EXHIBIT A

Ancora Technologies First Supplemental Infringement Conte
With Respect To U.S. Patent No. 6,411,941

Claim Element of the '941 Patent	iOS Devices
1. 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:	For devices operating on the iOS platform ("iOS devices"), Appl procedure that restricts non-verified programs from operating. (ANC 902, 925, 937.) The secure boot procedure includes: a Secure Boo Bootloader (LLB) and an iBoot. (ANCA 854-960.) Devices operatin are designed to include: (1) volatile RAM memory (*e.g.*, ANCA 875, 0067); (2) non-volatile, erasable memory such as Read Only Mem memory (*e.g.*, ANCA 875, ¶ 0083; ANCA 921-9222, ¶0067 & ¶ 0068 (*See also*, ANCA 756-787, 788-789, 880, 994, 926) The volatile me memory "may store firmware for the [iOS device], such as a basi (BIOS)." (ANCC 1027 ¶0080) The secure booting procedure is allege (1) manufacture of an iOS device and (2) recovery, update and/or re iOS device. (ANCA 916.) (APL10102-10117)
selecting a program residing in the volatile memory,	Kernel cache is loaded into volatile RAM memory and "causes a system components to be loaded into [volatile RAM memory] m (ANCA 875, ¶ 0082; ANCA 921, ¶ 0067; ANCA 952.) (APL10102-1
using an agent to set up a verification structure in the erasable, non-volatile memory of the BIOS, the verification structure accommodating data that includes at least one license record,	The agent, for example, includes a "ticket retrieving module 217," ar server" ("Apple Server") as well as any other additional Apple softwa used to set-up the "ticket" within the erasable, non-volatile memo (ANCA 917, ¶ 0042) (APL10102-10117) The "ticket retrieving module 217" first sends a "ticket request" requesting the boot components used for the secure boot procedure.

Claim Element of the '941 Patent	iOS Devices
	0042) The Apple Server generates a "signed ticket" that operates as a for the iOS device. Each "sighed ticket" includes a cryptographi identifiers" which are a license record used to verify the program. (912, 916-923.) The "signed ticket" is returned to the iOS device and i the returned "signed ticket" matches the "ticket request" sent. (ANC validated, the "signed ticket" is stored as a "local ticket" in the memory of the BIOS. *Id.* (APL10102-10117)
verifying the program using at least the verification structure from the erasable non-volatile memory of the BIOS, and	During the boot procedure for the iOS device, the cryptographic digest verified against the "signed ticket" that is stored in the erasable, non-v BIOS. (ANCA 854-855; 918-920.) (APL10102-10117)
acting on the program according to the verification.	If the program's digest is verified, the program is allowed to operate. is not verified, the program is determined to be invalid and the iOS d under an alternative operating mode (*e.g.*, DFU). (ANCA 854-855; 9 10117)
Claim: 2	
2. A method according to claim 1, further comprising the steps of: establishing a license authentication bureau.	Apple has established an Apple Server for the iOS devices. (A (APL10102-10117)
Claim: 3	

Claim Element of the '941 Patent	iOS Devices
3. A method according to claim 2, wherein setting up a verification structure further comprising the steps of: establishing, between the computer and the bureau, a two-way data-communications linkage;	A "ticket retrieving module" located on the iOS device establis communication link between the iOS device and the Apple Server. ((APL10102-10117)
transferring, from the computer to the bureau, a request-for-license including an identification of the computer and the license-record's contents from the selected program;	The iOS device transfer a "ticket request" or Plist file to the authoriz include: (1) a cryptographic digest of each program, (2) a nonce va identifier (*i.e.*, UID, ECID or GID) that is a unique identification of a (ANCA 854-855, 904, 912, 916-923.) (APL7846-49) (APL10102-101
forming an encrypted license-record at the bureau by encrypting parts of the request-for-license using part of the identification as an encryption key;	The Apple Server validates the "ticket request" and transfers a sign signature that includes a "signed ticket" having a digest correspon identified in the request. Each digest may be "a unique cryptographic 0044) Each "signed ticket" may further include a "signature cryptog the Apple Server. (ANCA 918, ¶ 0046) (APL10102-10117)
transferring, from the bureau to the computer, the encrypted license-record; and	The "signed ticket" is then transferred from the Apple server to the iO ¶ 0048) (APL10102-10117)

Claim Element of the '941 Patent	iOS Devices
storing the encrypted license record in the erasable non-volatile memory area of the BIOS.	The "signed ticket is "validated" to verify it matches the "ticket requ the iOS device. (ANCA 918, ¶ 0048) (APL10102-10117)Once validat is stored as a "local ticket" in the erasable, non-volatile memory of the
Claim: 5	
5. A method according to claim 3 wherein the identification of the computer includes the unique key.	The iOS devices include unique keys, such as "UID," "ECID" and 854-855, 912, 917, 951-952.) (APL7846-49) (APL10102-10117)
Claim: 6	
6. A method according to claim 1 wherein selecting a program includes the steps of: establishing a licensed-software-program in the volatile memory of the computer wherein said licensed-software-program includes contents used to form the license-record.	Loading the OS in volatile RAM (ANCA 875, ¶ 0082; ANCA 9 establishing the contents of the OS used to form the "signed t (APL10102-10117)
Claim: 7	
7. A method according to claim 6 wherein using an agent to set up the verification structure includes the steps of:	The iOS devices establish or certify pseudo-unique keys stored in memory area, such as a "GID," "ECID," or "UID." (ANCA 854-855, 951-952.) (APL7846-49) (APL10102-10117)

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.