Chart B-5 **Invalidity Contentions: U.S. Patent No. 8,843,125**

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

Displaying and Receiving a Selection of a Contactless Card Applet

CLAIM LIMITATIONS: "displaying a contactless card applet based on attributes of the mobile device" and "receiving a s applet" ('125 patent claim 11).

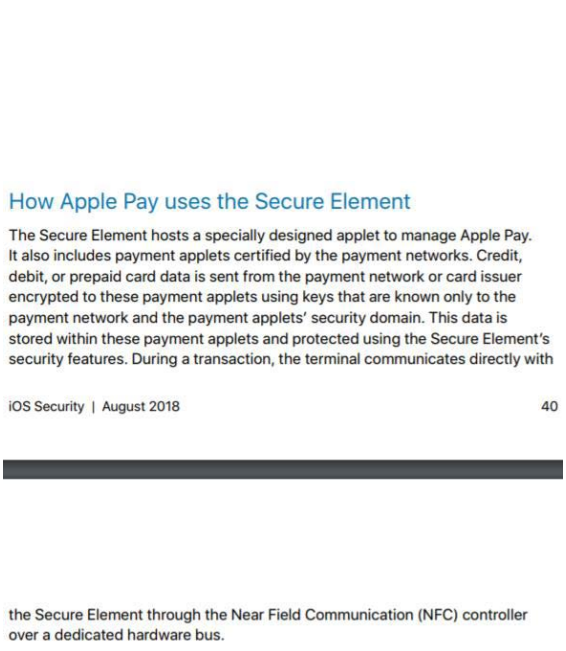
ASSERTED CLAIMS: These limitations are present in the following asserted claim: '125 patent claim 11 (and its deper

DISCLOSURE/MOTIVATION TO COMBINE: Under Fintiv's interpretation of these claim limitations, mobile devices tha selection of a contactless card applet ("CCA") were well-known to POSITA at the time of the alleged inventions. [1]

For both the "displaying …" and "receiving …" limitations, the entirety of Fintiv's Infringement Contentions is reprodu

[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.

Chart B-5 **Invalidity Contentions: U.S. Patent No. 8,843,125**

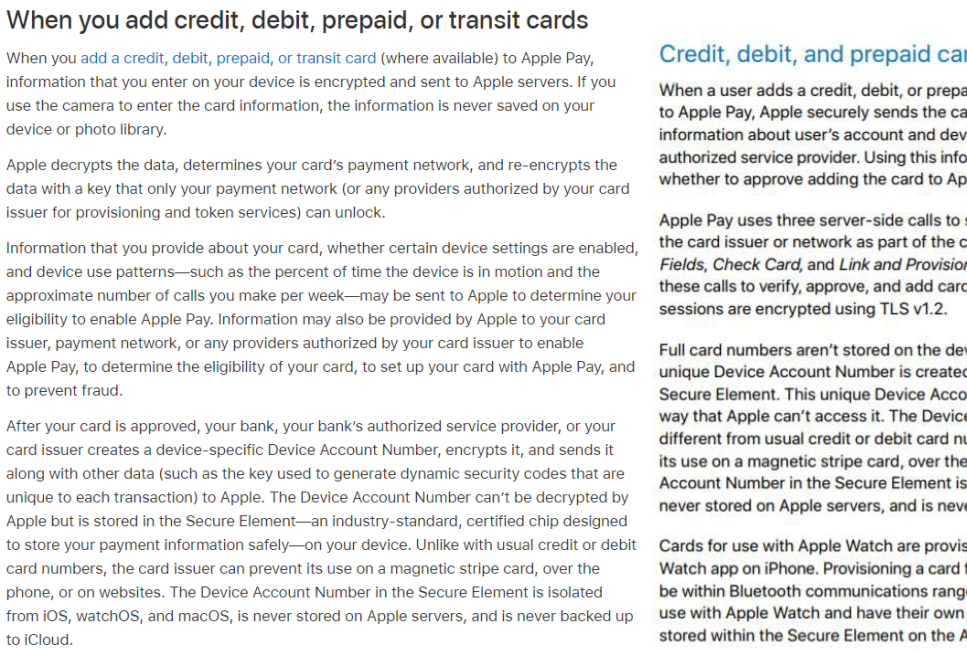


How Apple Pay uses the Secure Element

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

iOS Security | August 2018 40

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



When you add credit, debit, prepaid, or transit cards

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

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

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

After your card is approved, your bank, your bank's authorized service provider, or your card issuer creates a device-specific Device Account Number, encrypts it, and sends it along with other data (such as the key used to generate dynamic security codes that are unique to each transaction) to Apple. The Device Account Number can't be decrypted by Apple but is stored in the Secure Element—an industry-standard, certified chip designed to store your payment information safely—on your device. Unlike with 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, watchOS, and macOS, is never stored on Apple servers, and is never backed up to iCloud.

Credit, debit, and prepaid ca

When a user adds a credit, debit, or prepa to Apple Pay, Apple securely sends the ca information about user's account and dev authorized service provider. Using this info whether to approve adding the card to Ap

Apple Pay uses three server-side calls to the card issuer or network as part of the c *Fields*, *Check Card*, and *Link and Provisio* these calls to verify, approve, and add card sessions are encrypted using TLS v1.2.

Full card numbers aren't stored on the dev unique Device Account Number is created Secure Element. This unique Device Acco way that Apple can't access it. The Device different from usual credit or debit card nu its use on a magnetic stripe card, over the Account Number in the Secure Element is never stored on Apple servers, and is neve

Cards for use with Apple Watch are provis Watch app on iPhone. Provisioning a card be within Bluetooth communications rang use with Apple Watch and have their own stored within the Secure Element on the A

See Infringement Contentions Ex. A at pp. 13-18.

These passages disclose nothing about "displaying a contactless card applet …" Nor do they disclose "receiving a selec applet …" from a user. Rather, the passages disclose a user manually entering credit card information (e.g., by typing i a picture of their card for provisioning purposes. Under Fintiv's interpretation, these claim limitations were well-known obvious to POSITAs at the time of the alleged invention as reflected by the prior art references below. The Asserted Pat contactless card applet is displayed in any novel manner or that "receiving a selection of a contactless card applet" is acc unconventional or new way. *See*, *e.g.*, '125 patent at 11:2-4 ("TSM system 120 sends the list of applets to display to the which relays it back to the mobile wallet application 24 in step 405."); *id*. at 8:46-51 ("mobile device user is prompted to the mobile wallet application 24 with the changes made at the TSM system 120"). To the contrary, such activities were it would have been obvious to modify prior art system or methods wherein a contactless card applet is provisioned on a mobile device displays and receives a selection of that contactless card applet. Nothing in the Asserted Patent suggests "displaying" and "receiving" techniques used outside the context of contactless card applications (e.g., for displaying an software such as games apps and the like) would have required anything beyond the ordinary skill to implement in the c applets.

A POSITA would have been motivated to implement these standard practices to provide a simple, intuitive, and conveni software such as contactless card applications. This is especially true given the proliferation of available applications (su applets) from companies like Visa, Mastercard, and Discover. *See, e.g.*, Khan at 2:43-67 ("A card number for a soft car on the device is obtained form the user of the device…Soft card personalization data along with branding image, market imprint data, account summary data for provisioning the soft card is received from the provisioning issuer server. The so on the device based on the personalization data."); Brudnicki at Figs. 4A-4B, ¶ 53 ("As an example, FIGS. 4A and 4B, i "Charge-It Card into the wallet using one exemplary wallet user interface 410 that may be deployed on a Smartphone. U interface, the card services module 420 preferably transmits the first six digits of the identified credit card (commonly re Identification Number or BIN) to the control server, which then validates the card issuer's compliance rules and facilitate between the OpenWallet 100 (or Card Services Module 420) on the user's mobile device 50 and the appropriate issuer s as was previously known in the art."). Further, it would have been obvious to display to a user the contactless card appl credit card accounts a user had already setup with his/her bank. For example, if a user had a Visa and American Express Mastercard cards, a POSITA would have been motivated to simplify the selection process for the user by only displayin Express options.

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 ("Aiglstorfer"). Aiglstorfer was filed on November 18, 2009 and published on June 3, 2010.	*See, e.g.*: • Aiglstorfer at paragraph [0039] ("It is appreciated that additional banking card inform modules associated therewith may be similarly received and installed and messaged b example, a second banking card information 113 may be transmitted from the TSM 1 may store the second banking card information 113 in the removable security elemen subsequently automatically notify 115 the first moblet software module 106 of the tra card information. According to one embodiment, the first moblet software module 10 130 that the second banking card information 113 has been received.").

Chart B-5 **Invalidity Contentions: U.S. Patent No. 8,843,125**

Reference	Disclosure
	• Aiglstorfer at paragraph [0042] ("According to one embodiment, the third moblet sof transmitted wirelessly and installed on the electronic device 110 transparent to the us to the third moblet software module 112 may be transmitted and installed automatical that the third moblet software module 112 or any update thereof may be received and 110 responsive to a user request."). • Aiglstorfer at paragraph [0072] ("At step 734, graphical icons of the second and the t rendered on a display of the portable device. The graphical icons are user selectable. and selection of the second and the third moblet software modules are controlled by c software module."). • *See also* Aiglstorfer at ¶¶ 51, 54. The teachings of this reference are explicitly directed to systems and methods wherein a conta on a mobile device, and a POSITA at the relevant time would have been motivated to combine systems and methods in which a mobile device displays and receives a selection of a contactle identified in Exhibit A.
U.S. Pat. Pub. 2010/0190437 ("Buhot 437"). Buhot 437 was filed December 23, 2009 and published on July 29, 2010.	*See, e.g.*: • "The user interface element 224 also includes a user interface engine 330 for providin NFC services provided by the NFC application elements 302-312 to a user via the MI presented to the user may include a list of the NFC services which may be provided b 302-312. Using the examples given above for the NFC application elements 302-312, PayPass.TM. payment card, VSDC.TM. payment card, train ticket, airline ticket, boo loyalty card. The user interface element 224 therefore enables the user to select one o application elements 302-312 from information provided to the user via the MMI 214 interface element 224 manages the selected NFC application element via the respectiv to provide the selected service or to update a NFC service. Managing the selected NF interface element 224 includes selecting and executing the managing application elem selected NFC application element and the selected managing application element ther application element and its behaviour during the provision of the associated service. U include deleting, updating, installing an application element in the NFC unit 218, and an NFC managing element in the program memory 216. The user interface element 2 see also ¶¶46, 21-22, 57-58, 89-90, 97, 118, 120.

Reference	Disclosure
	• "installCard: the user interface element 224 informs a NFC managing element to chec elements available for installation … After a successful card installation, the NFC ma interface element 224 are updated accordingly. New card application elements install registration element 331 and can be selected by the user interface element 224 to proc transaction." ¶81. • "Since the user interface element 224 provides to the user information relating to the interface element 224 needs to be notified accordingly to take these changes into acco information displayed to the user to provide the user an updated list of the available N application elements that are present in the NFC unit 218 after an OTA update. The d the branding information, the CALC information may have changed too. Thus, the pr to update the information provided to the user by the user interface element 224 accor information transferred to the NFC unit 218. In a mobile device having a database ele 316 is updated when the received update information is transferred to the NFC unit ar the user may be updated from the updated information in the database element 316." • "The mobile device 102 also has a Man Machine Interface MMI 214, including eleme microphone, speaker, display screen, for providing an interface between the mobile d device. The MMI 214 is also coupled to the processing unit 200." ¶39. • "In the above, the user interface element 224 informs a NFC managing element in res selection via a display of the mobile device 102." ¶84; see also ¶81. • "The user interface element enables information for the different application elements the user in a simple user friendly manner, for example, by a central menu which lists NFC services, and enables the user to select and initiate a NFC service out of a plural information presented to the user which selected NFC service is then provided by the selected NFC service managing the appropriate application element(s)." ¶124. • "The user selects a card application element to proceed with the contactless transactio selection of a card application element, the user interface engine 330 forwards a start registration element 331, step 706. As the selected card application element belongs t the registration element 331 notifies the NFC managing element by invoking the sele 708. The NFC managing element A initialises itself, and activates the card applicatio (such as the NFC communication section 204), step 710. When the NFC managing el the contactless transaction, the user interface element 224 is put on standby, step 712 managing element A is activated (step 714). The activated user interface notifies the u

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.