business in Delaware and in this judicial district, directly or through intermediaries, including: (i) at least a portion of the infringements alleged herein; and (ii) regularly doing or soliciting business, engaging in other persistent courses

of conduct and/or deriving substantial revenue from goods and services provided to individuals in the State of Delaware.

BACKGROUND

The Inventions

11. Scott A. Moskowitz and Michael W. Berry are the inventors of U.S. Patent No. 7,813,506 ("the '506 Patent"). A true and correct copy of the '506 patent is attached as Exhibit A.

12. Scott A. Moskowitz is the inventor of U.S. Patent Nos. 7,159,116 ("the '116 patent"). A true and correct copy of the '116 patent is attached as Exhibit C.

13. Scott A. Moskowitz is the inventor of U.S. Patent Nos. 8,538,011 ("the '011 patent"). A true and correct copy of the '011 patent is attached as Exhibit B.

14. The '506 patent, the '116 patent, and the '011 patent (collectively, "the patents in suit") all cover pioneering technologies for rights management and content security.

15. The patents in suit are all assigned to and owned by Wistaria. Blue Spike LLC is the exclusive licensee of the patents in suit. Blue Spike LLC's exclusive license to the patents in suit includes the right to assert infringement under 35 U.S.C. §271 and grant sub-licenses to the patents in suit.

16. Blue Spike Int. is a prior exclusive licensee of the patents in suit, which license was revoked upon the grant of the exclusive license to Blue Spike LLC; however, Blue Spike Int. retains the right to receive all revenues from Blue Spike LLC's licensing of the patents in suit.

17. Blue Spike LLC, Blue Spike Int., and Wistaria are each exclusively and entirely owned and controlled by Scott Moskowitz.

18. The '506 Patent resulted from the pioneering efforts of Scott Moskowitz and Mike Berry in the area of monitoring and analysis of digital information. These efforts resulted

in the development of systems and methods for open access and secured data objects memorialized in 2010. At the time of these pioneering efforts, a number of fundamental issues discouraged copyright holders from making their works available for general dissemination while ensuring payment for those works. This was especially the case for copyrighted works that may be digitally sampled and made available to open networks such as the World Wide Web. Mr. Moskowitz and Mr. Berry conceived of the inventions claimed in the '506 patent as a way to utilize sophisticated security, scrambling, and digital watermarking technology to resolve the aforementioned problems with digital copyrighted works.

19. The '116 patent and the '011 patent (collectively, the "Trusted Transaction patents") resulted from the pioneering efforts of Mr. Moskowitz (hereinafter "the Inventor") in the area of transferring information between parties. These efforts resulted in the development of systems, methods, and devices for trusted transactions memorialized in mid-2000. At the time of these pioneering efforts, the most widely implemented technology used to address the difficulty of providing to a prospective acquirer of good or services full, accurate, and verifiable information regarding the nature, value, authenticity, and other suitability-related characteristics of the product in question was inadequate. In that type of system, reciprocal and non-reciprocal systems could use non-secret algorithms to provide encryption and decryption. The Inventor conceived of the inventions claimed in the Trusted Transaction patents as a way to enhance trust on the part of participants in the transaction.

20. For example, the Inventor developed methods and systems which enhance trust in transactions in connection with sophisticated security, scrambling, and encryption technology by, for example, steganographic encryption, authentication, and security means.

Advantage Over the Prior Art

21. The patented inventions disclosed in the '506 Patent provide many advantages over the prior art, and in particular improved the open access to data objects and securing data within the data objects. *E.g.*, Exhibit A, '506 Patent at 2:23–31. One advantage of the patented invention is the protection of, and access to, copyrighted works that may be digitally sampled and made available to open networks such as the World Wide Web. *Id.*

22. Because of these significant advantages that can be achieved through the use of the patented invention, Blue Spike believes that the '506 Patent presents significant commercial value for companies like SoundCloud. Indeed, the technology described and claimed in the '506 Patent reads on the core functionality of SoundCloud's product and services.

23. The patented inventions disclosed in the Trusted Transaction patents provide many advantages over the prior art, and in particular improved the operations of transaction devices. *E.g.*, Exhibit C, '116 patent at 3:38–7:67; Exhibit B, '011 patent at 3:42–7:60. One advantage of the patented invention is the handling of authentication, verification, and authorization with a combination of cryptographic and steganographic protocols to achieve efficient, trusted, secure exchange of digital information. *See* Exhibit C, '116 patent at 3:46–51; Exhibit B, '011 patent at 3:50–57.

24. Another advantage of the patented invention is leveraging the benefits of digital information (such as media content) to consumers and publishers, while ensuring the development and persistence of trust between all parties. *E.g.*, Exhibit C, '116 patent at 3:16–30.

25. Another advantage of the patented invention is the integration of system components, optimally requiring comparatively little processing resources so as to maximize its

usefulness and minimize its cost. *E.g.*, Exhibit C, ‘116 patent at 3:52–55; Exhibit B, ‘011 patent at 3:53–57.

26. Because of these significant advantages that can be achieved through the use of the patented invention, Plaintiffs believe the Trusted Transaction patents present significant commercial value for companies like Dish. Indeed, the technology described and claimed in the Trusted Transaction patents read on the core security functionality of Dish’s downloadable apps.

Technological Innovation

27. The ’506 Patent is directed to electronically securing data objects by scrambling a data object to degrade the data object to a predetermined signal quality level. *See, e.g.*, Exhibit A at 2:38–52.

28. By scrambling a data object to degrade the data object to a predetermined signal quality level, the ’506 Patent describes a technical solution to a technical problem that is intrinsically tied to electronically securing data objects. *Id.* at Abstract.

29. The ’506 Patent describes improvements to electronically securing data objects. As an example, rather than providing disparate security schemes for audio files of different signal quality, the ’506 Patent describes methods for “designing security to meet either model [streaming and downloads].” *Id.* at 7:66–8:5.

30. The ’506 Patent also discloses multiple inventive concepts and improvements over prior data security systems. *E.g.*, *id.* at 11:36–62.

31. The ’506 Patent is not directed to any abstract idea, method of organizing human activity, or any fundamental economic practice. The claims of the ’506 Patent are directed toward technical solutions to technical problems-how to protect digital audio files when those files are widely distributed over a large, networked population. *See, e.g.*, *id.* at 11:36–63.

32. As demonstrated by its frequent citation by the USPTO in other later-issued patents and pending patent applications involving data security systems, the ’506 Patent represents a fundamental technical improvement involving electronically securing data objects. Specifically, the ’506 Patent has been cited during the prosecution of 112 subsequently issued U.S. patents and pending U.S. patent applications.

33. Accordingly, the claims in the ’506 Patent recite a combination of elements sufficient to ensure that the claim in substance and in practice amounts to significantly more than a patent-ineligible abstract idea.

34. The patented invention disclosed in the Trusted Transaction patents resolves technical problems related to transferring information between parties, particularly problems related to the utilization of sophisticated security, scrambling, and encryption technology by, for example, steganographic encryption, authentication, and security means. As the Trusted Transaction patents explain, one of the limitations of the prior art as regards the technical problems related to transferring information between parties was the difficulty of providing to a prospective acquirer of good or services full, accurate, and verifiable information regarding the nature, value, authenticity, and other suitability-related characteristics of the product in question. In that type of system, reciprocal and non-reciprocal systems could use non-secret algorithms to provide encryption and decryption. (*See* Exhibit C, ‘116 patent at 2:53–3:35; Exhibit B, ‘011 patent at 2:57–3:38.)

35. The claims of the Trusted Transaction patents do not merely recite the performance of some well-known business practice from the pre-Internet world along with the requirement to perform it on the Internet. Instead, the claims of the Trusted Transaction patents recite inventive concepts that are deeply rooted in engineering technology, and overcome

problems specifically arising out of how to enhance trust on the part of participants in the transaction.

36. In addition, the claims of the Trusted Transaction patents recite inventive concepts that improve the functioning of devices for conducting trusted transactions, particularly by creating a bridge between mathematically determinable security and analog or human measure of trust.

37. Moreover, the claims of the Trusted Transaction patents recite inventive concepts that are not merely routine or conventional use of computer components. Instead, the patented invention disclosed in the Trusted Transaction patents provides a new and novel solution to specific problems related to enhancing trust on the part of participants in a transaction.

38. And finally, the patented inventions disclosed in the Trusted Transaction patents do not preempt all the ways that enhancing trust on the part of participants in a transaction may be used to improve devices for trusted transactions, nor do the Trusted Transaction patents preempt any other well-known or prior art technology.

39. Accordingly, the claims in the Trusted Transaction patents recite a combination of elements sufficient to ensure that the claim in substance and in practice amounts to significantly more than a patent-ineligible abstract idea.

COUNT I – INFRINGEMENT OF U.S. PATENT NO. 7,813,506

40. The allegations set forth in the foregoing paragraphs are incorporated into this First Claim for Relief.

41. On October 12, 2010, the ’506 Patent was duly and legally issued by the United States Patent and Trademark Office under the title “System and Methods for Permitting Open Access to Data Objects and for Securing Data Within the Data Objects.”

42. Upon information and belief, SoundCloud has and continues to directly infringe one or more claims of the ’506 Patent by selling, offering to sell, making, using, and/or providing and causing to be used products, specifically one or more streaming services, which by way of example include http://www.soundcloud.com (the “Accused Instrumentalities”).

43. Upon information and belief, the Accused Instrumentalities infringe claim 6 of the ‘506 patent. The Accused Instrumentalities include a method for distributing accessible digital content. Said method is found in the Accused Instrumentalities. For example, SoundCloud offers a method for streaming (distributing) digital music (accessible digital content) through its SoundCloud website and applications. (Exhibit 1, SoundCloud, *SoundCloud—Listen to Free Music & Podcasts on SoundCloud,* SoundCloud website, https://soundcloud.com/ (last accessed October 8, 2018); Exhibit 14, SoundCloud, *SoundCloud—Listen to Free Music & Podcasts on SoundCloud,* SoundCloud website, https://soundcloud.com/ (last accessed January 2, 2019).)

44. Upon information and belief, the Accused Instrumentalities include a method for distributing accessible digital content by providing a digital content comprising digital data and file format information. Said method is found in the Accused Instrumentalities. For example, SoundCloud provides streaming music services for user-selected digital audio files (digital content). On information and belief, the digital audio files include the audio content (digital data) and header information that includes information indicative of the coding format of the audio content (file format information). For example, SoundCloud provides audio files in the Opus format and other formats. (Exhibit 5 at 1, Miles Bowe, *SoundCloud Changed Its Audio Format and Users Are Not Happy About It*, Fact Mag (Jan. 4, 2018), http://www.factmag.com/2018/01/04/soundcloud-mp3-opus-format-sound-qualitychange-64-

128-kbps/ (last accessed 10/9/2018) ("SoundCloud recently swapped its audio format from 128 kbps MP3 to 64 kbps Opus and some users are not happy about it.").)

45. Upon information and belief, the Accused Instrumentalities include a method for distributing accessible digital content by selecting a scrambling technique to apply to the digital content. Said method is found in the Accused Instrumentalities. For example, SoundCloud provides digital audio files (digital content) that includes audio content owned by, among others, UMG. (Exhibit 12, SoundCloud, *Announcing Our Partnership With Universal Music Group*, SoundCloud website (Jan. 13, 2016), https://blog.soundcloud.com/2016/01/13/announcing-ourpartnership-with-universal-music-group/ (last accessed 10/9/2018).) On information and belief, at least the audio content owned by UMG includes a digital watermark within the digital audio file. (See Exhibit 10, Matt Montag, *Universal's Audible Watermark*, Matt Montag blog, http://www.mattmontag.com/music/universals-audible-watermark (last accessed 09/24/2018).) In order to have a digital watermark within the digital audio file, a digital watermarking process (a scrambling technique) must have been selected to apply to the digital content that includes the digital audio file.

46. Upon information and belief, the Accused Instrumentalities include a method for distributing accessible digital content by scrambling the digital content using a predetermined key resulting in perceptibly degraded digital content. Said method is found in the Accused Instrumentalities. For example, SoundCloud provides digital audio files (digital content) that includes audio content owned by, among others, UMG. On information and belief, at least the audio content owned by UMG includes a digital watermark within the digital audio file. (*See* Exhibit 10.) Audio watermarking includes combining audio content with a predetermined key signal (a predetermined key) to create a modified audio file with perceptibly degraded digital

content. (*See generally* Exhibit 11, Stephan Wiefling, *Comparison of Audio Watermarking Techniques*, Master Hauptseminar Medientechnologie WS 15/16 (2016), https://www.researchgate.net/publication/316192889_Comparison_of_Audio_Watermarking-Techniques (last accessed 09/24/2018).) On information and belief, at least the digital audio files that include audio content owned by UMG and provided by SoundCloud to its users include scrambled digital content using a predetermined key. The inclusion of the digital watermark in the digital audio file results in perceptibly degraded digital content. (*See* Exhibit 10.)

47. Upon information and belief, the Accused Instrumentalities include a method for distributing accessible digital content wherein the scrambling technique is based on a plurality of predetermined criteria including at least the criteria of reaching a desired signal quality level for the digital content and distributing the scrambled digital content. Said method is found in the Accused Instrumentalities. For example, SoundCloud offers its authorized users a streaming service that provides digital audio. The streaming digital audio is delivered to users as a target quality level (a desired signal quality level for the digital content). (Exhibit 9, *SoundCloud Responds to Decreased Sound Quality Claims, Addresses Code Confusion*, Pigeons & Planes (Jan. 5, 2018), https://pigeonsandplanes.com/news/2018/01/soundcloud-responds-lower-sound-quality (last accessed 10/9/2018).) On information and belief, in order to provide users with streaming content at target audio quality levels, the digital audio files are encoded at those audio quality levels. As the inclusion of the digital watermark is done prior to encoding, the digital watermarking process (the scrambling technique) is based at least on the criteria of reaching a desired signal quality level for the digital content. The digital watermarking process (the scrambling technique) is also based on a plurality of criteria, including the ability to identify audio content provided by the audio content owner and watermarking techniques used to

improve the audio quality. (*See generally* Exhibit 11.) On information and belief, SoundCloud distributes digital audio files that include digital watermarking. (Exhibit 12; Exhibit 10.)

48. Upon information and belief, since at least the time of receiving the Complaint filed on June 15, 2018 in 1:18-cv-01402 (D. Del. (transferred from C.D. Cal.), SoundCloud has induced and continues to induce others to infringe at least claim 6 of the ’506 Patent under 35 U.S.C. § 271(b) by, among other things, and with specific intent or willful blindness, actively aiding and abetting others to infringe, including but not limited to SoundCloud’s partners and customers, whose use of the Accused Instrumentalities constitutes direct infringement of at least claim 6 of the ’506 Patent. Additionally, SoundCloud induces the users of the Accused Instrumentalities to perform the method described above in the claims by instructing them how to utilize and access digital content on SoundCloud’s website and applications.

49. In particular, SoundCloud’s actions that aid and abet others such as their partners and customers to infringe include distributing the Accused Instrumentalities and providing materials and/or services related to the Accused Instrumentalities. On information and belief, the SoundCloud has engaged in such actions with specific intent to cause infringement or with willful blindness to the resulting infringement because the SoundCloud has had actual knowledge of the ’506 Patent and that its acts were inducing infringement of the ’506 Patent since at least the time of receiving the Complaint filed on June 15, 2018 in 1:18-cv-01402 (D. Del. (transferred from C.D. Cal.).

50. On information and belief, SoundCloud’s infringement has been and continues to be willful.

51. Plaintiffs have been harmed by SoundCloud’s infringing activities.

COUNT II – INFRINGEMENT OF U.S. PATENT NO. 7,159,116

52. The allegations set forth in the foregoing paragraphs are incorporated into this Second Claim for Relief.

53. On January 2, 2007, the '116 Patent was duly and legally issued by the United States Patent and Trademark Office under the title "Systems, Methods and Devices for Trusted Transactions."

54. Upon information and belief, SoundCloud has and continues to directly infringe one or more claims of the '116 Patent by selling, offering to sell, making, using, and/or providing and causing to be used SoundCloud's App Server (the "Accused Instrumentalities").

55. Upon information and belief, the Accused Instrumentalities infringe at least claim 14 of the '116 patent. The Accused Instrumentalities include a device for conducting a trusted transaction between at least two parties who have agree to transact. Said device is found within the Accused Instrumentalities. For example, SoundCloud provides to at least one user (at least two parties who have agreed to transact) multiple apps, including the "SoundCloud" app available from the Google Play store (among others). On information and belief, SoundCloud maintains at least one server (a device for conducting trusted transactions between at least two parties) on which is hosted SoundCloud's app downloading and app authentication services ("App Server") (a device). (Exhibit 14.) On information and belief, SoundCloud desires the apps it makes available via, among other sources, the Google Play store, to be as secure as possible. As detailed below, best practices for securing apps available via the Google Play store are outlined in Google's Android developer's guidelines. On information and belief, therefore, SoundCloud's App Server makes its apps (including the SoundCloud app) available via the Google Play store in a manner similar to that described in Google's Android developer's guidelines. (*See generally* Exhibit 2, Google, *Adding Licensing to Your App*, Android

Developers, https://developer.android.com/google/play/licensing/adding-licensing (last accessed October 1, 2018).)

56. Upon information and belief, the Accused Instrumentalities contain a device comprising a 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 value adding component. Said device is found within the Accused Instrumentalities. For example, as detailed below, on information and belief, SoundCloud's App Server includes one or more components configured to identify at least "the most recent successful license response in local persistent storage" (a unique identification of a value adding component). (Exhibit 2 at 4.) On information and belief, SoundCloud desires the apps it makes available via, among other sources, the Google Play store, to be as secure as possible. As detailed below, best practices for securing apps available via the Google Play store are outlined in Google's Android developer's guidelines. On information and belief, therefore, SoundCloud's App Server makes its apps (including the SoundCloud app) available via the Google Play store in a manner similar to that described in Google's Android developer's guidelines. Among those guidelines are the use of Google's License Verification Library ("LVL") in its SoundCloud app available through the Google Play store. Google's LVL allows Google Play to send a license check to SoundCloud's App Server. "Google Play licensing service does not itself determine whether a given user with a given license should be granted access to your application. Rather, that responsibility is left to a Policy implementation that you provide in your application." (Exhibit 2 at 1–2.) On information and belief, SoundCloud implements the license verification in order to best protect its available apps. Additionally, on information and belief, SoundCloud implements a custom license policy to best protect its available apps. One of Google's recommend

design points for a custom policy is obfuscation of license response (a unique identification of a value adding component). (Exhibit 2 at 4.)

57. Upon information and belief, the Accused Instrumentalities contain a device comprising a steganographic cipher for generating said unique identification information. Said device is found within the Accused Instrumentalities. For example, on information and belief, SoundCloud's App Server employs a steganographic cipher for generating the most recent successful license response (unique identification information). For example, on information and belief, SoundCloud incorporates in its SoundCloud app available through the Google Play store an obfuscation program similar to the "AESObfuscator" found in Google's License Verification Library ("LVL"). Google's LVL allows Google Play to send a license check to SoundCloud's App Server. "Google Play licensing service does not itself determine whether a given user with a given license should be granted access to your application. Rather, that responsibility is left to a Policy implementation that you provide in your application." (Exhibit 2 at 1–2.) On information and belief, SoundCloud implements the license verification in order to best protect its available apps. Additionally, on information and belief, SoundCloud implements a custom license policy to best protect its available apps. One of Google's recommend design points for a custom policy is obfuscation of license response (a unique identification of a value adding component). (Exhibit 2 at 4.)

58. Upon information and belief, the Accused Instrumentalities contain a device comprising a steganographic cipher wherein the steganographic cipher is governed by at least the following elements: a predetermined key, a predetermined message, and a predetermined carrier signal. Said device is found within the Accused Instrumentalities. For example, on information and belief, SoundCloud's App Server employs a steganographic cipher for generating the most recent successful license response (unique identification information). For example, on

information and belief, SoundCloud incorporates in its SoundCloud app available through the Google Play store an obfuscation program similar to the "AESObfuscator" found in Google's License Verification Library ("LVL"). The obfuscation provided by Google is an interface called "AESObfuscator" (a steganographic cipher). AESObfuscator "seed the encryption using three data fields provided by the application," a "salt" (an array of random bytes) [a predetermined key], an "application identifier string, typically the package name of the application" [a predetermined carrier signal], and "a device identifier string, derived from as many device specific sources as possible, so as to make it unique" [a predetermined message]. (Exhibit 2 at 7.)

59. Upon information and belief, the Accused Instrumentalities contain a device comprising a steganographic cipher wherein the steganographic cipher is governed by at least a means for verifying an agreement to transact between the parties. Said device is found within the Accused Instrumentalities. For example, on information and belief, SoundCloud desires the apps it makes available via, among other sources, the Google Play store, to be as secure as possible. As detailed below, best practices for securing apps available via the Google Play store are outlined in Google's Android developer's guidelines. On information and belief, therefore, SoundCloud's App Server makes its apps (including the SoundCloud app) available via the Google Play store in a manner similar to that describe in Google's Android developer's guidelines. (*See generally* Exhibit 2.) On information and belief, in line with Google's Android developer's guidelines, SoundCloud's App Server includes one or more components to verify the license information (an agreement to transact between the parties) in order to authorize the download and/or installation of SoundCloud's apps, including the SoundCloud app. (Exhibit 2 at 9-10.)

60. Upon information and belief, since at least the time of receiving the Complaint filed on June 15, 2018 in 1:18-cv-01402 (D. Del. (transferred from C.D. Cal.), SoundCloud has induced and continues to induce others to infringe at least claim 14 of the ’116 Patent under 35 U.S.C. § 271(b) by, among other things, and with specific intent or willful blindness, actively aiding and abetting others to infringe, including but not limited to SoundCloud’s partners and customers, whose use of the Accused Instrumentalities constitutes direct infringement of at least claim 14 of the ’116 Patent.

61. In particular, SoundCloud’s actions that aid and abet others such as their partners and customers to infringe include distributing the Accused Instrumentalities and providing materials and/or services related to the Accused Instrumentalities. On information and belief, the SoundCloud has engaged in such actions with specific intent to cause infringement or with willful blindness to the resulting infringement because SoundCloud has had actual knowledge of the ’116 Patent and that its acts were inducing infringement of the ’116 Patent since at least the time of receiving the Complaint filed on June 15, 2018 in 1:18-cv-01402 (D. Del. (transferred from C.D. Cal.).

62. On information and belief, SoundCloud’s infringement has been and continues to be willful.

63. Plaintiffs have been harmed by SoundCloud’s infringing activities.

COUNT III – INFRINGEMENT OF U.S. PATENT NO. 8,538,011

64. The allegations set forth in the foregoing paragraphs are incorporated into this Third Claim for Relief.

65. On September 17, 2013, the ’011 Patent was duly and legally issued by the United States Patent and Trademark Office under the title “Systems, Methods and Devices for Trusted Transactions.”

66. Upon information and belief, SoundCloud has and continues to directly infringe one or more claims of the ’011 Patent by selling, offering to sell, making, using, and/or providing and causing to be used SoundCloud’s App Server (the “Accused Instrumentalities”).

67. Upon information and belief, the Accused Instrumentalities infringe at least claim 35 of the ‘011 patent. The Accused Instrumentalities includes a device for conducting trusted transactions between at least two parties. For example, SoundCloud provides to at least one user (at least two parties who have agreed to transact) multiple apps, including the “SoundCloud” app available from the Google Play store (among others). On information and belief, SoundCloud maintains at least one server (a device for conducting trusted transactions between at least two parties) on which is hosted SoundCloud’s app downloading and app authentication services (“App Server”). (Exhibit 14.) On information and belief, SoundCloud desires the apps it makes available via, among other sources, the Google Play store, to be as secure as possible. As detailed below, best practices for securing apps available via the Google Play store are outlined in Google’s Android developer’s guidelines. On information and belief, therefore, SoundCloud’s App Server makes its apps (including the SoundCloud app) available via the Google Play store in a manner similar to that described in Google’s Android developer’s guidelines. (*See generally* Exhibit 2.)

68. Upon information and belief, the Accused Instrumentalities include a device for conducting trusted transactions between at least two parties, comprising a steganographic cipher. Said device is found within the Accused Instrumentalities. For example, on information and belief, SoundCloud’s App Server employs a steganographic cipher. For example, on information and belief, SoundCloud incorporates Google’s License Verification Library (“LVL”) in its SoundCloud app available through the Google Play store. Google’s LVL allows Google Play to

send a license check to SoundCloud's App Server. "Google Play licensing service does not itself determine whether a given user with a given license should be granted access to your application. Rather, that responsibility is left to a Policy implementation that you provide in your application." (Exhibit 2 at 1–2.) On information and belief, SoundCloud implements the license verification in order to best protect its available apps. Additionally, on information and belief, SoundCloud implements a custom license policy to best protect its available apps. One of Google's recommend design points for a custom policy is obfuscation of license response. (Exhibit 2 at 4.) The obfuscation provided by Google is an interface called "AESObfuscator" (a steganographic cipher). AESObfuscator "seed the encryption using three data fields provided by the application," a "salt" (an array of random bytes), an "application identifier string, typically the package name of the application," and "a device identifier string, derived from as many device-specific sources as possible, so as to make it unique." (Exhibit. 2 at 7.)

69. Upon information and belief, the Accused Instrumentalities include a device for conducting trusted transactions between at least two parties, comprising a controller for receiving input data or outputting output data and at least one input/output connection. Said device is found within the Accused Instrumentalities. For example, on information and belief, the SoundCloud App Server includes a controller for receiving input data or outputting output data. (Exhibit 14.) On information and belief, the SoundCloud App Server includes at least one input/output connection. (Exhibit 14.)

70. Upon information and belief, the Accused Instrumentalities include a device for conducting trusted transactions between at least two parties, wherein the device has a device identification code stored in the device. Said device is found within the Accused

Instrumentalities. For example, on information and belief, the SoundCloud App Server has an IP address, MAC address, or other device identification code stored in the device.

71. Upon information and belief, the Accused Instrumentalities include a device for conducting trusted transactions between at least two parties, wherein the device has an analog to digital converter. Said device is found within the Accused Instrumentalities. For example, on information and belief, the SoundCloud App Server has input/output and communications capabilities (an analog-to-digital converter).

72. Upon information and belief, the Accused Instrumentalities include a device for conducting trusted transactions between at least two parties, wherein the device has a steganographically ciphered software application, wherein said steganographically ciphered software application has been subject to a steganographic cipher for serialization. Said device is found within the Accused Instrumentalities. For example, on information and belief, the SoundCloud App Server provides multiple apps, including the SoundCloud App, whose code has been obfuscated in order to hinder reverse engineering (a steganographically ciphered software application). On information and belief, SoundCloud obfuscates its apps' source code in a manner similar to that described by Google in its recommendations to app developers, as detailed below.

73. For example, in its guidelines for app developers, Google states: "To ensure the security of your application, particularly for a paid application that uses licensing and/or custom constraints and protections, it's very important to obfuscate your application code. Properly obfuscating your code makes I much more difficult for a malicious user to decompile the application's bytecode, modify it – such as by removing the licensing check – and then recompile." (Exhibit 2 at 20.) Google recommends the obfuscating application ProGuard.

(Exhibit 2 at 20.) ProGuard obfuscates the actual code of the app by, for example, replacing human-readable names in compiled code with "short, machine generated alternatives. Rather than seeing a call to dontAllow(), an attacker would see a call to a(). This makes it more difficult to intuit the purpose of these functions without access to the original source code." (Exhibit 3 at 2, Trevor Johns, *Securing Android LVL Applications*, Android Developers Blog (Sept. 1, 2010), https://android-developers.googleblog.com/2010/09/securing-android-lvlapplications.html (last accessed October 1, 2018).) On information and belief, the code obfuscation provided by ProGuard and/or the license data obfuscation provided by Google's AESObfuscator (a steganographic cipher) allows the code to include be ciphered for serialization. For example, AESObfuscator obfuscates the most recent successful license response in local persistent storage. (Exhibit 2 at 4.) This obfuscation allows for serialized license responses

74. Upon information and belief, the Accused Instrumentalities include a device for conducting trusted transactions between at least two parties wherein said steganographic cipher receives said output data, steganographically ciphering said output data using a key to define stenganographically ciphered output data. Said steganographic cipher is found in the Accused Instrumentality. For example, on information and belief, as detailed above, SoundCloud's App Server makes use of steganographic ciphers similar to Google's AESObfuscator and/or ProGuard. On information and belief, therefore, SoundCloud's App server makes use of a steganographic cipher that receives output data. For example, AESObfuscator receives an "application identifier string" from the App Server. (Exhibit 2 at 7.) As another example, ProGuard receives the actual code of the apps output from the App Server. (Exhibit 3 at 2.) On information and belief, as detailed above, SoundCloud's App Server makes use of steganographic ciphers similar to Google's AESObfuscator and/or ProGuard. On information

and belief, therefore, SoundCloud's App server steganographically ciphers output data using a key. For example, AESObfuscator steganographically ciphers the application identifier string using a "salt," an "array of random bytes to use for each (un)obfuscation." (Exhibit 2 at 7.) On information and belief, ProGuard steganographically ciphers the code using either a public or private key. (Exhibit 3 at 2.) On information and belief, as detailed above, SoundCloud's App Server makes use of steganographic ciphers similar to Google's AESObfuscator and/or ProGuard. On information and belief, therefore, SoundCloud's App server defines steganographically ciphered output data. For example, AESObfuscator defines steganographically ciphered license responses. (Exhibit 2 at 7.) As another example, ProGuard defines steganographically ciphered code. (Exhibit 3 at 2.)

75. Upon information and belief, the Accused Instrumentalities include a device for conducting trusted transactions between at least two parties wherein said steganographic cipher transmits said steganographically ciphered output data to said at least one input/output connection. Said device is found within the Accused Instrumentalities. For example, SoundCloud provides multiple apps for its users, including the "SoundCloud" app. These apps are available from, among others, the Google Play store. On information and belief, the SoundCloud App Server transmits the steganographically ciphered output data (the stganographically ciphered code and/or code containing the steganographically ciphered license response) via the at least one input/output connection. (Exhibit 14.)

76. Upon information and belief, the Accused Instrumentalities include a device for conducting trusted transactions between at least two parties wherein the device is configured to steganographically cipher both value-added information and at least one value-added component associated with the value-added information. Said device is found within the Accused

Instrumentalities. For example, on information and belief, as detailed above, SoundCloud's App Server makes use of steganographic ciphers similar to Google's AESObfuscator and/or ProGuard. On information and belief, therefore, SoundCloud's App server is configured to steganographically cipher license information and/or proprietary source code. For example, AESObfuscator defines steganographically ciphered license responses, as well as an application identifier string. (Exhibit 2 at 7.) As another example, ProGuard defines steganographically ciphered code, including various proprietary code portions. (Exhibit 3 at 2.)

77. Upon information and belief, since at least the time of receiving the Complaint filed on June 15, 2018 in 1:18-cv-01402 (D. Del. (transferred from C.D. Cal.), SoundCloud has induced and continues to induce others to infringe at least claim 35 of the '011 Patent under 35 U.S.C. § 271(b) by, among other things, and with specific intent or willful blindness, actively aiding and abetting others to infringe, including but not limited to SoundCloud's partners and customers, whose use of the Accused Instrumentalities constitutes direct infringement of at least claim 35 of the '011 Patent.

78. In particular, SoundCloud's actions that aid and abet others such as their partners and customers to infringe include distributing the Accused Instrumentalities and providing materials and/or services related to the Accused Instrumentalities. On information and belief, the SoundCloud has engaged in such actions with specific intent to cause infringement or with willful blindness to the resulting infringement because SoundCloud has had actual knowledge of the '011 Patent and that its acts were inducing infringement of the '011 Patent since at least the time of receiving the Complaint filed on June 15, 2018 in 1:18-cv-01402 (D. Del. (transferred from C.D. Cal.).

79. On information and belief, SoundCloud's infringement has been and continues to be willful.

80. Plaintiffs have been harmed by SoundCloud's infringing activities.

JURY DEMAND

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, Plaintiffs Blue Spike LLC, Blue Spike Int., and Wistaria demand a trial by jury on all issues triable as such.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Blue Spike LLC, Blue Spike Int., and Wistaria demand judgment for themselves and against SoundCloud as follows:

A. An adjudication that SoundCloud has infringed the patents in suit;

B. An award of damages to be paid by SoundCloud adequate to compensate Plaintiffs for SoundCloud's past infringement of the patents in suit, and any continuing or future infringement through the date such judgment is entered, including interest, costs, expenses and an accounting of all infringing acts including, but not limited to, those acts not presented at trial;

C. A declaration that this case is exceptional under 35 U.S.C. § 285, and an award of Plaintiffs' reasonable attorneys' fees; and

D. An award to Plaintiffs of such further relief at law or in equity as the Court deems just and proper.

Dated: January 28, 2019

DEVLIN LAW FIRM LLC

/s/ Timothy Devlin
Timothy Devlin (No. 4241)
James Lennon (No. 4570)
1306 N. Broom St., 1st Floor
Wilmington, Delaware 19806
Telephone: (302) 449-9010
Facsimile: (302) 353-4251

Attorneys for Plaintiffs
Blue Spike LLC
Blue Spike International Ltd.
Wistaria Trading Ltd.