Chart B-1 **Invalidity Contentions: U.S. Patent No. 8,843,125**

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

Filtering Based on Mobile Device Information

CLAIM LIMITATIONS: "receiving filtered contactless card applet for provisioning, wherein the contactless card applet i device information" ('125 patent claim 14), "a rule engine configured to filter a widget based on the mobile device inform and "an over-the-air (OTA) proxy configured to provision the contactless card applet, a widget corresponding to the co WMA, wherein said OTA proxy is configured to capture mobile device information comprising SE information; and configured to transmit the mobile device information for registering the mobile wallet application" (claim 23 to the exte

ASSERTED CLAIMS: These limitations are present in the following asserted claims: '125 patent claims 14, 18, and 23

DISCLOSURE/MOTIVATION TO COMBINE: Under Fintiv's interpretation of these claim limitations, filtering a contactl corresponding widget, or other software was well-known to persons of ordinary skill in art at the time of the alleged inv Patent. [1]

Fintiv does identify how the accused products perform filtering. The entirety of Fintiv's Preliminary Infringement Cont limiation of claim 18 are reproduced below. See Preliminary Infringement Contentions, Ex. A at 68-71.

[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 ar 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 t 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.

How Apple Pay uses the Secure Element

The Secure Element hosts a specially designed applet to manage Apple Pay. It also includes payment applets certified by the payment networks. Credit, debit, or prepaid card data is sent from the payment network or card issuer encrypted to these payment applets using keys that are known only to the payment network and the payment applets' security domain. This data is stored within these payment applets and protected using the Secure Element's security features. During a transaction, the terminal communicates directly with

the Secure Element through the Near Field Communication (NFC) controller over a dedicated hardware bus.

iOS Security Guide, iOS 11.4, August 2018 at p. 40-41.

When you add credit, debit, prepaid, or transi

When you add a credit, debit, prepaid, or transit card (where available) to
information that you enter on your device is encrypted and sent to Apple
use the camera to enter the card information, the information is never sa
device or photo library.

Apple decrypts the data, determines your card's payment network, and r
data with a key that only your payment network (or any providers authori
issuer for provisioning and token services) can unlock.

Information that you provide about your card, whether certain device set
and device use patterns—such as the percent of time the device is in mo
approximate number of calls you make per week—may be sent to Apple
eligibility to enable Apple Pay. Information may also be provided by Apple
issuer, payment network, or any providers authorized by your card issuer
Apple Pay, to determine the eligibility of your card, to set up your card wi
to prevent fraud.

After your card is approved, your bank, your bank's authorized service pr
card issuer creates a device-specific Device Account Number, encrypts i
along with other data (such as the key used to generate dynamic securit
unique to each transaction) to Apple. The Device Account Number can't
Apple but is stored in the Secure Element—an industry-standard, certifie
to store your payment information safely—on your device. Unlike with us
card numbers, the card issuer can prevent its use on a magnetic stripe c
phone, or on websites. The Device Account Number in the Secure Eleme
from iOS, watchOS, and macOS, is never stored on Apple servers, and is
to iCloud.

https://support.apple.com/en-us/HT203027 (last access

Credit, debit, and prepaid card provisioning

When a user adds a credit, debit, or prepaid card (including store cards) to Apple Pay, Apple securely sends the card information, along with other information about user's account and device, to the card issuer or card issuer's authorized service provider. Using this information, the card issuer will determine whether to approve adding the card to Apple Pay.

Apple Pay uses three server-side calls to send and receive communication with the card issuer or network as part of the card provisioning process: *Required Fields*, *Check Card*, and *Link and Provision*. The card issuer or network uses these calls to verify, approve, and add cards to Apple Pay. These client-server sessions are encrypted using TLS v1.2.

Full card numbers aren't stored on the device or on Apple servers. Instead, a unique Device Account Number is created, encrypted, and then stored in the Secure Element. This unique Device Account Number is encrypted in such a way that Apple can't access it. The Device Account Number is unique and different from usual credit or debit card numbers; the card issuer can prevent its use on a magnetic stripe card, over the phone, or on websites. The Device Account Number in the Secure Element is isolated from iOS and watchOS, is never stored on Apple servers, and is never backed up to iCloud.

Cards for use with Apple Watch are provisioned for Apple Pay using the Apple Watch app on iPhone. Provisioning a card for Apple Watch requires that the watch be within Bluetooth communications range. Cards are specifically enrolled for use with Apple Watch and have their own Device Account Numbers, which are stored within the Secure Element on the Apple Watch.

iOS Security Guide, iOS 11.4, August 2018 at p. 41.

Adding a credit or debit card manually to Apple Pay

To add a card manually, the name, card number, expiration date, and CVV are used to facilitate the provisioning process. From within Sett the Wallet app, or the Apple Watch app, users can enter that informa by typing, or using the camera on the device. When the camera cap the card information, Apple attempts to populate the name, card nu and expiration date. The photo is never saved to the device or store in the photo library. After all the fields are filled in, the Check Card process verifies the fields other than the CVV. They are encrypted a sent to the Apple Pay Server.

If a terms and conditions ID is returned with the Check Card proces Apple downloads and displays the terms and conditions of the card to the user. If the user accepts the terms and conditions, Apple sen the ID of the terms that were accepted as well as the CVV to the Lin Provision process. Additionally, as part of the Link and Provision pro Apple shares information from the device with the card issuer or net like information about your iTunes and App Store account activity (fo example, whether you have a long history of transactions within iTu information about your device (for example, phone number, name, a model of your device plus any companion iOS device necessary to s up Apple Pay), as well as your approximate location at the time you your card (if you have Location Services enabled). Using this informa the card issuer will determine whether to approve adding the card to Apple Pay.

As the result of the Link and Provision process, two things occur:

- The device begins to download the Wallet pass file representing th credit or debit card.
- The device begins to bind the card to the Secure Element.

The pass file contains URLs to download card art, metadata about th card such as contact information, the related issuer's app, and supp features. It also contains the pass state, which includes information as whether the personalizing of the Secure Element has completed, whether the card is currently suspended by the card issuer, or whet additional verification is required before the card can make payment Apple Pay.

iOS Security Guide, iOS 12.1, November 2018 at p. 49.

The '125 patent explains that the "filtered list of downloadable applications" may be filtered based on a variety of inform device, including other software stored on the device or even an entity associated with that software: "mobile device 10 without limitation, the mobile network provider of the mobile device 100 (e.g. 'Sprint®', 'Verizon®', 'AT&T®', etc.), associated with the contactless card applets stored (e.g. 'Wachovia®', 'Bank of America®', 'Chase®', etc.), mobile dev 'HTC®', 'Motorola®', 'Apple®', etc.), and mobile device 100 hardware specifications (i.e. hardware, software, operati at 10:24-34; *see also id*. at 5:22-24 ("Rule engine 116 may filter widgets based on information related to the mobile dev not disclose that filtering applets, widgets, or other software was done in a way that was unconventional or based on crit

To the extent Fintiv contends that the claimed "applets" and "widgets" are software applications, a person of ordinary sk motivated to combine and/or apply teachings beyond only those found in mobile wallet prior art references. For as long software configurations have existed in computers, software purveyors have offered users software applications that are

respective devices. For example, vendors offered a Windows user the Windows-compitable version of a software applic Linux-comptaible version of the software, and a Mac user the Mac-compatible version of the same software. There is n this concept, regardless of whether it is performed by a human or on a server which filters based on "mobile device infor software being filtered is a contactless card applet or widget does not make it any less obvious.

In much the same way that a computer such as a laptop, desktop, or smartphone would send information (e.g., OS versio server in order to receive an operating system update, service pack, or security patch corresponding to the existing softw user could then choose to install, a mobile device would send "mobile device information" to a server to receive notifica or "widgets" which a user could then choose to install. This technique was well-known and obvious to POSITA prior to Asserted Patent in view of similar approaches used for things like providing Windows service-pack and security updates

A POSITA would have been motivated to implement this standard practice to advance the goal of ensuring that only the applications that work with the particular mobile device at issue are offered or provisioned to that device. *See, e.g.*, Aig appreciated that a first moblet software module 204 may be installed during manufacturing of the electronic device 210. moblet software module 204 may be requested 201 from the remote server 230. The request 201 may indicate a device t 210. In response to the request 201, the remote server 230 may transmit 203 the first moblet software module 204 to the Furthermore, responsive to the request 201, the remote server 130 may transmit 203 a device dependent software, e.g., M O'Neill at 11:62-12:32 ("…the client device 104 establishes a communication link with the update device server 136 and information 113 including, type, model, and/or make of the device, as well as version of operational system software cu client device information and checks the server manifest or queries the update store 133 for the presence of the update p the available versions of operational software on the server manifest or update store 133 to the onboard version of opera the client device 104, the update store 133 directs the transfer of the update package 110 to the client device 104…."). A motivated to apply filtering in this manner to improve the user experience, avoid the hassles and costs associated with at incompatible software, eliminate service calls and requests from users about compatibility problems, and provide faster server-based filtering.

Accordingly, a POSITA at the time of the alleged invention would have found it obvious to use known software filtering provisioning "applets" and "widgets" on a mobile device. More specifically, it would have been obvious to modify or c systems or methods in which a server filters for software on the basis of information related to the client-side device to a device with a contactless card applet and/or a corresponding widget which were first filtered by the server providing suc information relating to the mobile device.

Chart B-1 **Invalidity Contentions: U.S. Patent No. 8,843,125**

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.

Reference	Disclosure
U.S. Patent Publication No. 2010/0138518 A1 to Aiglstorfer ("Aiglstorfer"). Aiglstorfer was filed on November 18, 2009 and published on June 3, 2010.	*See, e.g.*: • Aiglstorfer at ¶ 12 ("It is appreciated that responsive to a user request, the electronic w remote server to download the first moblet software module. The sent message may i electronic wallet. Accordingly, the electronic wallet receives from the remote server t module via a wireless network. Moreover, the electronic wallet receives from the rem software module via a wireless network. Accordingly, the electronic wallet executes t using the device dependent software module. According to one embodiment, the first modules are written using MOJAX commands."). • Aiglstorfer at ¶ 31 ("It is appreciated that the first moblet software module 106 may b of the elec tronic device 110. Alternatively, the first moblet software module 106 may remote server 130 and subsequently downloaded. The request 101 may indicate a dev 110. In response to the request 101, the remote server 130 may transmit 103 the first m the electronic device 110. Furthermore, responsive to the request 101, the remote ser device dependent software, e.g., MOJAX environment, to the electronic wallet."). • Aiglstorfer at Fig. 1:

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.