



## **Exhibit A**

# **Apple Infringing Functionality and Devices Preliminary Infringement Chart**

**Claim Chart of [U.S. Patent No. 8,843,125](#) as practiced by  
Apple iPhone devices (including, at least, iPhone 6, 6 Plus, 6s, 6s Plus, SE, 7, 7 Plus, 8, 8 Plus, X, XR, XS, XS Max)  
Apple Watch devices (including, at least, Series 1, Series 2, Series 3, and Series 4) implementing  
the Apple Wallet Application (collectively, “the Accused Apple Devices”)  
Claims 11, 13, 14, 16, 17, 18, 20, 21, 22, 23, 24, 25**

Claims	Infringing Functionality/Structure
<b>Claim 11</b>	
11. A method for provisioning a contactless card applet in a mobile device comprising a mobile wallet application, the method comprising:	<p>On information and belief, the Accused Apple Devices enable provisioning of a contactless card applet (e.g., a software component related to a contactless card applet in a mobile device (e.g., iPhone or Apple Watch) implementing a mobile wallet application (e.g., Apple Wallet).</p> <div style="text-align: center;">  <p><b>Find it all in Wallet.</b></p> <p>Apple Pay Cash and your credit and debit cards are in the Wallet app along with boarding passes, tickets, rewards cards, and more. You can also add your student ID card to Apple Wallet to access places like your dorm and the library, or to pay for things like laundry and snacks on campus. Apple Pay works with most credit and debit cards from <b>nearly all U.S. banks</b>. Just add your participating cards to Wallet and you'll continue to get all the rewards and benefits of your cards.</p>  <p><a href="https://www.apple.com/apple-pay/">https://www.apple.com/apple-pay/</a> (last accessed on 2/6/2019).</p> </div>

Claims	Infringing Functionality/Structure
<p>activating the mobile wallet application;</p>	<p>On information and belief, the Accused Apple Devices enable a mobile wallet application (e.g., Apple Wallet).</p> <p><b>Apple Pay components</b></p> <p><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><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><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><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>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><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>iOS Security Guide, iOS 11.4, August 2018 at p. 40.</p>

Claims	Infringing Functionality/Structure
	<p data-bbox="808 709 1611 747"><b>When you add credit, debit, prepaid, or transit cards</b></p> <p data-bbox="808 768 1624 890">When you <a href="#">add a credit, debit, prepaid, or transit card</a> (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="808 915 1624 1003">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.</p> <p data-bbox="808 1029 1624 1247">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="808 1272 1624 1583">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="808 1633 1624 1671"><a href="https://support.apple.com/en-us/HT203027">https://support.apple.com/en-us/HT203027</a> (last accessed on 2/6/2020)</p>

Claims	Infringing Functionality/Structure
	<p data-bbox="808 722 1463 758"><b>Credit, debit, and prepaid card provisioning</b></p> <p data-bbox="808 779 1624 926">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 data-bbox="808 961 1624 1115">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 data-bbox="808 1146 1624 1388">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 data-bbox="808 1419 1624 1577">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 data-bbox="808 1629 1471 1661">iOS Security Guide, iOS 11.4, August 2018 at p. 41.</p>

# 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.