Exhib

U.S. Patent No. 5,892,906 to Wayne W. Chou et al. ("Chou")

U.S. Patent No. 5,892,906 to Wayne W. Chou et al. ("Chou") anticipates and/or renders obvious, at least under Ancora's appa infringement theories, the claims as detailed below of U.S. Patent No. 6,411,941 (the "'941 Patent") under at least 35 U.S.C. § 102(and 103. Chou was filed on July 19, 1996, and issued on April 6, 1999, and is therefore prior art to the '941 Patent.

Nothing stated in this chart shall be treated as an admission or suggestion that Defendants agree with Ancora regarding either the s of any of the asserted claims or the claim constructions advanced by Ancora in its infringement contentions, or that Defendants' acc products meet any limitations of the claims.

The chart below provides representative examples of where each element of each claim is found within Chou, at least under Anco apparent construction of the claims as applied in Ancora's infringement contentions. The cited evidence is merely illustrative, Defendants reserve the right to cite alternative or additional evidence.

To the extent that Ancora contends that Chou does not disclose one or more limitations of the claims, it would have been obviou combine the teachings of Chou with: (1) the knowledge of one of ordinary skill in the art to show all the limitations of the claims; (2 teachings of the prior art references set forth in Defendants' other invalidity charts with respect to the one or more limitations; an (3) the teachings of any of the prior art references cited and discussed in the cover document of Defendants' invalidity contention cited below for the one or more limitations.

Because Ancora has yet to identify any limitation of the asserted claims that it contends is not fully disclosed by Chou, either alon in combination with other prior art cited by Defendants, Defendants expressly reserve the right to rebut any such contention, inclu by identifying additional obviousness combinations, if any such contention is made by Ancora.

Where the chart below states that Chou "discloses" a limitation, such disclosure may be express, inherent or obvious to one of ordi skill in the art based on Chou.

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

'941 Patent Claim Limitation	U.S. Patent No. 5,892,906 to Paul C. Chou et al. ("Chou")
1[preamble]: A method of restricting software operation within a license for use with a computer including an erasable, non-volatile memory area of a BIOS of the computer, and a volatile memory area; the method comprising the steps of:	Chou discloses and/or renders obvious this limitation. See, e.g., "In accordance with one embodiment of the invention, when the computer is in the locke state, the external memory must be operatively connected to the computer each time th computer is booted up. If the user removes the external memory, or inadvertently forgets attach it to the computer, the security function will halt complete execution of the BIO routines. In another embodiment of the invention, the locked state requires the user to manually ent the password through the keyboard in response to a prompt during execution of the BIO routine. The security function compares a unique, user defined password stored in the BIO memory to the user supplied password. If the two passwords agree, the computer complet execution of the BIOS routine." 2:33-47 "During the execution of the normal BIOS routines within the BIOS memory 15 of FIG. the contents of memory location 30 are checked and if the contents of memory location 3 of the CMOS RAM 17 indicate a locked condition, the POST routine 23 will stop executio before the BOOT routine 22 can be executed, and enter the security routine 25. Once in th security 25 routine, the security routine attempts to read the contents of the security ke ROM 19 connected to the serial port 16. If security key 19 is connected to serial port 16, th unique key serial number and encrypted product M are read. The security function forms product of the read serial number and the computer I.D. 28 stored in BIOS EEPROM 1 The security function 25 decrypts the second encrypted value M read from security key 1 and compares it with the computed product. If a match is produced by the comparison, th computer goes on to execute the BOOT codes 22 and peripheral routines 21." 4:42-58. "FIG. 5 illustrates the step-by-step process for executing the security function 25 as well a locking and unlocking the computer in accordance with the preferred embodiment. In ste 40 the user attaches the key containing the ROM 19 to the serial port 16 of the compute The computer is rebooted in step 41 through a software reboot command.

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

'941 Patent Claim Limitation	U.S. Patent No. 5,892,906 to Paul C. Chou et al. ("Chou")
	Any subsequent operation of the computer requiring the computer to be rebooted can onl occur after the user attaches the key having ROM 19 to serial port 16 as shown in step 4 unless the user enters the unlocked state. After completing the POST routine 42, the BIO routine examines the contents of CMOS RAM 17 in step 43, and enters the security routin 25 if the computer 10 was not previously set in the unlocked state as is determined in decisio block 44. The computer will be in the lock state if it has not previously been specifically set in th unlocked state. If the external ROM 19 is not connected as determined in decision 45, message is posted to the user "CONNECT KEY". The security routines are executed in ste 46, by first reading the contents of the ROM of the key 19 attached to serial port 16. Th ROM contains two values, an unencrypted serial number unique to the key, and an encrypte value M which represents the product of the serial number of the key and the computer I.D number. A decryption subroutine is entered in step 48, which using the public key 29 store within the BIOS memory 15, decrypts the value of the product M. The security routines the reads, in step 49, the computer I.D. from location 28 of the BIOS memory 15. A product calculated in step 50, between the read serial number from the attached key 19, and th computer I.D. 28 obtained from the BIOS memory 15. The two products are compared in decision block 51 and if a match occurs, then the user ha been verified as possessing the connect key and is authorized to use the computer. Th remaining boot code is executed in steps 53 and the peripheral routines are executed in ste 54. This represents the completion of the BIOS routine execution, permitting the user operate the computer in the normal way. In the event the comparison is not obtained decision block 51, the boot up process is stopped in step 52 inhibiting any further use of th computer." 5:21-62. "FIG. 10 illustrates, in flow chart form, execution of the BIOS routines including the securit function. At the user site, the user first executes a boot up command in step 101 for enterin one or two passwords which he will use. The POST Routine is executed in step 102. As n passwords exists within the BIOS EEPROM memory 15(a) as determined in 103, the boo up process completes by executing the remaining BIOS routines in step 104. Followin

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

'941 Patent Claim Limitation	U.S. Patent No. 5,892,906 to Paul C. Chou et al. ("Chou")
	completion of the boot up process the user may enter a SETUP mode 105 common operating system configurations. The security administration mode 106 is selected by th user from the SETUP mode menu, which includes several submenu items. If the setup mod is not selected, the boot up ends in step 106. The new PASSWORD menu item is selecte by the user in step 107 from the administration function 106. The user may enter one or tw passwords in step 108 and the security function routine will store the password in step 10 in the BIOS EEPROM memory 15(a). This feature also permits new passwords to be entere in place of any two previously entered passwords. If a single password has been entered into the BIOS EEPROM 15A, a subsequent boot u and selection of the security administration mode will require use of the single passwor An additional password may be entered into the system by the first user, from the same men selection from the security administration mode. If the user wishes to lock or unlock the computer and enter the SETUP mode in step 105, h enters the security administration mode in step 106 again. One of the menu items provide in the security administration mode is a lock state 112, as well as an unlock state 113. B selecting the lock state 112 each subsequent boot up of the computer 10 will request password verification from the user. The selection of the lock state clears the memor location 30(a) of the CMOS RAM 17(a). The BIOS routine will therefore encounter th default value in location 30(a) during each subsequent execution in step 115 and decisio block 116 will require that the BIOS function execute the security function. Execution of the security function in step 118 will generate a prompt to enter the passwor in step 119. The user enters a password which is verified in decision block 120 by th security function and the boot up process completes execution in step 104. The computer 10 may be unlocked by returning to the security administration mode an selecting the appropriate unlock submenu item 113. Selecting the unlocked state will wri a unlock code at location 30(a) of the CMOS RAM 17(a) in step 123. Subsequent boot u

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

'941 Patent Claim Limitation	U.S. Patent No. 5,892,906 to Paul C. Chou et al. ("Chou")
	processes will check the contents of location 30(a) of CMOS RAM 17(a) in decision bloc 116 and skip the security function. The embodiment provides an emergency mode such that the user can enter th administration mode without entering either one of the user selected passwords, if he ha access to the digital signature supplied with the computer. The user, instead of entering password, enters the encrypted signature supplied to him in step 119. The public key store within the BIOS memory 15A decrypts the entered digital signature, to a value equal to th computer serial number. This signature is verified by the BIOS security function in decisio block 124, by comparing it to the computer serial number stored within the BIOS EEPRO 15A. The administration mode may then be entered in step 106 which provides for a men selection of either selecting a new password. Entry and storage of the new password ar effected as in the original password registration. If the decrypted signature and stored computer serial number do not match, execution ste in step 125, and a message is displayed in step 126 "INCORRECT PASSWORD"." 8:4 9:44. "Referring now to FIG. 1, a general organization of a personal computer 10 is shown whic includes a security function stored as a programming routine within the BIOS EEPROM 1 As will be evident with respect to the description of this embodiment, the BIOS routine which provide for the basic input/output system cannot be completely executed unless th security function is successfully executed. As will be understood by those familiar with the architecture of a personal computer, a CP 14, a CMOS RAM 17, and the BIOS memory is supported on a mother board which permi upgrades to be made to the system. A serial port 16 permits the computer 10 to communicat with externally connected devices. A monitor 11 and keyboard 13 provide a user interfac with the personal computer 10. In accordance with the preferred embodiment of the present invention, a memory devic such as a detachable read only memory (ROM), 19 shown in FIG. 2 having nine pi

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

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.