Defendant's Invalidity Contentions
Exhibit H3

Invalidity of U.S. Patent No. 10,212,586
by
U.S. Patent No. 7,941,534 to de la Huerga ("de la Huerga '534")

The excerpts cited herein are exemplary. For any claim limitation, Defendant may rely on excerpts cited for any other limitation and/or additional excerpts not set forth fully herein to the extent necessary to provide a more comprehensive explanation for a reference's disclosure of a limitation. Where an excerpt refers to or discusses a figure or figure items, that figure and any additional descriptions of that figure should be understood to be incorporated by reference as if set forth fully therein.

Except where specifically noted otherwise, this chart applies the apparent constructions of claim terms as used by Plaintiff in its infringement contentions; such use, however, does not imply that Defendant adopts or agrees with Plaintiff's constructions in any way.

U.S. Patent No. 10,212,586 ("the '586 Patent") claims priority to Japanese Application No. 2012-117105, filed May 23, 2012. For purposes of these invalidity contentions, Defendant applies the May 23, 2012, priority date for the '586 Patent. However, Defendant reserves the right to contest Plaintiff's reliance on the May 23, 2012, priority date, should the priority date become an issue in this proceeding.

De la Huerga '534 was filed on June 26, 2004 and was published on April 28, 2005. As such, de la Huerga '534 qualifies as prior art with regard to the '586 patent under 35 U.S.C. § 102(a), 102(b) and 102(e). Alternatively, should the claims of the '586 patent be found to not be entitled to priority to the foreign filing date, de la Huerga '534 qualifies as prior art under §§ 102(a)(1) and 102(a)(2) (post-AIA). Using Plaintiff's interpretation of the claims, de la Huerga '534 anticipates claims 1-2, 6-7, 9-10, 13-14, and 16-18 under 35 U.S.C. § 102(a), (b) and (e).

Alternatively, de la Huerga '534 renders obvious claims 1-2, 6-7, 9-10, 13-14, and 16-18 under 35 U.S.C. § 103(a).

Alternatively, de la Huerga '534 in view of U.S. Patent Application Publication No. 2006/0041746 to Kirkup, et al. ("Kirkup '746") renders obvious claims 1-2, 6-7, 9-10, 13-14, and 16-18 under 35 U.S.C. § 103(a). Kirkup '746 was filed on August 17, 2004 and published on Feb 23, 2006. As such, Kirkup '746 qualifies as prior art with regard to the '586 patent under 35 U.S.C. §§ 102(a), 102(b), and 102(e).

Alternatively, de la Huerga '534 in view of U.S. Patent No. 6,871,063 to Schiffer ("Schiffer '063") renders obvious claims 1-2, 6-7, 9-10, 13-14, and 16-18 under 35 U.S.C. § 103(a). Schiffer '063 was filed on Jun 20, 2000 and issued on March 22, 2005. As such, Schiffer '063 qualifies as prior art with regard to the '586 patent under 35 U.S.C. § 102(a), 102(b) and 102(e).

Alternatively, Kirkup '746 in view of U.S. Patent No. 8,149,089 to Lin ("Lin '089") renders obvious claims 1-2, 6-7, 9-10, 13-14, and 16-18 under 35 U.S.C. § 103(a). Lin '089 was filed on November 21, 2008 and issued on April 3, 2012. As such, Lin '089 qualifies as prior art with regard to the '586 Patent under 35 U.S.C. § 102(a) and 102(e).

U.S. Patent No. 10,212,586	de la Huerga '534
Claim 1	
[1(pre)]A mobile terminal configured to switch between an unlocked state and a locked state in which a predetermined operation is limited, comprising:	To the extent the preamble is limiting, de la Huerga '534 teaches an electronic security device that can take the form of a cell phone (a mobile terminal): *As before, security device 10 can be in the form [of a] security badge or a cell phone or PDA or other convenient shape that is typically worn or held by an employee of an enterprise, henceforth referred to as computer user.* de la Huerga '534 at 65:47-51. De la Huerga '534's mobile terminal can be unlocked or locked (where the function of authenticating the user to other devices is disabled): *In an initial or basic version, the user has an electronic security device and authenticates himself according to the standard computer security protocol, e.g. a user name and password, biometric indicia, or by using codes in the electronic device itself.* *Id.* at 12:8-12. This authentication of the user to security device 10 is distinct from unlocking and unlocking other devices: *Where device authentication protocol information 1153 is used to authenticate a user to security device 10, system authentication protocol 1165 is used to authenticate security device (and therefore its user or owner) to computer system 194.* *Id.* at 67:17-21.
[1(a)] a transceiver which performs short-range wireless communications;	De la Huerga '534's security device 10 includes "communications transceiver 14":

	Device 10 includes a processor 250 linked to memory 262, activation button 18, indicator 20 (e.g. a LED or speaker), wireless communication transceiver 14, power source (e.g. a battery, photocell, or fuel cell or magnetic field induced power source), and an optional biometric indicia sensor 405 (e.g. a fingerprint sensor placed on the back of device 10). In some cases a small key pad (e.g. buttons 207, 209, 211, 213, and 215 or others) is also provided and display 258 can be provided as a graphic display, e.g. a LCD. de la Huerga '534 at 65:53-62. De la Huerga '534 characterizes the transmission range of security device 10 as three meters ("3 m"): *Transceiver 14 can be under control of processor 250 to repeatedly broadcast device identifier 1148 (or other message) when it is not in communication with a specific terminal 60. This can also be instigated by pressing activation button 18. When the user with device 10 approaches within communication range (e.g. 3 m) of terminal 60, transceiver 64 will receive identifier 1148."* *Id*. at 69:23-29. De la Huerga '534 further characterizes this as "limited range" communication: *When the electronic device has wireless communication it can be used to log the user onto the computer system. This can be done by pressing an activation button on the device, which then transmits the reauthentication code and other user information as needed within a limited range.* *Id.* at 12:53-57
[1(b)] a memory which previously stores information about an another mobile terminal; and	De la Huerga '534 teaches that security device 10 stores information about other computer devices it can unlock: *In some cases the electronic security device can include an address of one or more trusted computer systems or servers.* de la Huerga '534 at 15:3-4.

	These computer devices can include mobile devices (e.g., patient monitoring devices) to which the user may authenticate ("mobile terminals"): *System 194 includes a plurality of personal computers or computer terminals comprising workstations 60 and 60', which may be located in patient rooms, at nurse stations, in doctor offices and administrative offices, a plurality of network devices including databases 158 and 162 and servers including an Admit, Discharge, and Transfer system or server 166, at least one laboratory system or server 170, various bedside treatment devices 116 and 116' such as ventilators and IV infusion pumps, patient monitoring devices 80 and 80', a pharmacy system or server 186, a security verification system or server 168, a billing system or server 171, a patient historical records system or server 173 and a unit dose medication dispenser 150."* *Id.* at 20:1-15 (parentheticals omitted). De la Huerga '534 further contemplates mobile terminals including patient bracelets (*see* FIG. 2) and locking pill containers (FIG. 5): *The other devices include two smart devices including a patient monitor 80' and a patient treatment device 116', each equipped with a wireless transceiver input device 64 which is similar to transceiver 81' on band 40 (see FIG. 2) and transceiver 81' on container 200 (see FIG. 5)* *Id.* at 24:1-5; *see also* FIGs. 2, 5:

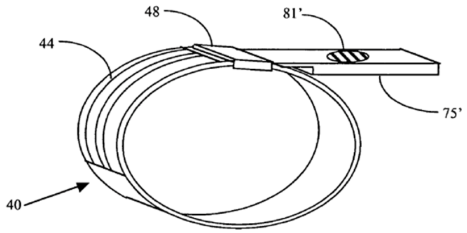

Figure 2

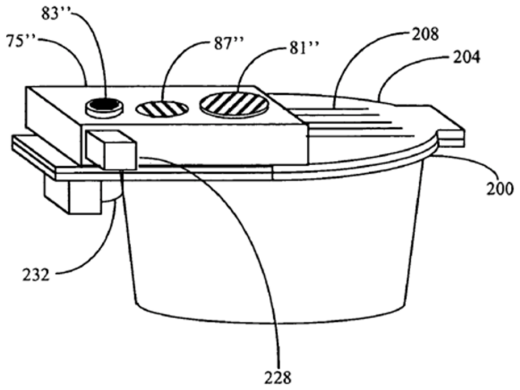

Figure 5

Furthermore, de la Huerga '534 disparages the prior art as not being suitable for portable devices:

> *This [prior art] system is primarily directed to accessing desktop computer terminals on a sensitive computer network and is not easily adaptable, however, for restricting access to laptops, portable instruments, medical equipment such as respirators, or electronically-controlled medication dispensers.*

Id. at 11:38-42.

Additionally, Schiffer '063 teaches this limitation. Schiffer '063 teaches that mobile phone 100 includes "SIM 101" (*see* FIG. 1, *supra*), which in turn includes a "protected memory region having data stored therein":

> *SIM 101 of FIG. 1 includes a protected memory region having data stored therein. A protected memory region is a memory region that is not generally modifiable by typical users. Thus, important information may be securely stored in the protected memory region of SIM 101 with a low risk of being compromised. The data stored in the protected memory region of SIM 101 includes the subscriber identity number associated with the user of mobile phone 100.*

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.