IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

ROUTE1 INC., *Plaintiff,* *v.* AIRWATCH LLC, *Defendant.*	C.A. No: _____ **JURY TRIAL DEMANDED**

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Route1 Inc. ("Route1"), for its Complaint against Defendant AirWatch LLC ("AirWatch"), alleges as follows:

PARTIES, JURISDICTION AND VENUE

1. Plaintiff Route1 is a publicly-held Canadian corporation with its principal place of business at 8 King St. East, Suite 600, Toronto, Ontario M5C 1B5, Canada.

2. Defendant AirWatch is a Delaware Limited Liability Company with its principal place of business at 1155 Perimeter Center West, Suite 100, Atlanta, GA 30338 and its Registered Agent's address at 1209 Orange Street, Wilmington, Delaware 19801.

3. This action arises under the Patent Laws of the United States, 35 U.S.C. §§ 1 *et seq.* This Court has original subject matter jurisdiction over this action under 28 U.S.C. § 1338.

4. Venue is proper in this judicial district under 28 U.S.C. §§ 1391(b) and 1400(b) because Defendant is organized under the laws of Delaware and, on information and belief, is doing business in this District and has directed its infringing conduct into this District.

THE PATENT-IN-SUIT

5. U.S. Patent No. 7,814,216 (the "'216 Patent), titled "System And Method For Accessing Host Computer Via Remote Computer," was issued by the United States Patent and Trademark Office ("USPTO") on October 12, 2010. Route1 is the owner by assignment of the entire right, title and interest in the '216 Patent, including the sole and undivided right to sue for infringement. A copy of the '216 Patent is attached as Exhibit 1.

BACKGROUND FACTS

6. Route1's predecessor was founded in 2002 to develop secure data protection technologies and user authentication for government and businesses; specifically, enabling secure access from mobile remote devices to the entity's digital resources and sensitive data. Route1 provides its customers with a suite of hardware and software enterprise solutions that combines user authentication, data security and secure communications. The field in which Route1 operates is sometimes referred to as Enterprise Mobility Management ("EMM"). Route1's customers include the U.S. Department of Defense, the U.S. Department of the Navy, the U.S. Department of the Interior, the Canadian Human Rights Commission, The Financial Transactions and Reports Analysis Centre of Canada, and other government agencies. Route1's customers also include, among others, companies in the banking, healthcare, legal and education sectors.

7. Route1 has sought and obtained patent protection for its innovations in secure access by mobile devices to a host environment. The '216 Patent was filed on September 7, 2004, and issued on October 12, 2010. Route1 has other issued and pending patents, in the U.S. and in Canada.

8. AirWatch entered into the business of providing software and systems for secure remote data communications well after Route1 filed the application that matured into the '216 Patent. According to an interview of AirWatch's former Chairman in the June 2013 issue of *Georgia Trends* magazine, AirWatch was founded in 2003 as a company involved in setting up commercial Wi-Fi hot spots (a hot spot is a location that provides Wi-Fi service to usually transient customers), but in or after 2006 began moving into enterprise network management, and thereafter into EMM. AirWatch announced the launch of its EMM solution in a press release dated January 14, 2008.

AIRWATCH'S INFRINGING CONDUCT

9. Route1 incorporates by reference the allegations of paragraphs 1-8 of this Complaint.

10. The '216 Patent is generally directed to using a controller to enable secure communication between a remote device, such as a smartphone or a portable computer, and a host computer. The controller, remote and host are in different locations; the host is usually part of a customer's computer system. The method disclosed in the '216 Patent includes: the remote and the host validating their identities to the controller; the controller receiving, from the remote, a selection of a host; the controller sending characteristics of the remote to the selected host, along with an instruction to the selected host to establish a connection to the remote; and then the host and the remote communicate without using the controller to transport data.

11. Claim 1 of the '216 Patent recites:

> A method of enabling communication between a host and a remote device using a controller, comprising:
>
> connecting the controller to the host;
>
> connecting the controller to the remote device, the host and the remote device being in separate locations;

validating, at the controller, digital identity certificates received from each of the host and the remote device, each identity certificate containing (i) the public half of an asymmetric key algorithm key pair, (ii) identity information, and (iii) a digital signature of the issuing certificate authority, thereby converting the host to a validated host, and converting the remote device to a validated remote device;

receiving, at the controller, a selection of the host from the validated remote device;

sending parameters for the validated remote device from the controller to the selected host;

sending an instruction, from the controller to the selected host, to establish a connection to the remote device;

receiving, at the controller, notifications from the selected host and the validated remote device that a connection exists therebetween; and

after receiving notice of a connection between the selected host and the validated remote device refraining from involvement, at the controller, in transporting data between the selected host and the validated remote device, so that the selected host and the validated remote device subsequently communicate with each other without using any resource of the controller.

12. AirWatch infringes the ‘216 Patent in violation of 35 U.S.C. § 271 through at least the operation of a cloud-based controller of what it refers to as “The AirWatch Enterprise Mobility Management System” (herein, the “AirWatch EMM System”) in order to facilitate secure communications between remote computing devices such as cell phones and tablets and resources residing on corporate networks, such as email and corporate intranets, and application programs such as spreadsheets and word processors.

13. Publicly-available information, including, the following, provides evidence that an as yet unknown portion of AirWatch EMM System configurations infringe at least claim 1 of the ‘216 Patent through AirWatch’s operation of the AirWatch EMM System:

- AirWatch PoC Technical Architecture – A guide for selecting an AirWatch PoC Evaluation Architecture June 2013 (“PoC”), attached as Exhibit 2 and available at www.scribd.com/doc/285352246/AirWatch-PoC-Technical-Architecture.

- Georgia Enterprise Technology Services AirWatch MDM handbook, October 2014 ("GETS Handbook"), attached as Exhibit 3 and available at http://gta.georgia.gov/sites/gta.georgia.gov/files/related_files/site_page/AirWatch-MDM-Handbook-Oct2014.pdf.

- Introduction to the AirWatch Cloud Connector (ACC) Guide ("ACC Guide"), attached as Exhibit 4 and available at https://www.vodafone.de/downloadarea/AirWatch_Cloud_Connector_Installation.pdf

- AirWatch EMM Platform Architecture video ("AirWatch EMM Architecture video"), transcription attached as Exhibit 5 and video available at airwatch.com/resources/videos/.

- U.S. Patent No. 8,713,646 (Stuntebeck) (the "AirWatch '646 Patent"), attached as Exhibit 6, and identified on a virtual patent marking web page hosted by AirWatch's parent company VMware, Inc., thus constituting a representation under 35 U.S.C. § 287 that AirWatch practices that patent.

14. In particular, AirWatch, via the AirWatch EMM System, practices each step of the method covered by claim 1 of the '216 Patent in at least the following way through the operation of a cloud-based server referred to as the AirWatch SaaS Cloud, alone or in combination with other devices (herein, the "AirWatch SaaS Cloud"):

- The AirWatch SaaS Cloud connects to both the customer's remote computing device and the customer's computer network. PoC at, e.g., 10, 13, 16, 19 (Network Requirements charts describing connections between AirWatch SAAS and internal network server as well as remote computing device). The AirWatch SaaS Cloud, the customer's remote computing device and the customer's computer network validate their

identities to each other using Public Key Infrastructure ("PKI") encryption algorithms. PoC page 6. PKI encryption relies on digital identity certificates containing the public half of an asymmetric key algorithm key pair, identity information, and a digital signature of the issuing certificate authority. Route1 '216 Patent, column 3, lines 4-26.

- AirWatch SaaS Cloud receives a request from the customer's remote computing device to access the customer's computer network. PoC at, e.g., 8, 11, 14, 17 (diagrams showing communications from remote computing device to AirWatch SaaS Cloud); AirWatch '646 Patent at, e.g., Fig. 1: 136; Fig. 2: 203; sentence bridging columns 6-7.

- AirWatch SaaS Cloud routes identity information for the customer's remote computing device to the customer's computer network, along with an instruction to connect. AirWatch '646 Patent at, e.g., Fig. 1: 133; Fig. 2:223; column 7, lines 51-55.

- The customer's remote computing device and computer network provide the AirWatch SaaS Cloud with notice of a connection therebetween by transmitting event information to AirWatch SaaS Cloud which, on information and belief, includes the event of the customer's computer network transmitting data to the remote computing device, and the event of the remote computing device receiving data from the customer's computer network. PoC at, e.g., 11, 14, 17 (diagrams showing mobile device management (MDM) data sent from remote computing device to AirWatch SaaS Cloud); GETS Handbook at 4 (AirWatch system administrator has the ability to view, on their console, real-time data such as amount of data transferred to and from the remote computing device); ACC Guide at 1 (SysLog (internal event log data) integrated to ACC, which is in communication with the AirWatch SaaS Cloud).

- After the communications channel is established, the customer's remote computing device and computer network communicate without using any resource of AirWatch SaaS Cloud. AirWatch EMM Architecture video transcription, fifth sentence ("Your policies and configurations are stored securely in the AirWatch SaaS Cloud while device data such as email and VPN traffic are separated and connect directly to your IT infrastructure."); AirWatch '646 Patent column 6, lines 56-58 and column 7, lines 62-64.

CLAIM FOR RELIEF – PATENT INFRINGEMENT
UNDER 35 U.S.C. § 271 OF U.S. PATENT NO. 7,814,216

15. Route1 incorporates by reference the allegations of paragraphs 1-14 of this Complaint.

16. In view of the foregoing, AirWatch infringes the '216 Patent in violation of 35 U.S.C. § 271(a).

17. Route1 has at all relevant times been in compliance with 35 U.S.C. § 287 to the extent applicable.

18. AirWatch will continue its acts of infringement unless and until enjoined by this Court.

19. AirWatch's infringement has caused and, unless enjoined by this Court, will continue to cause serious and irreparable damage to Route1 for which Route1 has no adequate remedy at law.

20. AirWatch's infringement has also caused monetary damage to Route1 for which Route1 is entitled to be compensated by Defendant.

WHEREFORE, Route1 prays:

a) that Defendant be found to have infringed the '216 Patent;

b) that Defendant, its officers, directors, employees, agents, and affiliated entities, and all other parties in active participation or privity with them, be preliminarily and permanently enjoined from infringing the '216 Patent;

c) that Defendant be ordered to pay Route1 damages adequate to compensate it for the infringement described in this Complaint; and

d) that Route1 have such other and further relief as this Court may deem just and proper.

JURY DEMAND

Pursuant to Federal Rule of Civil Procedure 38(b) and District of Delaware Local Rule 38.1, Plaintiff Route1 Inc. demands trial by jury for all claims and issues thus triable by right.

Dated: March 27, 2017

Of Counsel:

Michael J. Garvin
Marcel C. Duhamel
Aaron M. Williams
VORYS, SATER, SEYMOUR
AND PEASE LLP
200 Public Square, Suite 1400
Cleveland, Ohio 44114
(216) 479-6100 Phone

William H. Oldach III
VORYS, SATER, SEYMOUR
AND PEASE LLP
1909 K Street N.W., 9th Floor
Washington, DC 20006
(202) 467-8800 Phone

HEYMAN ENERIO
GATTUSO & HIRZEL LLP

/s/ *Dominick T. Gattuso*
Dominick T. Gattuso (# 3630)
300 Delaware Ave., Suite 200
Wilmington, DE 19801
(302) 472-7300
dgattuso@hegh.law

Attorneys for Plaintiff
Route1 Inc.