IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

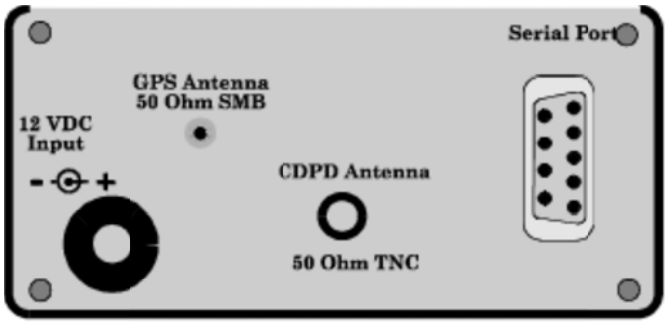
M2M SOLUTIONS LLC, a Delaware limited liability company, Plaintiff, v. MOTOROLA SOLUTIONS, INC., a Delaware corporation, TELIT COMMUNICATIONS PLC, a United Kingdom public limited company, and TELIT WIRELESS SOLUTIONS INC., a Delaware corporation, Defendants.	**C.A. No. 12-033-RGA**

EXPERT REPORT OF KIMMO SAVOLAINEN ON THE INVALIDITY OF U.S. PATENT NO. 8,094,010

I have been retained by Telit Communications PLC ("Telit PLC") and Telit Wireless Solutions Inc. ("Telit Wireless") (collectively with Telit PLC, "Telit"), Motorola Solutions, Inc. and Kowatec Corporation ("Kowatec") to serve as an expert in this lawsuit. I expect to testify at trial regarding the matters discussed in this report if asked about them by the Court or the parties' attorneys.[1]

[1] This report constitutes notice under 35 U.S.C. §282. Defendants reserve the right to rely on prior art, invalidity contentions or information contained in the expert reports submitted by other defendants against which M2M asserted the '010 Patent.

U.S. Patent No. 8,094,010 Claims	Hotlink patent application
	would have been obvious to add incoming call screening as described in the GSM standard. Further, it would have been dangerous, and would undermine the concept of call screening, to allow a stranger to program or change the allowed numbers. Therefore, it would have been obvious to modify the device to authenticate anyone trying to change the allowed caller numbers.
a memory module for storing the at least one telephone number or IP address from the authenticated transmission as one of one or more permitted callers if the processing module authenticates the at least one transmission by determining that the at least one transmission includes the coded number; and	"[T]he hot link communicator is able to select one of a plurality of numbers stored in the preprogrammed identity module. This can be realised [sic] in a number of ways such as programming the call initiate button 14 to toggle through the list of stored numbers wherein each is sequentially displayed on the screen." (Ex. 15, 0409, ll. 26-31). E. Wesby admitted that the Hotlink "include[d] a simple programming feature which was to populate a permitted callers list." (Ex. 50, EW Tr. Aug. 14, 2012 at 25:10-11). Further, E. Wesby admitted that a permitted caller list is "essentially a list of phone numbers to which that communicator is permitted to communicate, *whether it is for receiving a call from that number or to make a call to that number*." (Ex. 50, EW Tr. Aug. 14, 2012 at 25:14-16, emphasis added). These admissions confirm my view that there was no significant difference between restricting incoming or outgoing calls. In fact, the same +CLCK command was used for both (see facilities FD for outgoing and NT-NA for incoming at Ex. 20, 6474-5). The decision to restrict incoming calls, outgoing calls, or both was application dependent, and was easy to implement by any competent engineer.
wherein the at least one transmission from a programmable transmitter comprises a Short Message Service	The '010 Patent admitted that it would have been obvious to use SMS for communicating with the Hotlink: "Existing and known methods of



PinPoint Rear Panel

78. "Hardware flow control" of the serial port was programmable to be turned on (2) or off (0) (Ex. 17, 4119). Hardware flow control enables the Raven to control the flow of data over the serial port from the monitored technical devices. Raven disclosed programming the hardware flow control over the serial port using AT command AT\Q0 (Ex. 17, 4119) or wirelessly using the Wireless Ace (Ex. 17, 4150, 4116). AT&C and AT&D also control the flow of data over the serial port (Ex. 20, 6447). M2M asserted that these were programmable interface commands (e.g., see Ex. 47, Second Supplemental Preliminary Infringement Contention Claim Chart against Telit Nov. 18, 2013, for the claim element 1c, GE863-QUAD/GPS module, pp. 1-2; Ex. 48, First Supplemental Preliminary Infringement Contention Claim Chart against Kowatec, April 8, 2013, for element 1c, SIM5200 Series wireless modules, p. 3). All of these commands control the flow of data through the serial port.

ii. Permitted Caller

79. The Raven has three modes of operation: "command mode" for programming the modem, "data mode" for sending outgoing data packets and receiving incoming data packets, and "half open mode" for switching in and out of command mode in response to incoming data packets (Ex. 17, 4108). In half open mode, if the destination IP address was set to 0.0.0.0, the

CDPD modem could receive data packets from any destination IP address (Ex. 17, 4112). The incoming data packets include the destination IP address of the sending device (i.e., "the source address") (Ex. 17, 4108). When the modem received its first incoming packet from a destination IP address, the modem "locks onto" that destination until a timer expires (Ex. 17, 4112). During the lockout period, the modem is "locked onto" and therefore could only receive incoming data packets from that destination IP address, i.e., a "permitted caller" (Ex. 17, 4112). To lock onto the destination IP address for a period of time (the duration of the half-open timer), the IP address must be stored for at least that period of time.

iii. Authentication

80. Raven disclosed programming the modem to operate in half-open mode using a "Wireless Ace" (AirLink Configuration Executive) (Ex. 17, 4112). The Wireless ACE required that a password is authenticated to program the modem: "When you have changed a parameter in your modem, using ACE, and click on Write to Modem, you will be prompted for a password. The default password is 12345. You need to change the password to your modem. Passwords can be case sensitive and include numbers. Use Options → Change Modem Password ... or Ctrl-H. The password can be up to eight characters in length." (Ex. 17, 4104). To the extent that M2M asserted a 4-digit password is unique,[6] Raven's eight-character password must also be unique. Regardless, a person or ordinary skill in the art would have understood that an eight-digit password designated to be changed by a user was meant to be personalized to be a unique

[6] I have been informed that M2M asserts that the password identified in its infringement contentions against Kowatec, PIN2 (e.g., see Ex. 48, p. 3), is a "'coded number' as construed by the Court" i.e. that the PIN2 is "unique" (Ex. 49, TELIT0068277). The PIN2 password is a 4-digit number (e.g., see Ex. 20, 6490).

number. Additionally, it would have been obvious as a matter of design choice to require a unique password to increase the security of the device.

iv. Wireless Programming

81. The Wireless Ace programmed the modem wirelessly: "with our Windows application Wireless ACE, you can see the status and configure the modem both locally via the serial cable *or remotely from the network*" (Ex. 17, 4116, emphasis added). Therefore, the password would have been sent over the CDPD network, which is cellular (wireless), as a packet-switched (CDPD) transmission.

82. The attached Appendix C shows the correspondence between Raven (Ex. 17) and the Asserted Claims of the '010 Patent. For these reasons, in my opinion, the Asserted Claims of the '010 Patent were anticipated by and/or would have been obvious over Raven and are invalid.

D. The Asserted Claims Were Anticipated By and/or Obvious Over GSM 11.14

83. GSM is the "Global System for Mobile Communication" that was developed in the 1980s. GSM 11.14 version 7.3.0 dated July 1999 (Ex. 18) described the SIM Application toolkit. GSM 11.14 incorporated by reference, for example:

- "the commands and protocols relevant to the SIM Application Toolkit in GSM 11.11" (Ex. 18, 6118), the "Proactive SIM" (Ex. 18, 6122), and "proactive command" (Ex. 18, 6125) of GSM 11.11 (Ex. 19).
- the AT commands of GSM 07.07 at Ex. 18, 6191, 6140. See GSM 07.07, Ex. 20.
- the security features of GSM 03.48 at Ex. 18, 6195. See GSM 03.48, Ex. 22.
- The SMS interface of GSM 07.05 at Ex. 18, 6116. See GSM 07.05, Ex. 21.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.