

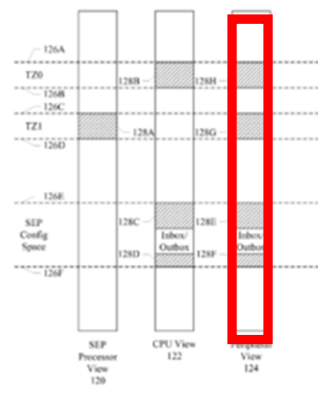
Claim Chart for U.S. Patent No. 8,620,039 (“the ’039 Patent”)

The Accused Instrumentalities include, but are not necessarily limited to, Apple iPhones, iPads equipped with Apple Card or device that is substantially or reasonably similar to the functionality set forth below. The Accused Instrumentalities infringe the claims of the ’039 Patent, as described below.

<u>Claim 13</u>	<u>Specification Support</u>	<u>Apple Card</u>
A biometric card pointer enrolment system comprising:	<p>A pointer is a computing device that points to a location in memory. ‘039 Patent, col. 7, lines 31-35; Fig. 4.</p> <p>The term “card” is synonymous with “card device,” and refers to a device containing “card information.” <i>Id.</i>, col. 1, lines 21-24.</p>	<p>Apple’s CPU processor encryption includes a pointer to a memory location at which the data to be encrypted is stored. U.S. Patent Appl. No. 2014/0089682 (“the ‘682 Application”), ¶ [0083].</p> <p>Apple Card is a Sachs-linked credit card. https://www.cnbc.com/2019/03/25/apple-unveils-new-credit-card-the-apple-card.html.</p>
a card device reader for receiving card information;	<p>A “reader” includes a receiver that receives card data from the card device. <i>Id.</i>, col. 1, lines 55-58.</p>	<p>Apple’s Secure Enclave is a separate, isolated processor built into the device’s main system-on-a-chip with a separate processor and area of memory. https://www.howtogeek.com/387934/your-smartphone-has-a-special-security-chip.-heres-how-it-works/.</p> <p>“Your fingerprint data is encrypted, stored on device, and protected with a key available only to the Secure Enclave.” https://support.apple.com/en-us/HT204587.</p> <p>Utilizing Touch ID, the Apple Card uses a “unique security and privacy architecture,” <i>i.e.</i>, the Secure Enclave receives information from the Apple Card to pair with stored fingerprint data.</p>

<u>Claim 13</u>	<u>Specification Support</u>	<u>Apple Card</u>
		<p>https://www.creditcardinsider.com/credit-cards/goldman-sachs/apple-card/.</p>
<p>a biometric reader for receiving the biometric signature;</p>	<p>A fingerprint is a biometric signature. <i>Id.</i>, col. 2, lines 18-19.</p>	<p>The Home Button on the Apple iPhone receives fingerprint data to enroll a fingerprint. https://support.apple.com/en-us/HT201371#setup.</p>
<p>means¹ for defining, dependent upon the received card information, a memory location in a local memory external to the card;</p>	<p>Computer code defines a memory location for a biometric signature based upon provided card information. <i>See, e.g., id.</i>, col. 4, lines 62-67.</p>	<p>Apple’s Secure Enclave is a separate, isolated processor built into the device’s main system-on-a-chip with a separate processor and area of memory. https://www.howtogeek.com/387934/your-smartphone-has-a-special-security-chip.-heres-how-it-works/.</p> <p>Apple Card is built into the Apple Wallet app on iPhone, <i>i.e.</i>, the Secure Enclave memory is external to the Apple Card. <i>See</i> https://www.apple.com/newsroom/2019/03/introducing-apple-card-a-new-kind-of-credit-card-created-by-apple/.</p> <p>The address locations of an Apple security enclave are depicted below:</p>

¹ “An element in a claim for a combination may be expressed as a means or step for performing a specified function without the recital of structure, material, or acts in support thereof, and such claim shall be construed to cover the corresponding structure, material, or acts described in the specification and equivalents thereof.” 35 U.S.C. § 112.

<u>Claim 13</u>	<u>Specification Support</u>	<u>Apple Card</u>
		 <p data-bbox="1071 714 1543 755">'682 Application, ¶ [0018] & Fig. 7.</p>
<p data-bbox="199 763 556 868">means for determining if the defined memory location is unoccupied; and</p>	<p data-bbox="577 763 1060 966">Computer code determines whether the memory location defined by the provided card information is unoccupied. <i>See, e.g., id.</i>, col. 5, lines 21-23.</p>	<p data-bbox="1071 763 1890 836">Up to five fingerprints can be registered for Apple Touch ID. https://support.apple.com/en-us/HT201371.</p> <p data-bbox="1071 885 1890 1047">Deleting a stored fingerprint requires user action, i.e., stored fingerprints are not over-written by new fingerprints once the five fingerprint maximum has been reached. https://support.apple.com/en-us/HT201371.</p> <p data-bbox="1071 1096 1890 1258">The foregoing evidences that each registered fingerprint is stored in a separate memory location that must be empty to accommodate such storage, which requires determining that a memory address is unoccupied.</p>
<p data-bbox="199 1266 556 1372">means for storing, if the memory location is unoccupied, the biometric</p>	<p data-bbox="577 1266 1060 1380">Computer code for storing, if a memory location defined by the card information is unoccupied, the</p>	<p data-bbox="1071 1266 1890 1380">“Your fingerprint data is encrypted, stored on device, and protected with a key available only to the Secure Enclave.” https://support.apple.com/en-us/HT204587.</p>

<u>Claim 13</u>	<u>Specification Support</u>	<u>Apple Card</u>
signature at the defined memory location.	biometric signature at the defined memory location. <i>See, e.g., id.</i> , col. 5, lines 21-23.	<p>New fingerprint data is enrolled via Touch ID for comparison against fingerprint data subsequently acquired by the Touch ID sensor. iOS Security (Sept. 2014) at 7.</p> <p>Each stored fingerprint is identified to a user in a list presented in the interface, evidencing fingerprint storage:</p> 