Defendant's Invalidity Contentions
Exhibit H1

Invalidity of U.S. Patent No. 10,212,586
by
U.S. Patent No. 6,871,063 to Schiffer ("Schiffer '063")

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.

Schiffer '063 was filed on June 30, 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, should the claims of the '586 patent be found to not be entitled to priority to the foreign filing date, Schiffer '063 qualifies as prior art under §§ 102(a)(1) and 102(a)(2) (post-AIA). Using Plaintiff's interpretation of the claims, Schiffer '063 anticipates claims 1-2, 6-7, 9-10, 13-14, and 16-18 under 35 U.S.C. § 102(a), (b) and (e).

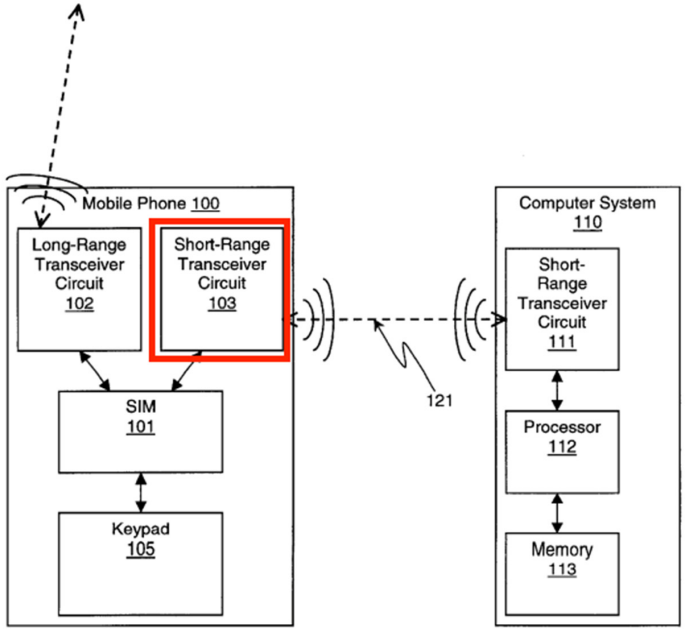
Alternatively, Schiffer '063 renders obvious claims 1-2, 6-7, 9-10, 13-14, and 16-18 under 35 U.S.C. § 103(a).

Alternatively, Schiffer '063 in view of U.S. Patent No. 7,941,534 to de la Huerga ("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). 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, Schiffer '063 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, Schiffer '063 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	**Schiffer '063**
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, Schiffer '063 teaches "mobile phone 100" (mobile terminal): *Mobile phone 100 of FIG. 1 may be any mobile phone capable of long-range communication. For example, for one embodiment, mobile phone 100 is a cellular phone, in which case long-range transceiver circuit 102 may communicate with a cell base.* Schiffer '063 at 2:30-34. Schiffer '063's mobile phone 100 is configured to be unlocked or locked (in which case the ability of the phone to send and receive calls is limited): *In accordance with one embodiment of the present invention, before step 200 of FIG. 2 a user may authenticate him or herself to their mobile phone. Authentication of a user to the mobile phone may be accomplished by, for example, the user entering a password onto keypad 105 of mobile phone 100 of FIG. 1. This password may then be compared to information stored in the protected memory region of SIM 101 to verify the password. If the password is verified, mobile phone 100 may then be unlocked. Unlocking the phone enables the phone to send and receive calls via long-range transceiver circuit 102, exchange information via short-range transceiver circuit 103, and allows the user to modify phone settings via keypad 105. Alternatively, authentication of the user by the mobile phone may include performing voice recognition of the user.* Schiffer '063 at 3:23-37.
[1(a)] a transceiver which performs short-range wireless communications;	Schiffer '063 teaches that mobile phone 100 includes "short-range transceiver circuit 103." *See* FIG. 1, *infra.* This short-range transceiver circuit is characterized as establishing a short-range, wireless communication link: *Consequently, a short-range, wireless communication link, 121, is established between computer system 110 and mobile phone 100, according to step 205. In accordance with one*

	embodiment of the present invention, this short-range, wireless communication link is a Bluetooth link, and the short-range, wireless communication range is the range of the Bluetooth wireless network. Schiffer '063 at 3:42-49.  **Figure 1**
[1(b)] a memory which previously stores information about an another mobile terminal; and	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. Schiffer '063 at 2:38-45. Schiffer '063 further discloses that this SIM may store data including an "access code" (or data used to generate the access code) for computer system 110: *In response, the mobile phone transmits an access code back to the computer system via the link. This access code is generated using data stored in the SIM in the mobile phone. After the computer system verifies the access code, access to the computer system is granted in response to receiving the access code.* *Id.* at 2:7-13. In some embodiments, the access code is an "alternate value" stored in the SIM and encrypted using the subscriber identity number: *The access code transmitted from mobile phone 100 to computer system 110 via short-range, wireless communication link 121 of FIG. 1 is generated by mobile phone 100 using data stored in SIM 101. For one embodiment of the present invention, this data includes the subscriber identity number stored in the protected memory region of SIM 101. For added security, the access code may be encrypted by mobile phone 100 before being transmitted. The algorithm used to encrypt the access code may use data stored in SIM 101. For one embodiment, the access code is all or some portion of the subscriber identity number itself. For another embodiment, the access code may be an alternate value that may be encrypted using all or some portion of the subscriber identity number as an encryption key.* *Id.* at 4:23-36. This "alternate value" (once decrypted) may be a "security code" previously stored in computer system 110 by the user: *For one embodiment of the present invention, the access code may be decrypted by computer system 110 before being verified. Verification may include comparing the access code to a previously stored value to detect a match or other predetermined relationship. The previously stored value may be stored in a protected memory region of memory 113, such as the BIOS. This previously stored value may be entered by the user upon initially setting up an authentication system in accordance with the present invention. This previously stored value*

	may include, for example, the subscriber identity number, or some portion thereof, or other security code. Thus, mobile phone 100 stores the "security code" in the memory of its SIM, and the security code is "information about" computer system 110 by virtue of having been stored as the access code for computer system 110 by the user. Finally, Schiffer '063 discloses that computer systems (such as computer system 110) may be a "small handheld electronic device" or a "mobile" system: *Computer systems, from small handheld electronic devices to medium-sized mobile and desktop systems to large servers and workstations, are becoming increasingly pervasive in our society. As such, people are becoming more reliant on computer systems to store and access information, much of which may be confidential. To maintain the confidentiality of this information, some computer systems may be voluntarily "locked" or "secured" by a user. When a computer system is locked, access to the computer system may be limited. This not only serves to maintain the confidentiality of information stored on the computer system but also deters theft of the computer system.* Schiffer '063 at 1:11-22. Alternatively, de la Huerga '534 teaches this limitation. 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*

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.