Chart B-2 **Invalidity Contentions: U.S. Patent No. 8,843,125**

***Fintiv, Inc. v. Apple Inc.*, Case No. 1:19-CV-1238-ADA (W.D. Tex.)**

<u>Retrieving/Capturing Secure Element (SE) Information</u>

<u>CLAIM LIMITATIONS:</u> "retrieving mobile device information comprising SE information" ('125 patent claim 14) and
configured to capture mobile device information comprising SE information" ('125 patent claim 23).

<u>ASSERTED CLAIMS:</u> These limitations are present in the following asserted claims: '125 patent claims 14 and 23 (and

<u>DISCLOSURE/MOTIVATION TO COMBINE:</u> The Court construed "SE information" as "information that is about or rela
not limited to, production life cycle, card serial number, card image number, and integrated circuit card identification" (
and Fintiv's Infringement Contentions state that "SE info [includes] Card Production Life Cycle (CPLC), Card Serial Nu
Number CIN), Integrated Circuit Card Identification (ICCID)) comprising SE information." *See* Infringement Contenti
id.at 36 ("SE information [includes] financial institution."). Under Fintiv's interpretation of these claim limitations and
mobile devices that were capable of retrieving and/or capturing information about their own secure element were well-k
alleged inventions of the Asserted Patent.[1]

Accordingly, known prior art systems or methods in which a mobile device retrieves and/or captures information relatin
teach these well-known claim limitations, and it would have been obvious to a POSITA to modify a system or method w
provisioned on a mobile device and/or a mobile device registers a mobile wallet application with a TSM so that either of
retrieval of SE information. Moreover, to the extent SIM cards, UICC (Universal Integrated Circuit Card), embedded S
cards/chips are secure elements, retrieving information from and/or about those componenets was also well-known to P
alleged invention. For example, SD Card Association announced the microSD format at CTIA Wireless 2005 on March
microSD details were announced on July 13, 2005. https://simple.wikipedia.org/wiki/MicroSD. And UICC/SIM cards
before that. Smart cards were sold worldwide as early as 1991 by manufacturers such as Giesecke & Devrient. https://w
group/about-us/history/. ETSI released the SIM standard, TS 11.11, shortly thereafter, and a technical specification for
released as early as 1999. https://www.etsi.org/deliver/etsi_ts/102200_102299/102221/03.00.00_60/ts_102221v030000

[1] To the extent that these Invalidity Contentions rely on or otherwise embody particular constructions of terms or phrases in the Asserted Claims
ordered by the Court in this action, Defendant is not proposing any such constructions as proper constructions of those terms or phrases and rese
claim construction positions in this and other proceedings. Various positions put forth in this document are predicated on Plaintiff's incorrect a
claims as evidenced by its Preliminary Infringement Contentions, dated May 20, 2019 and proposed Amended Infringement Conventions, dated
the "Infringement Contentions" or "Preliminary Infringement Contentions"). Those positions are not intended to and do not necessarily reflect
true and proper scope of Plaintiff's claims, and Defendant reserves the right to adopt claim construction positions that differ from or even confli
in this document.

telephone calls made on GSM mobile devices, all of which require a SIM card, the mobile device receives the SIM card ICCID number) and/or the MSISDN (which contains the user's telephone number) from the SE and transmits it to the ca

As reflected by the prior art references and citations below, it was well-understood by POSITAs that software (*e.g.*, an C device retrieved and/or captured its own SE information. A POSITA would have been motivated to implement this stan number of goals, including: 1) ensuring secure registry of the mobile device or the SE with a TSM, 2) allowing for soft provisioned onto the device and/or the SE; 3) to allow a TSM and the mobile device and/or SE to synchronize, backup, to allow the secure verification of a removable SE when it has been transferred from one mobile device to another; and 5 telephone call to verify the identity of the caller and/or their SE. *See, e.g.*, Pesonen at 8:21-43, 11:1-11 ("….the inventio generate Issuer Security Domain keys of a Global Platform Java card, whereby the initialized chip will contain Issuer Se specific keys, which keys have been generated from issuer-specific master keys diversified with the unique chip serial n number may be constructed, for example, from the card production life cycle (CPLC) data on the secure element chip. It several CPLC data fields, such as the IC fabrication date, the IC serial number, and the IC batch identifier….in certain e encrypted communication can take place, the issuer 230 must have the unique chip serial number and the master keys fo discussed above, the device vendor 220 returns the unique chip serial numbers to the issuer 230 after the successful initi device. Alternatively, an issuer without the unique chip serial number may obtain that number from other public sources itself…."); Bauer at 7:29-36, 7:48-54 ("The mobile device 3 may also include one or more other third party application secure memory 4, for example an application module related to third party loyalty scheme. The secure memory 4 may al which is an application to manage and hold the mobile network operator's functionality and secure information, such as PIN…. the automated process begins at Step S3-1 where the middleware server 16 in the account provisioning system 7 new mobile payment account from the mobile device 3 via the communications server 13, the request including data ide and details entered by the user for provisioning the new mobile payment account.").

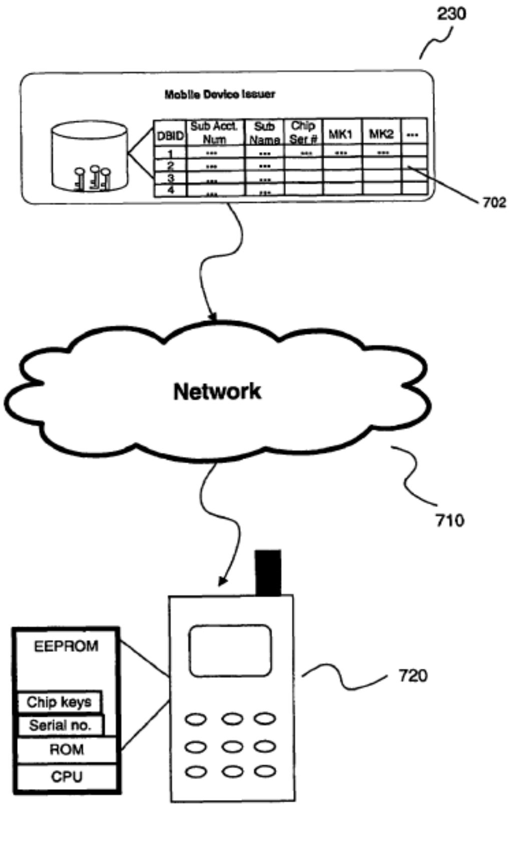
To the extent Fintiv contends that any reference identified in Exhibit A does not disclose any portion of the above limita disclosed by the references herein. Moreover, the exemplary pincites to the prior art identified in the table below also es missing portions would have been obvious to one of ordinary skill in the art. Further, a person of ordinary skill in the ar to combine each reference identified in Exhibit A with any one or more of the following references for at least the reaso document of Apple's Initial Invalidity Contentions or as identified herein.

Chart B-2 **Invalidity Contentions: U.S. Patent No. 8,843,125**

Reference	Disclosure
U.S. Patent No. 7,699,233 to Pesonen (“Pesonen”). Pesonen was filed on filed on November 2, 2005, published on May 3, 2007, and issued on April 20, 2010.	*See, e.g.:* • Pesonen at 2:46-57 (“In light of the foregoing background, embodiments of the prese method for installing and initializing secure element chips into mobile devices. In one a smart card manufacturer creates smart cards with embedded but uninitialized secure are shipped to a mobile device manufacturer/vendor in an uninitialized state, rather th issuer. The uninitialized smart cards may contain pre-installed encryption keys and a may support an initialization routine that can be invoked by the device vendor to pers specific issuer.”). • Pesonen at 5:1-22 (“According to embodiments of the present invention, the pre-insta for each individual smart card manufactured, and will only later be diversified by the chip serial numbers. This process is discussed in detail below. Also, note that the unin other data besides the pre-installed root keys, such as the MAC seed, transfer key, and which are discussed in detail below…Only the unique chip serial number, which is a value, might be public information accessible to the device vendor 220.”). • Pesonen at 5:55-63 (“In contrast, the unique chip serial number may be public inform device vendor. Certain embodiments of the present invention involve occasions wher unsecure or untrusted, and thus the pre-installed root keys, transfer key, and MAC see must remain completely inaccessible to a device vendor in possession of the uninitiali serial numbers, and the encrypted initialization data.”). • Pesonen at 6:27-39 (“The initialization routine, discussed in further detail below, will embedded in the mobile device, personalizing the smart card chip for the issuer 230. manage the device and provide mobile customers with secure data transfer capabilitie 220 delivers the initialized mobile devices to the issuer 230 for distribution to retailer corresponding chip serial numbers of the secure element in each device. The issuer 23 serial numbers in a secure database, to facilitate future communications with the mob 230 distributes these personalized mobile devices to customers.”). • Pesonen at 7:51-57 (“The EEPROM 308 in FIG. 3 illustrates the initial state of the op shows the state of the secure element chip 302 when it is shipped from the smart card 220. The uninitialized chip 302 has initial key values built into the EEPROM 308: the 312, the root keys 314, and the unique serial number 316.”). • Pesonen at 8:21-43 (“Each secure element chip 302 also initially contains a unique se into the OS system area of the EEPROM 308. However, according to other embodim different arrangements for storing the unique serial number 316 can be made. Each se different serial number. In certain embodiments, the unique serial number is 16 digits

Chart B-2 **Invalidity Contentions: U.S. Patent No. 8,843,125**

Reference	**Disclosure**
	after it is written into the EEPROM 308. While the methods presented herein do not c operating system, certain embodiments involve secure elements running a JavaCard v system. For example, the invention can be used to securely generate Issuer Security D Java card, whereby the initialized chip will contain Issuer Security Domain with chip been generated from issuer-specific master keys diversified with the unique chip seria number may be constructed, for example, from the card production life cycle (CPLC) It may be constructed from several CPLC data fields, such as the IC fabrication date, batch identifier.”). • Pesonen at 10:26-35 (“After the Successful execution of the initialization routine, the chip keys 518 and the unique chip serial number 316. As previously mentioned, whil do not depend on a secure element operating system, certain embodiments involve se JavaCard with Global Platform operating system. In such embodiments, FIG.5 may c mode of the JavaCard Global Platform operating system, and the ROM 306 may store • Pesonen at 10:53-58 (“To generate the chip keys for a specific secure element, the iss chip serial number, which the device vendor 220 may send to the issuer, for example, database. The issuer 230 may then diversify the master keys with the unique chip seri • Pesonen at 11:1-11 (“However, in certain embodiments, before encrypted communica 230 must have the unique chip serial number and the master keys for the target device vendor 220 returns the unique chip serial numbers to the issuer 230 after the successf device. Alternatively, an issuer without the unique chip serial number may obtain tha sources, or from the device itself. However, the issuer 230 still needs the master keys numbers before communicating with the device USC.”). • Pesonen at 11:43-47 (“Once the chip keys are securely embedded into the mobile dev possession of the unique chip serial numbers and the corresponding master keys, encr transactions can take place between the issuer 230 and the mobile device.”). • Pesonen at Fig. 7:

Reference	Disclosure
	 230 Mobile Device Issuer DBID Sub Acct. Num Sub Name Chip Ser # MK1 MK2 ... 1 2 3 4 702 Network 710 EEPROM Chip keys Serial no. ROM CPU 720 FIG. 7 The teachings of this reference are explicitly directed to systems and methods wherein softwar device and/or a mobile device registers a mobile wallet application with a TSM, and a POSITA been motivated to combine these teachings with other systems and methods in which software device and/or a mobile device registers a mobile wallet application with a TSM, such as those

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.

WHAT WILL YOU BUILD? | sales@docketalarm.com | 1-866-77-FASTCASE