

Chart B-4

## Invalidity Contentions: U.S. Patent No. 8,843,125

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

### Synchronizing the Mobile Wallet Application with the TSM

**CLAIM LIMITATIONS:** “synchronizing the mobile wallet application with the TSM system” (’125 patent claim 11) and “mobile wallet application with the TSM system comprises: checking for a change made to a configuration of the mobile wallet application and transmitting the change to the TSM system” (’125 patent claim 13).

**ASSERTED CLAIMS:** These limitations are present in the following asserted claims: ’125 patent claims 11 (and its dependent claims) and 13.

**DISCLOSURE/MOTIVATION TO COMBINE:** Under *Fintiv*’s interpretation of these claim limitations, synchronizing a mobile wallet application with a TSM was well-known at the time of the alleged inventions of the asserted claims.<sup>1</sup>

Synchronization technologies and techniques were quite mature by the time of the alleged invention and would have been known to those of ordinary skill in the art, as evidenced by the references herein. The ’125 patent specification discusses synchronization only as a general matter, and does not describe how the mobile wallet application 24 connects to the TSM system 120, which may house WMS 110, for synchronization in steps 8:30-33. The same is true of the synchronization resulting from a change made to the mobile wallet application recited in claim 13. Paragraph 11 of Figure 5 discusses synchronization initiated from the server (*id.* at 11:5-53)—the specification simply states that synchronization occurs in response to a change made on the mobile device: “while mobile wallet application 24 is still active, any modifications that are made to the mobile wallet application 24 itself will be updated in the WMS 110 in step 505 as synchronization is a continuous one during usage.” The asserted patent also states that synchronization may be updating a “change[d] user preference” or “expiration date.” *Id.* at 11:5-53. No detail is provided with respect to how synchronization occurs and no suggestion is made that synchronization was new or non-obvious. Synchronization of mobile wallet software or data would be any different than synchronization of any other type of information known in the art.

*Fintiv*’s Preliminary Infringement Contentions do not point to any evidence of synchronization, whether generally or with respect to device-initiated synchronization of claim 13. Indeed, for the synchronizing element of both claim 11 and claim 13, *Fintiv*’s contentions are unavailing.

---

<sup>1</sup> To the extent that these Invalidity Contentions rely on or otherwise embody particular constructions of terms or phrases in the Asserted Claims, Defendant is not proposing any such constructions as proper constructions of those terms or phrases and reserves the right to adopt claim construction positions in this and other proceedings. Various positions put forth in this document are predicated on Plaintiff’s incorrect and inconsistent claim constructions (as evidenced by its Preliminary Infringement Contentions, dated May 20, 2019 and proposed Amended Infringement Contentions, dated May 20, 2019, and the “Infringement Contentions” or “Preliminary Infringement Contentions”). Those positions are not intended to and do not necessarily reflect the true and proper scope of Plaintiff’s claims, and Defendant reserves the right to adopt claim construction positions that differ from or even conflict with those positions in this document.

Chart B-4


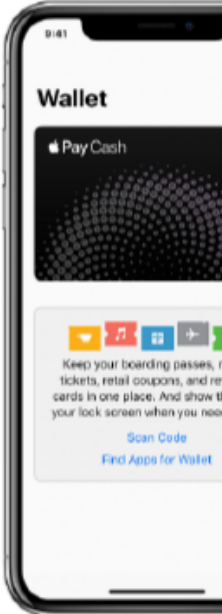
## Invalidity Contentions: U.S. Patent No. 8,843,125

Contentions cite only to the same evidence that it also cites with respect to activating the mobile wallet application and c Preliminary Infringement Contentions Ex. A at pp. 2-5 (activating the mobile wallet application), 5-9 (same citations for (same citations for synchronization element of claim 11), 20-32 (same citations for all elements of claim 13). Fintiv’s er “synchronizing ...” limitation in claim 11 is pasted below. See Preliminary Infringement Contentions, Ex. A at 9-13.

Infringing Functionality/Structure	Infringing Functionality/Structure
<p data-bbox="402 894 646 919"><b>Apple Pay components</b></p> <p data-bbox="402 932 959 995"><b>Secure Element:</b> The Secure Element is an industry-standard, certified chip running the Java Card platform, which is compliant with financial industry requirements for electronic payments.</p> <p data-bbox="402 1016 959 1100"><b>NFC controller:</b> The NFC controller handles Near Field Communication protocols and routes communication between the application processor and the Secure Element, and between the Secure Element and the point-of-sale terminal.</p> <p data-bbox="402 1121 959 1226"><b>Wallet:</b> Wallet is used to add and manage credit, debit, rewards, and store cards and to make payments with Apple Pay. Users can view their cards and additional information about their card issuer, their card issuer’s privacy policy, recent transactions, and more in Wallet. Users can also add cards to Apple Pay in Setup Assistant and Settings.</p> <p data-bbox="402 1247 959 1310"><b>Secure Enclave:</b> On iPhone, iPad, and Apple Watch, the Secure Enclave manages the authentication process and enables a payment transaction to proceed.</p> <p data-bbox="402 1331 959 1415">On Apple Watch, the device must be unlocked, and the user must double-click the side button. The double-click is detected and passed to the Secure Element or Secure Enclave where available, directly without going through the application processor.</p> <p data-bbox="402 1436 959 1541"><b>Apple Pay servers:</b> The Apple Pay servers manage the setup and provisioning of credit and debit cards in Wallet and the Device Account Numbers stored in the Secure Element. They communicate both with the device and with the payment network servers. The Apple Pay servers are also responsible for re-encrypting payment credentials for payments within apps.</p> <p data-bbox="402 1583 878 1608">iOS Security Guide, iOS 11.4, August 2018 at p. 40.</p>	<p data-bbox="1008 894 1620 919"><b>When you add credit, debit, prepaid, or transit cards</b></p> <p data-bbox="1008 932 1624 1037">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.</p> <p data-bbox="1008 1058 1624 1121">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 issuer for provisioning and token services) can unlock.</p> <p data-bbox="1008 1142 1624 1289">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 to prevent fraud.</p> <p data-bbox="1008 1310 1624 1562">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.</p> <p data-bbox="1008 1583 1624 1608"><a href="https://support.apple.com/en-us/HT203027">https://support.apple.com/en-us/HT203027</a> (last accessed on 2/6/2018)</p>

Chart B-4

**Invalidity Contentions: U.S. Patent No. 8,843,125**

<p><b>Infringing Functionality/Structure</b></p> <p><b>Credit, debit, and prepaid card provisioning</b></p> <p>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.</p> <p>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: <i>Required Fields</i>, <i>Check Card</i>, and <i>Link and Provision</i>. 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.</p> <p>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.</p> <p>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.</p> <p>iOS Security Guide, iOS 11.4, August 2018 at p. 41.</p>	<p><b>Infringing Functionality/Structure</b></p> <p><b>Add a card on your iPhone</b></p> <ol style="list-style-type: none"> <li>1. Go to Wallet and tap .</li> <li>2. Follow the steps to add a new card. <i>Watch the demo</i> to see how it works. If you're asked to add the card that you use with iTunes, cards on other devices, or cards that you've recently removed, choose them, then enter the card security codes. You might be required to download an app from your bank or card issuer to add a card to Wallet.</li> <li>3. Tap Next. Your bank or card issuer will verify your information and decide if you can use your card with Apple Pay. If your bank or issuer needs more information to verify your card, they'll ask you for it. When you have the information, go back to Wallet and tap your card.</li> <li>4. After your bank or issuer verifies your card, tap Next. Then start using Apple Pay.</li> </ol> <p>Get help adding your card to Wallet.</p> <p><a href="https://support.apple.com/en-us/HT204506">https://support.apple.com/en-us/HT204506</a> (last accessed on 10/10/2018)</p> 
---	---

As reflected by references below, synchronizing a mobile wallet application with a TSM system was well-known and used at the time of the alleged invention. A POSITA would have been motivated to implement this standard practice in a mobile wallet application of keeping financial information current and accurate, backing up and restoring information in the event of a data loss or theft, and allowing both users and service providers to update information. *See, e.g.*, Buhot EP 481 at ¶ 42 (“The instructions to update one or more parameters may include personalisation information to update one or more parameters of a NFC application element in a user...In the case of a payment card application element, the instructions to update one or more parameters may include instructions to the issuing bank to update the payment card expiration date, to change a security code, to set the credit card number, to set the maximum amount for a payment transaction, to set the maximum amount for a payment transaction element, to be triggered by the user...”); AllwaySync (describing “Free File Synchronization, Backup, Data Replication, PC Sync Software”) <https://web.archive.org/web/20090318105616/http://allwaysync.com/>; Ilium Software (describing “Ilium Software Synchronization, you can make simultaneous changes to different cards on your Windows PC and Windows Mobile devices”).

Chart B-4

**Invalidity Contentions: U.S. Patent No. 8,843,125**

synchronized.”). Accordingly, a POSITA would be motivated to combine standard file synchronization techniques in the mobile wallet with a TSM server.

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

Reference	Disclosure
<p>“Toward a Mobile Digital Wallet” by Alan Cole et al. published October 16, 2009 in IBM Research Report (“Cole”).</p>	<p><i>See, e.g.:</i></p> <ul style="list-style-type: none"> <li>• “[N]ative wallet applications on mobile devices could operate against replicated snapshots of the user’s wallet in a situation where network connectivity to the central wallet service is unavailable or unreliable. The replication strategies where localized copies are synchronized at opportune times. ... It should also be possible to transfer one wallet to another. Transfer capabilities should be in effect even if the two wallets are not managed by the same server.” Cole at pg. 4-5.</li> <li>• “Sharing. In many usages, the contents of a wallet could be shared among users - for example, family members - for payment instruments or virtual cash. This can be realized in two ways: replication of the shared items to each device, periodic synchronization, or via virtualized views on a base wallet. Operations carried out on a virtualized view are transferred to the base wallet. Virtualization storage schemes would induce the need for virtualized storage. For example, a conservative scheme that computes and enforces the maximum access requirements among all devices across all wallets. Staged import and export. The combination of the above wallet storage, access control, and synchronization capabilities can be combined in useful ways that yield higher level policies about wallet usage.” <i>Id.</i></li> </ul> <p>The teachings of this reference are explicitly directed to systems and methods wherein a central server administers a central server and provides mobile wallet synchronization capabilities to mobile devices. A POSITA at the relevant time would be motivated to combine these teachings with other systems and methods in which servers provide software for provisioning and management of those identified in Exhibit A.</p>
<p>“Ilium Software eWallet- Users Guide and Reference for Windows PCs and Windows Mobile-based Pocket PCs and</p>	<p><i>See, e.g.:</i></p> <ul style="list-style-type: none"> <li>• “Synchronization</li> </ul>

Smartphones, Version 4.0”  
 Copyright 1997-2006, Ilium  
 Software, Inc. (“Ilium”).

eWallet 4.0 lets you choose between two ways of synchronizing your information: SyncPro™ and

With SyncPro Synchronization, you can make simultaneous changes to different cards on your Win device and both changes will be synchronized. If you're using File Synchronization, however, you wallet (your Visa card, for example) on your Windows PC and another (your calling card) on your take effect. Only whole files are synchronized.

The Status Bar at the bottom of the Windows PC version of eWallet will show you the type of sync currently opened wallet file.

Use the picks on eWallet’s Synchronization menu to change synchronization settings for your open for another wallet file, first open the file, then use the Wallet Synchronization Wizard.

See Graphics and Sounds for information about the choosing the best options for using graphics and synchronized.” Ilium at pg. 20-21.

- “SyncPro Synchronization

With SyncPro™ Synchronization, you can make simultaneous changes to different cards on your V Mobile-based Pocket PC or Smartphone, and all changes will be synchronized. SyncPro allows two one Windows Mobile device as well as an automatic wallet file copy to any other connected Wind

SyncPro is for use only with Windows Mobile-based Pocket PCs and Smartphones. If you have a F HotSync to synchronize your eWallet information.

We recommend you install the latest version of Microsoft ActiveSync for use with SyncPro.

Follow the steps below to set up your Windows PC and Pocket PC or Smartphone for synchronization

1. Make sure your Windows PC and your mobile device are connected using Microsoft ActiveS
2. Start the Wallet Synchronization Wizard by selecting Synchronization Setup from eWallet's S ready, press Next.
3. Select your device in the wizard and press Next.
4. Pick the Synchronization Action you'd like and press Next.
5. Press Finish” *Id* at 21.

The teachings of this reference are explicitly directed to systems and methods wherein a central server admin and provides mobile wallet synchronization capabilities to mobile devices. A POSITA at the relevant time v



# 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.