IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

SELENE COMMUNICATION TECHNOLOGIES, LLC, Plaintiff, v. CISCO SYSTEMS, INC., Defendant.	C.A. No. _____ **JURY TRIAL DEMANDED**

COMPLAINT FOR PATENT INFRINGEMENT

This is an action for patent infringement in which Plaintiff, Selene Communication Technologies, LLC ("Selene"), makes the following allegations against Defendant Cisco Systems, Inc. ("Cisco"):

PARTIES

1. Plaintiff Selene is a Delaware limited liability company with its principal place of business at 2961 Fontenay Road, Shaker Heights, Ohio 44120.

2. On information and belief, Defendant Cisco Systems, Inc. is a California corporation with its principal office at 170 West Tasman Drive, San Jose, California 95134. Cisco has appointed Corporation Service Company which will do business in California as CSC – Lawyers Incorporating Service, 2710 Gateway Oaks Dr Ste 150N, Sacramento, California 95833, as its agent for service of process.

JURISDICTION AND VENUE

3. This action arises under the patent laws of the United States, 35 U.S.C. § 1, *et seq.*, including § 271. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

4. This Court has personal jurisdiction over Cisco because, among other reasons, Cisco has done business in this District, has committed and continues to commit acts of patent infringement in this District, and has harmed and continues to harm Selene in this District, by, among other things, using, selling, offering for sale, and importing infringing products and services in this District.

5. Venue is proper in this District under 28 U.S.C. §§ 1391(b)-(c) and 1400(b) because, among other reasons, Cisco is subject to personal jurisdiction in this District, and has committed and continues to commit acts of patent infringement in this District. On information and belief, for example, Cisco has used, sold, offered for sale, and imported infringing products/services in this District.

FACTUAL BACKGROUND

6. United States Patent No. 7,143,444 ("the '444 Patent"), entitled "Application-Layer Anomaly and Misuse Detection," issued on November 28, 2006 and was invented by Phillip Andrew Porras, Magnus Almgren, Ulf E. Lindqvist, and Steven Mark Dawson of SRI International ("SRI"). SRI, which began as an initiative among researchers at Stanford University, was founded as Stanford Research Institute, a 501(c)(3) nonprofit corporation, by Stanford University in 1946.

7. Since its inception, SRI was a pioneer in advancing technology in ways that had a profound global impact. For instance, in 1963, engineers at SRI created the first optical video disk recording system, paving the way for modern optical storage technologies such as CD-ROMs, DVDs, and Blu-Ray discs. In the early 1960s, SRI engineers invented the world's first computer mouse.

8. In the late 1960s, SRI collaborated with the U.S. Department of Defense to create "ARPANET"—the progenitor of what would become the global Internet.

9. SRI was spun out from Stanford University in 1970. In the early 1970s, SRI was the first organization to utilize domain names, with extensions such as ".com," ".org," or ".gov." In 1977, SRI created what is considered to be the first true Internet connection, by connecting three dissimilar networks.

10. In 1988, SRI combined with Sarnoff Corporation ("Sarnoff"). The Sarnoff Corporation, formed in 1941, traces its origins to David Sarnoff, a principal technology researcher at RCA Laboratories. It was created to be a research and development company specializing in vision, video, and semiconductor technology, and it later expanded its research areas to include various facets of information technology. Sarnoff is known for several important technological advances. For instance, in 1953, David Sarnoff and RCA Laboratories created the world's first color television system. From 1963 to 1968, a team of engineers at the David Sarnoff Research Center developed a revolutionary method for the electronic control of light reflected from liquid crystals—leading to their invention of the liquid crystal display (LCD). Sarnoff is also credited for the development of the electron microscope and early optoelectronic components such as lasers and LEDs.

11. In 2007, SRI spun off its creation of Siri, a virtual personal assistant with a natural language interface, as Siri, Inc. Siri was acquired by Apple Inc. in 2011.

12. SRI today is a nonprofit, independent research and innovation center serving government and industry that derives revenue from a variety of sources, including licensing. SRI employs over 2,500 employees at research facilities across the United States and abroad, including researchers at the former Sarnoff facilities in Princeton, New Jersey.

13. All of the inventions disclosed and claimed in the '444 Patent were invented and patented by technology researchers at SRI, a premier institution with a long history of leading technological innovation. The '444 Patent issued as the result of the inventiveness of SRI personnel and SRI's substantial investments in research and development.

14. Pursuant to a purchase agreement and assignment from SRI completed in July 2013, Plaintiff Selene owns the '444 Patent, and has the exclusive right to sue for infringement and recover damages for all past, present, and future infringement. A true and correct copy of the '444 Patent is attached as Exhibit A.

15. On November 28, 2001, Phillip Andrew Porras, Magnus Almgren, Ulf E. Lindqvist, and Steven Mark Dawson filed their application for what would become the '444 Patent. Each of the inventors were employed by SRI at its facilities in Menlo Park, California.

16. SRI pioneered the field of network intrusion detection. In 1997, SRI researchers published their creation of the Event Monitoring Enabling Responses to Anomalous Live Disturbances ("EMERALD"),[1] which became a foundational and patented industry standard for intrusion detection. See http://www.sri.com/work/timeline-innovation/timeline.php?timeline=computing-digital#!&innovation=network-intrusion-detection:

[1] *See* Porras et al., *EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances*, 1997 National Information Systems Security Conference (Oct. 1997), *available at* http://www.csl.sri.com/papers/emerald-niss97/ (last visited Sept. 22, 2013).

1990s

Network Intrusion Detection

For many years, SRI has pioneered cyber security technology to protect vital infrastructures against malicious attacks. SRI's patented, software-based intrusion detection solution called Event Monitoring Enabling Responses to Anomalous Live Disturbances (EMERALD®) led to today's network intrusion detection solutions. EMERALD uses lightweight sensors distributed over a network or series of networks for real-time detection of cyber-attack activity.

SRI's other R&D related to cyber security includes malware threat detection and information sharing, highly predictive blacklisting, cyber-threat analytics, industrial control systems (ICS) in the energy and financial sectors, telecommunications, and the Internet. SRI has been providing technical, managerial, and administrative support to the Department of Homeland Security's Cyber Security Research and Development Center since the center was established in 2004.

17. SRI continues to license its patents related to its EMERALD technology to industry leaders in the field of cyber-security to date, including, most recently, Symantec and IBM.[2] SRI's EMERALD research team is led by Principal Investigator Phillip Porras, the Program Director of SRI's Internet Security Group and an inventor of the '444 Patent.[3]

18. The '444 Patent, while covering technology distinct from EMERALD, advanced the state of the art of intrusion detection by teaching methods and systems for effectively hosting an intrusion detection process in a server and integrating the intrusion detection processes into server processes. The inventions of the '444 Patent are fundamental to modern methods and systems for intrusion detection. The '444 Patent has been cited during the prosecution of more

---

[2] *See, e.g.*, Press Release, SRI International Licenses EMERALD Network Intrusion Detection Patents to IBM (Mar. 14, 2013), *available at* http://www.sri.com/newsroom/press-releases/sri-international-licenses-emerald-network-intrusion-detection-patents-ibm (last visited Sept. 22, 2013).

[3] *See* SRI International, EMERALD, at http://www.csl.sri.com/projects/emerald/ (last visited Sept. 22, 2013). Dr. Ulf Lindqvist, another inventor of the '444 Patent, is also a staff member of the EMERALD team.

than 13 later-filed patents. The ’444 Patent has been cited in the patent applications of a variety of industry leaders in intrusion detection including Hewlett-Packard, Symantec, and Microsoft.

19. By way of example only, Claim 1 recites one of the inventions disclosed in the ’444 Patent: “1. A method comprising: in a server, hosting an intrusion detection process that provides intrusion detection services; integrating the intrusion detection process with a server process; and passing a request for data received by the server process to the intrusion detection process, where the intrusion detection process comprises: packing a subset of information from the request into an analysis format; and delivering the subset in a funneling process, via a socket, to an analysis process.”

COUNT I
INFRINGEMENT OF U.S. PATENT NO. 7,143,444

20. Cisco is a privately owned, multinational computer technology company that develops, sells, repairs, and supports computers and related products and services, including software and network security products. In 2012, Cisco was the third largest PC vendor in the world and reported approximately $62.1 billion in revenue. Cisco was a publicly traded company until October 30, 2013, when it became private in a leveraged buyout.

21. Cisco markets products called Cisco Security Agents (“Agents”), which are “[h]ost-based IPS software running on servers and desktops to be protected and monitored,” Management Center for Cisco Security Agents (“Cisco Security Agent MC”), which is “a standalone application that provides centralized security policy configuration, monitoring, and administration for Cisco Security Agents … perform[ing] global correlation based on event and posture information generated by the Cisco Security Agent [which can] integrate with IPS,” and Cisco IPS (“Sensor”), which is “[a]ny Cisco IPS platform running at minimum Cisco IPS Sensor

Software Version 6.0, configured either in inline protection (IPS) or promiscuous mode (IDS)." See http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5729/ps5713/ps4077/prod_white_paper0900aecd805c389a_ns441_Networking_Solutions_White_Paper.html.

22. Cisco also markets products called Cisco ASA 5500-X Series Next-Generation Firewalls, which run Cisco ASA Next-Generation Firewall Services, including Intrusion Prevention System (IPS). See http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/data_sheet_c78-701659.pdf. Cisco's IPS operates, inter alia, to analyze incoming packets over the network and determine whether to forward or drop a packet. See http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/4.1/user/guide/monidiag.html#wpxref140238.

23. On October 7, 2013, Cisco acquired Sourcefire for an aggregate purchase price of roughly $2.6 billion. See http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/ime/8_0_2/config/ime-802.pdf. As a result of the Sourcefire acquisition, Cisco also markets the Sourcefire Virtual Appliance, which "enable[s] organizations to inspect traffic between virtual machines (VMs) … The Sourcefire Virtual Appliance detects … any malicious traffic between the two [virtual] networks." See https://na8.salesforce.com/sfc/p/80000000dRH9KXPLJqkSwWBoW3e_vtLbnXOyiNg=.

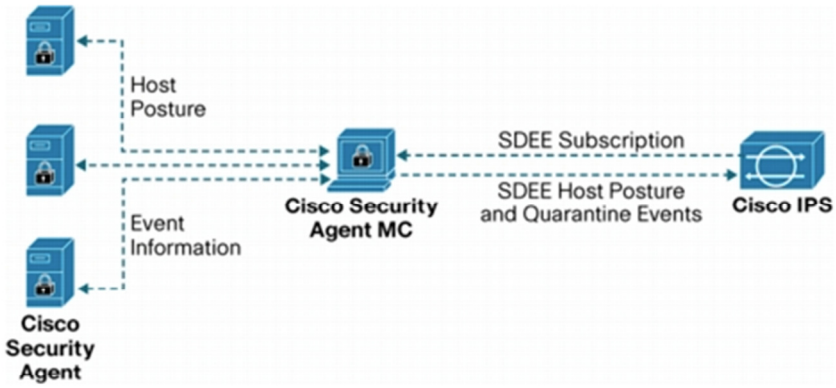
24. As a result of the Sourcefire acquisition, Cisco also markets the Sourcefire Virtual Defense Center™, which can correlate and prioritize event data with network and user awareness" and "aggregate[e] and analyz[e] security and compliance events from across the organization." See https://materials.proxyvote.com/Approved/83616T/20120404/AR_124967/PDF/sourcefire-ar2011_0015.pdf, Page 5.

25. Cisco has been and now is directly infringing the ‘444 Patent literally and/or under the doctrine of equivalents, in this judicial District and elsewhere in the United States, by, among other things, practicing a method comprising: in a server, hosting an intrusion detection process that provides intrusion detection services; integrating the intrusion detection process with a server process; and passing a request for data received by the server process to the intrusion detection process, where the intrusion detection process comprises: packing a subset of information from the request into an analysis format; and delivering the subset in a funneling process, via a socket, to an analysis process. Cisco has also been and now is directly infringing the ‘444 Patent literally and/or under the doctrine of equivalents, in this judicial District and elsewhere in the United States, by, among other things, making, using, selling, offering for sale, or importing a computer program product residing on a computer readable medium having instructions stored thereon which, when executed by a processor, cause the processor to: host, in a server, an intrusion detection process that provides intrusion detection services; integrate the intrusion detection process with a server process; and pass a request for data received by the server process to the intrusion detection process, where the intrusion detection process comprises: packing a subset of information from the request into an analysis format; and delivering the subset in a funneling process, via a socket, to an analysis process. The infringing products and services include, for example, (1) Cisco Security Agent/IPS Collaborative Architecture, including Cisco Security Agent, Cisco Security Agent MC, and Cisco IPS; (2) Cisco ASA 5500-X Series Next-Generation Firewalls running Cisco ASA Next-Generation Firewall Services, including Intrusion Prevention System (IPS) and/or Cisco Prime Security Manager; (3) the Sourcefire Virtual Appliance; and (4) the Sourcefire Virtual Defense Center™.

26. Cisco has had knowledge of the '444 Patent and evidence of infringement of the '444 Patent by (1) the Cisco Security Agent/IPS Collaborative Architecture, including Cisco Security Agent, Cisco Security Agent MC, and Cisco IPS, (2) Cisco ASA 5500-X Series Next-Generation Firewalls running Cisco ASA Next-Generation Firewall Services, including Intrusion Prevention System (IPS) and/or Cisco Prime Security Manager, (3) the Sourcefire Virtual Appliance; and (4) the Sourcefire Virtual Defense Center™, since at least the date Cisco was served with this Complaint for Patent Infringement, and Cisco has induced its customers, users of (1) the Cisco Security Agent/IPS Collaborative Architecture, including Cisco Security Agent, Cisco Security Agent MC, and Cisco IPS, (2) Cisco ASA 5500-X Series Next-Generation Firewalls running Cisco ASA Next-Generation Firewall Services, including Intrusion Prevention System (IPS) and/or Cisco Prime Security Manager, (3) the Sourcefire Virtual Appliance; and (4) the Sourcefire Virtual Defense Center™ to infringe the '444 Patent by providing instructions to (1) assemble the Cisco Security Agent/IPS Collaborative Architecture, including Cisco Security Agent, Cisco Security Agent MC, and Cisco IPS and use same, and use (2) the Cisco ASA 5500-X Series Next-Generation Firewalls running Cisco ASA Next-Generation Firewall Services, including Intrusion Prevention System (IPS) and/or Cisco Prime Security Manager; (3) the Sourcefire Virtual Appliance; and (4) the Sourcefire Virtual Defense Center™, to practice a method comprising: in a server, hosting an intrusion detection process that provides intrusion detection services; integrating the intrusion detection process with a server process; and passing a request for data received by the server process to the intrusion detection process, where the intrusion detection process comprises: packing a subset of information from the request into an analysis format; and delivering the subset in a funneling process, via a socket, to an analysis process.

27. For example, Cisco has instructed its customers, users of the Cisco Security Agent/IPS Collaborative Architecture, including Cisco Security Agent, Cisco Security Agent MC, and Cisco IPS, to connect and configure Cisco Security Agent, Cisco Security Agent MC, and Cisco IPS as shown in Figure 1 below:

Figure 1. Cisco Security Agent/IPS Collaborative Architecture



Note: The minimum software versions required for integration are Cisco Security Agent MC 5.0 and Cisco IPS Sensor Software 6.0.

See http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5729/ps5713/ps4077/prod_white_paper0900aecd805c389a_ns441_Networking_Solutions_White_Paper.html. Cisco further explains the functionality of this configuration to its customers as follows:

> "The Cisco Security Agent is a host-based agent that seats between the applications and OS kernel, gaining maximum endpoint visibility, and providing defense-in-depth protection to mission-critical servers and desktops. As part of their operation, Cisco Security Agents generate valuable event and posture information that is collected and correlated by Cisco Security Agent MC. The transfer of information between the agents and Cisco Security Agent MC is protected by the use of SSL.
>
> In addition to the detailed endpoint information collected from agents, Cisco Security Agent MC global correlation generates threat data that can be valuable to Cisco IPS. When shared with Cisco IPS, this data helps increase the sensor visibility on endpoints and global threats. The Cisco IPS sensor accesses this information via Secure Device Event Exchange (SDEE), a protocol developed by a consortium (led by Cisco) designed for the secure exchange of network event information. Communications between Cisco Security Agent MC and IPS are protected with SSL/TLS encryption and HTTP authentication."

See also http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5729/ps5713/ps4077/prod_white_paper0900aecd805c389a.pdf ("Integrating Cisco Security Agent with Cisco Intrusion Prevention System "), Pages 3-4 (explaining that the Cisco Security Agent and Cisco IPS collaborate "to capture traffic from and to the hosts protected with Cisco Security Agents" and "block attacks dynamically as malicious packets move through the system.").

28. By way of further example, Cisco explains to its customers, users of Cisco ASA 5500-X Series Next-Generation Firewalls running Cisco ASA Next-Generation Firewall Services, including Intrusion Prevention System (IPS) and/or Cisco Prime Security Manager, that such products/services operate to "[p]rotect[] against theft of data and passwords" (see http://www.cisco.com/cdc_content_elements/flash/asa_vpn/demo.htm) and monitor "traffic patterns throughout the network" to "support[] real-time and historical event analysis" "that may be required for anomalous traffic." See http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5739/ps12635/data_sheet_c78-711823.html.

29. By way of further example, Cisco explains to its customers, users of the Sourcefire Virtual Appliance, that the Sourcefire Virtual Appliance, which can be hosted on VMware ESX/ESXi 4.1/5.0, and Xen 3.3.2/3.4.2 or RHEV 3.0 servers, and deployed in passive or inline mode (see https://na8.salesforce.com/sfc/p/80000000dRH9KXPLJqkSwWBoW3e_vtLbnXOyiNg=), "provide[s] the capability to inspect communications between different virtual machines residing on the same box, providing the same control and protection as their physical counterparts." See https://materials.proxyvote.com/Approved/83616T/20120404/AR_124967/PDF/sourcefire-ar2011_0015.pdf, Page 5.

30. By way of further example, Cisco explains to its customers, users of the Sourcefire Virtual Defense Center™, that the Sourcefire Virtual Defense Center™ is "[i]dentical

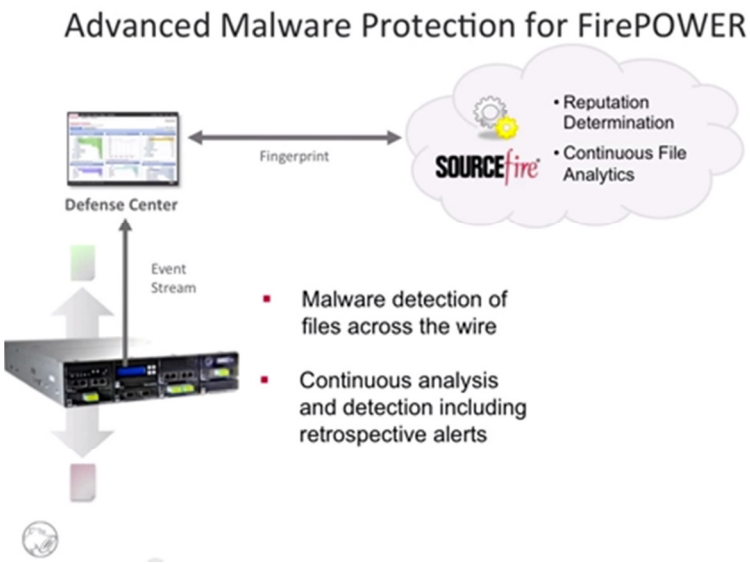
in functionality to Sourcefire's physical Defense Center management console", which can "correlate and prioritize event data with network and user awareness" and "aggregate[e] and analyz[e] security and compliance events from across the organization." See https://materials.proxyvote.com/Approved/83616T/20120404/AR_124967/PDF/sourcefire-ar2011_0015.pdf, Page 5. In particular, "[s]nort-based security alerts are generated at the sensor and forwarded to the DC. The DC evaluates each threat against RNA's asset data." See http://tinyurl.com/kqhlzdh. Furthermore, "[t]he Snort output system receives events from the event selector and processes them. It checks whether they match suppression and thresholding rules, and withholds processing of these rules if they do. If not, the events are logged or passed to other systems for remediation and response purposes." See http://www.imerja.com/files/file/White_Papers/Sourcefire/Snort%20Threat%20Prevention.pdf.

The Sourcefire Virtual Defense Center™ logs event information details:

SOURCEfire®

Direct integration into the Sourcefire Defense Center gives you contextual detail to any alert delivered by this popular IPS and Real-time Adaptive Security solution. With access to the full network payload, you can determine what happened before, during, and after any Sourcefire alert.

See http://soleranetworks.co.jp/ecosystem/integrations/. This information is then used for "Continuous File Analytics". See https://www.youtube.com/watch?v=OzptyVo5yFU&noredirect=1:



31. These instructions were made available by Cisco to its customers on Cisco's own cisco.com websites as specified in Paragraphs 27-30 above, and in making these instructions available, Cisco specifically intended to encourage its customers to follow these instructions to (1) assemble the Cisco Security Agent/IPS Collaborative Architecture, including Cisco Security Agent, Cisco Security Agent MC, and Cisco IPS and use same, and use (2) the Cisco ASA 5500-X Series Next-Generation Firewalls running Cisco ASA Next-Generation Firewall Services, including Intrusion Prevention System (IPS) and/or Cisco Prime Security Manager, (3) the Sourcefire Virtual Appliance; and (4) the Sourcefire Virtual Defense Center™, knowing that the assembly and use of these systems described in its instructions constituted infringement of the '444 Patent.

32. Thus, Cisco has induced its customers to infringe the '444 Patent literally and/or under the doctrine of equivalents. Upon information and belief, Cisco acted with the specific intent to induce its customers to use the methods claimed by the '444 Patent by continuing the above-mentioned activities with knowledge of the '444 Patent.

33. Selene has suffered and continues to suffer damages as a result of Cisco's infringement of Selene's '444 Patent. Pursuant to 35 U.S.C. § 284, Selene is entitled to recover damages from Cisco for its infringing acts in an amount subject to proof at trial, but no less than a reasonable royalty.

34. Cisco's infringement of Selene's '444 Patent has damaged and will continue to damage Selene, causing irreparable harm for which there is no adequate remedy at law, unless Cisco is enjoined by this Court.

PRAYER FOR RELIEF

Selene, respectfully requests the Court to enter judgment in its favor and against Cisco, granting the following relief:

A. Judgment in Plaintiff's favor that Cisco has infringed and continues to infringe, literally and/or under the doctrine of equivalents, directly and/or indirectly, the '444 Patent;

B. A permanent injunction enjoining Cisco and its officers, directors, agents, servants, affiliates, employees, divisions, branches, subsidiaries, parents, and all others acting in active concert therewith from infringement of the '444 Patent, or such other equitable relief the Court determines is warranted;

C. An award to Plaintiff of damages adequate to compensate it for Cisco's acts of patent infringement, but in no event less than a reasonable royalty, together with interest, costs, and expenses as fixed by the court pursuant to 35 U.S.C. § 284;

D. A judgment and order requiring Cisco to provide an accounting and to pay supplemental damages to Selene, including without limitation, pre-judgment and post-judgment interest; and

E. Any further relief to which Selene may be entitled.

JURY DEMAND

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

Date: February 1, 2014

Of Counsel:

Marc A. Fenster
Alexander C.D. Giza
Jeffrey Z.Y. Liao
RUSS, AUGUST & KABAT
12424 Wilshire Boulevard, 12th Floor
Los Angeles, CA 90025-1031
(310) 826-7474
mfenster@raklaw.com
agiza@raklaw.com
jliao@raklaw.com

BAYARD, P.A.

/s/ Stephen Brauerman

Richard D. Kirk (rk0922)
Stephen B. Brauerman (sb4952)
Vanessa R. Tiradentes (vt5398)
Sara E. Bussiere (sb5725)
222 Delaware Avenue, Suite 900
Wilmington, DE 19801
(302) 655-5000
rkirk@bayardlaw.com
sbrauerman@bayardlaw.com
vtiradentes@bayardlaw.com
sbussiere@bayardlaw.com

Counsel for Plaintiff
Selene Communication Technologies, LLC