EXHIBIT F

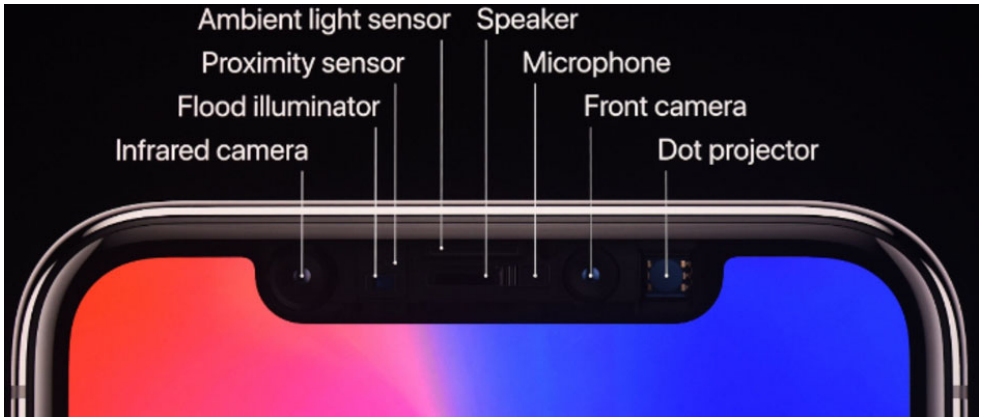
Claim Chart for U.S. Patent No. 9,269,208 ("the '208 Patent")

The Accused Instrumentalities include, but are not necessarily limited to, Apple iPhone type cellular phones and Apple iPad type tablets, including the Apple iPhone X and any Apple product or device that is substantially or reasonably similar to the functionality set forth below. The Accused Instrumentalities infringe the claims of the '208 Patent, as described below, either directly under 35 U.S.C. § 271(a), or indirectly under 35 U.S.C. §§ 271(b)–(c). The Accused Instrumentalities infringe the claims of the '208 Patent literally and, to the extent not literally, under the doctrine of equivalents.

The products accused of infringing the '208 Patent include the Secure Access Accused Products equipped with Apple Card loaded into the iPhone Wallet ("the Secure Pay Accused Products").

Claim 10	**Apple iPhone X**
10. A method for providing secure access to a controlled item in a system comprising a database of biometric signatures, a transmitter sub-system comprising a biometric sensor for receiving a biometric signal, and means for emitting a secure access signal capable of granting more than two types of access to the controlled item, and a receiver sub-system comprising means for receiving the transmitted secure access signal, and means for providing conditional access to the controlled	To the extent that the preamble is deemed to be a limitation, the Apple iPhone X is configured to use a system in accordance with this claim.

Claim 10	Apple iPhone X
item dependent upon information in said secure access signal, the method comprising the steps of:	
10a. populating the database of biometric signatures by: receiving a series of entries of the biometric signal;	**The Apple iPhone populates the database of biometric signatures by receiving a series of entries of the biometric signal.** More specifically, the Apple iPhone X has a secure enclave (SEP) in the A11 chip that populate the database of an encrypted mathematical representation of face images used for Face ID based on a series of face image received by TrueDepth camera system. With a simple glance, Face ID securely unlocks iPhone X. It provides intuitive and secure authentication enabled by the TrueDepth camera system, which uses advanced technologies to accurately map the geometry of your face. Face ID confirms attention by detecting the direction of your gaze, then uses neural networks for matching and anti-spoofing so you can unlock your phone with a glance. Face ID automatically adapts to changes in your appearance, and carefully safeguards the privacy and security of your biometric data. https://www.apple.com/business-docs/FaceID_Security_Guide.pdf The TrueDepth camera is intelligently activated; for example, by tapping to wake your screen, from an incoming notification that wakes the screen, or by raising to wake your iPhone. Each time you unlock your device, the TrueDepth camera recognizes you by capturing accurate depth data and an infrared image. This information is matched against the stored mathematical representation to authenticate. https://support.apple.com/en-us/HT208108

Claim 10	Apple iPhone X
	 https://www.ifixit.com/Teardown/iPhone+X+Teardown/98975  https://www.phonearena.com/news/TrueDepth-camera-iPhone-X-Face-ID-Animoji_id108355

Claim 10	Apple iPhone X
	Face ID data, including mathematical representations of your face, is encrypted and only available to the Secure Enclave. This data never leaves the device. It is not sent to Apple, nor is it included in device backups. The following Face ID data is saved, encrypted only for use by the Secure Enclave, during normal operation: • The mathematical representations of your face calculated during enrollment. • The mathematical representations of your face calculated during some unlock attempts if Face ID deems them useful to augment future matching. Face images captured during normal operation aren't saved, but are instead immediately discarded once the mathematical representation is calculated for either enrollment or comparison to the enrolled Face ID data. https://www.apple.com/business-docs/FaceID_Security_Guide.pdf

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.