

March 19, 2020

George C. Summerfield  
george.summerfield@klgates.com  
(312) 807-4376

**SUBJECT TO FRE 408  
VIA ELECTRONIC MAIL**

Brian Ankenbrandt  
Senior Legal Counsel - IP Transactions  
Apple, Inc.  
One Apple Park Way  
Cupertino, California 95014

**Re: Charter Pacific Corporation Ltd. Patent Portfolio**

Dear Mr. Ankenbrandt:

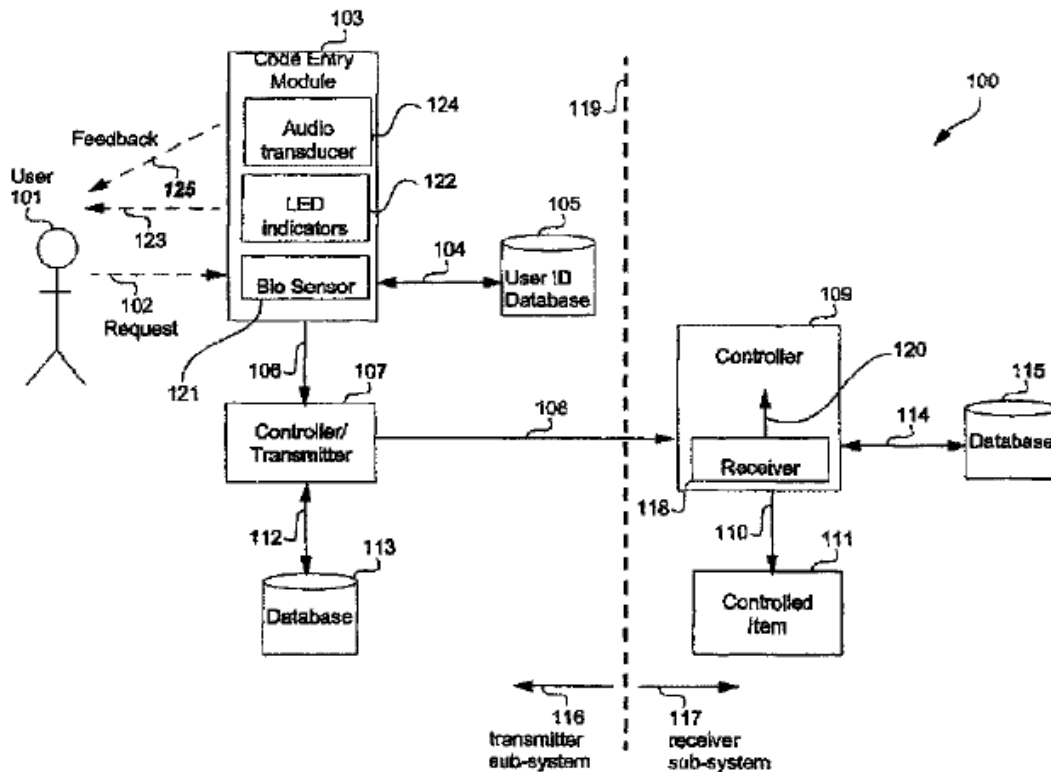
We represent Charter Pacific Corporation Ltd/ (“Charter”) in connection with its licensing and enforcement of its patent portfolio generally directed to electronic access security measures. That portfolio includes U.S. Patent No. 9,665,705 (“the ‘705 Patent”). I understand that the ‘705 Patent, its application, and its European counterpart have been the subject of previous correspondence between Charter and Apple, Inc. (“Apple”). As you alluded to in your March 5, 2020, the ‘705 Patent issued from U.S. Patent App. No. 15/000818, which claims priority of August 13, 2004. Although the ‘705 Patent has been the subject of prior correspondence, I attach a copy thereof for your convenience.

It appears from the prior correspondence that there is an issue regarding the ownership of the ‘705 Patent. To address that issue, I include a January 8, 2020 assignment from Securicom (NSW) Pty Ltd. (“Securicom”) to CPC Patent Technologies Pty Ltd. (“CPC”)<sup>1</sup> Therein, Securicom confirms assignment of the IP Rights set forth in the Schedule to such Assignment to CPC. As you will note, item 19 in the Schedule is the ‘705 Patent. Thus, no other entity is authorized to negotiate with Apple regarding the ‘705 Patent (or any other asset listed on the Schedule).

The invention of the ‘705 Patent is graphically depicted in Figure 2 of that patent:

---

<sup>1</sup> CPC is a wholly-owned subsidiary of Charter.



As shown in Figure 2, the major components of the claimed invention are transmitter and receiver subsystems, which work in concert to provide access to a “controlled item.” A “controlled item” can be “an electronic key circuit in a personal computer” that is to be accessed by the user. ‘705 Patent, col. 6, lines 17-20. Representative claim 1 of the ‘705 Patent reads as follows:

A system for providing secure access to a controlled item, the system comprising:

a memory comprising a database of biometric signatures;

a transmitter sub-system comprising:

a biometric sensor configured to receive a biometric signal;

a transmitter sub-system controller configured to match the biometric signal against members of the database of biometric signatures to thereby output an accessibility attribute; and

a transmitter configured to emit a secure access signal conveying information dependent upon said accessibility attribute; and

a receiver sub-system comprising:

a receiver sub-system controller configured to:

receive the transmitted secure access signal; and

provide conditional access to the controlled item dependent upon said information;

wherein the transmitter sub-system controller is further configured to:

receive a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry;

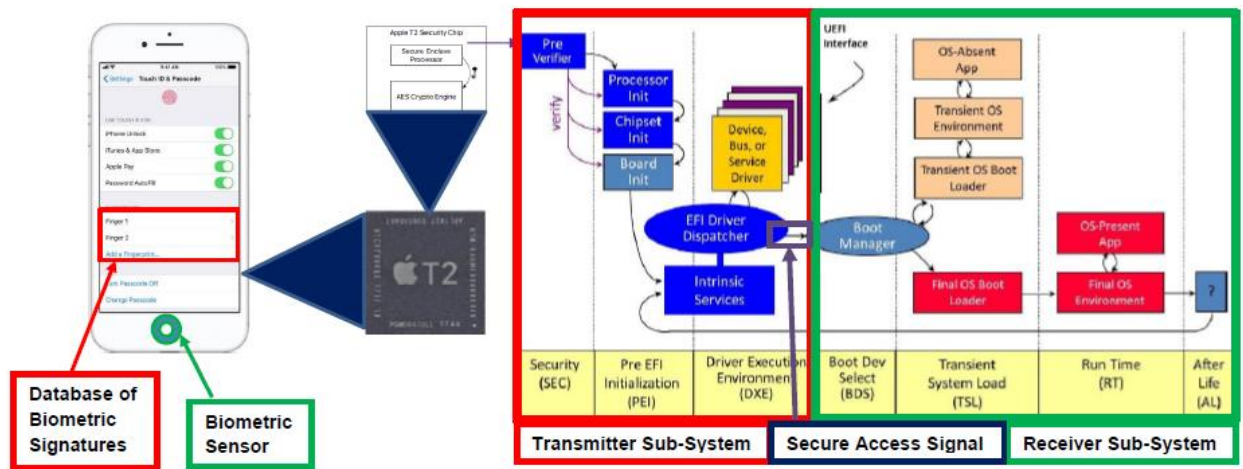
map said series into an instruction; and

populate the data base according to the instruction, wherein the controlled item is one of: a locking mechanism of a physical access structure or an electronic lock on an electronic computing device.

The “biometric signature” can be a fingerprint (*id.*, col. 7, line 40), and the “biometric sensor” can be a fingerprint sensor (*id.*, col. 5, lines 60-63). Further, the “secure access signal” can be transmitted from the transmitter to the receiver can be over a wired medium. *Id.*, col. 7, lines 9-12. In particular, the controlled item can be an electronic key circuit in a personal computer that is to be accessed by the user. *Id.*, col. 6, lines 17-20. In that case, the computer can store the biometric signature in internal memory, and the computer can be integrated into the receiver sub-system. *Id.*, col. 7, lines 22-26.

On a related note, in your March 5, 2020 letter, you contend that “[t]he intrinsic record of the ‘705 patent makes clear, however, that the two sub-systems are separate devices that wirelessly transmit signals between them.” The afore-quoted passage from the ‘705 Patent belies that position.

Apple’s Touch ID secure access technology, as implemented in, *e.g.*, Apple’s iPhone, is described in various Apple publications, such as *Apple T2 Security Chip Security Overview* (Oct. 2018) and *iOS Security* (Sept. 2014). Further, the Apple T2 security Chip implementing such access technology is the subject of third party analyses, such as Davidov, M., *et al.*, *Inside the Apple T2*. Finally, the subject technology is described in Apple patent documents, such as U.S. Patent Appl. No. 2014/0089682. Such information evidences the operation of Apple’s Touch ID technology in the manner depicted below:



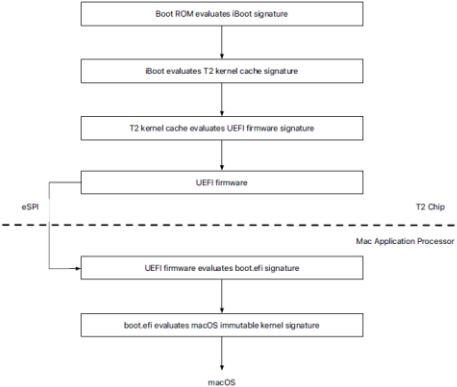
While the above figure illustrates Touch ID as implemented in the iPhone, such illustration is also applicable to Apple's MacBook products:



<https://support.apple.com/en-us/HT207054>.

The following claim chart demonstrates how claim 10 of the '705 Patent literally reads on Apple's Touch ID devices:

Claim 1	Infringement
A transmitter sub-system for operating in a system for providing secure access to a controlled item, wherein the	As shown in the figure above, the Apple T2 Security Chip comprises a transmitter sub-system that provides access to the operating system of an Apple device. Also as shown in that figure, access is provided

transmitter sub-system comprises:	to the device’s operating system conditioned upon successful completion of the security protocol in the T2 chip.
a biometric sensor configured to receiving [sic] a biometric signal;	The Home Button on the iPhone receives fingerprint data to enroll a fingerprint. <a href="https://support.apple.com/en-us/HT201371#setup">https://support.apple.com/en-us/HT201371#setup</a> . The Touch ID button on the MacBook receives fingerprint data to enroll a fingerprint. <a href="https://support.apple.com/en-us/HT207054">https://support.apple.com/en-us/HT207054</a> .
a controller configured to match the biometric signal against members of a database of biometric signatures to thereby output an accessibility attribute; and	Secure Enclave is a coprocessor of Apple’s T2 Security Chip. <i>Apple T2 Security Chip Security Overview</i> (Oct. 2018) at 3. Apple’s Secure Enclave is a separate processor built into the device’s main system. <a href="https://www.howtogeek.com/387934/your-smartphone-has-a-special-security-chip.-heres-how-it-works/">https://www.howtogeek.com/387934/your-smartphone-has-a-special-security-chip.-heres-how-it-works/</a> .
a transmitter configured to emit a secure access signal conveying said information dependent upon said accessibility attribute	<p>As is shown in the figure above, the EFI Driver Dispatcher of the transmitter sub-system (outlined in red) transmits a secure access signal to the Boot Manager of the receiver sub-system (outlined in green). In the figure below, the transmission is from the T2 Chip to the Mac Application Processor via the Enhanced Serial Peripheral Interface (“eSPI”) bus:</p>  <p><i>Apple T2 Security Chip Security Overview</i> (Oct. 2018) at 8.</p>
wherein the controller is further configured to:	The T2 Secure Enclave coprocessor is configured to:
receive a series of entries of the biometric signal, said series being characterised according to at least one of the number of said entries and a duration of each said entry;	Register a fingerprint for Apple Touch ID by the user tapping a finger several times on the home button to record the fingerprint data. <a href="https://video.search.yahoo.com/yhs/search?fr=yhs-pty-pty_converter&amp;hsimp=yhs-pty_converter&amp;hspart=pty&amp;p=registering+fingerprint+apple+touch+id+on+screen+instructions#id=1&amp;vid=">https://video.search.yahoo.com/yhs/search?fr=yhs-pty-pty_converter&amp;hsimp=yhs-pty_converter&amp;hspart=pty&amp;p=registering+fingerprint+apple+touch+id+on+screen+instructions#id=1&amp;vid=</a>

# 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.