

# EXHIBIT D

## EXHIBIT D

### UNITED STATES PATENT NO. 6,008,737

#### PRELIMINARY INFRINGEMENT CONTENTIONS<sup>1</sup>

**Accused Apple Products:** Apple iPhone 3G, Apple iPhone 3GS, Apple iPhone 4, and Apple iPhone 4S, Apple iPhone 5<sup>2</sup>, Apple iPad, Apple iPad with 3G, Apple iPad 2, Apple iPad 2 with 3G, 3rd Generation Apple iPad, 3rd Generation Apple iPad + 4G, 4<sup>th</sup> Generation Apple iPad<sup>3</sup>, 4<sup>th</sup> Generation Apple iPad [with cellular], Apple iPad mini<sup>4</sup>, Apple iPad mini [with cellular], 3<sup>rd</sup> Generation Apple iPod Touch, 4<sup>th</sup> Generation Apple iPod Touch, 5<sup>th</sup> Generation Apple iPod Touch<sup>5</sup> (collectively, "Apple Phones"), Apple Mac Pro, Apple iMac, new Apple iMac<sup>6</sup>, Apple Mac mini, new Apple Mac mini<sup>7</sup>, Apple MacBook, Apple

---

<sup>1</sup> Motorola Mobility's investigation is ongoing and discovery is not yet complete. Apple has, thus far, not produced all of its documents and source code relevant to the accused methods and products. Motorola reserves the right to supplement or amend these contentions based on subsequent discovery or disclosures made pursuant to FRCP 26. Motorola further reserves the right to amend and supplement its contentions with respect to any products released by Apple subsequent to the service of these initial infringement contentions, in accordance with the schedule set forth in the Court's Order of October 25, 2012. Further, to the extent Apple releases any new products with the same functionality accused of infringement in the Accused Apple Products in these contentions, Motorola reserves the right to seek appropriate relief from the court in accordance with its order of October 25, 2012 and in accordance with the Federal Rules of Civil Procedure.

<sup>2</sup> The term "Apple iPhone 5" means Apple's new iPhone announced by Apple on September 12, 2012. *See* <http://www.apple.com/pr/library/2012/09/12Apple-Introduces-iPhone-5.html>.

<sup>3</sup> The terms "4<sup>th</sup> Generation Apple iPad" and "4<sup>th</sup> Generation Apple iPad [with cellular]" mean Apple's new iPad devices announced by Apple on October 23, 2012. *See* <http://www.apple.com/pr/library/2012/10/23Apple-Introduces-iPad-mini.html>.

<sup>4</sup> The terms "Apple iPad mini" and "Apple iPad mini [with cellular]" mean Apple's new iPad mini devices announced by Apple on October 23, 2012. *See* <http://www.apple.com/pr/library/2012/10/23Apple-Introduces-iPad-mini.html>.

<sup>5</sup> The term "5<sup>th</sup> Generation Apple iPod Touch" means Apple's new iPod Touch announced by Apple on September 12, 2012. *See* <http://www.apple.com/pr/library/2012/09/12Apple-Introduces-New-iPod-touch-iPod-nano.html>.

<sup>6</sup> The term "new Apple iMac" means Apple's new iMac computers announced by Apple on October 23, 2012. *See* <http://www.apple.com/pr/library/2012/10/23All-New-iMac-Features-Stunning-Design-Brilliant-Display-Faster-Performance.html>.

<sup>7</sup> The term "new Apple Mac mini" means Apple's new Mac mini computers announced by Apple on October 23, 2012. *See* <http://www.apple.com/pr/library/2012/10/23All-New-iMac-Features-Stunning-Design-Brilliant-Display-Faster-Performance.html>.

**EXHIBIT D**

MacBook Pro, 15-inch Apple MacBook Pro with Retina Display, 13-inch Apple MacBook Pro with Retina Display<sup>8</sup>, Apple MacBook, and Apple MacBook Air (collectively, "Apple Computers").

Apple directly infringes the ‘737 patent, either literally or through the doctrine of equivalents, pursuant to 35 U.S.C. § 271(a).

In addition to Apple's direct infringement of the ‘737 patent through its development, testing, use, distribution and sale of its products and services, Apple also indirectly infringes the ‘737 patent pursuant to 35 U.S.C. § 271(b) and (c). End-users and others in the distribution channel of the Accused Apple Products directly infringe this claim by using, selling, offering for sale, and/or importing these devices into the United States. Apple contributes to and induces infringement through its promotion and provision of marketing, sale and/or technical support of the Accused Apple Products and associated services in the United States, and through the design, marketing, manufacture, sale, and/or technical support of the Accused Apple Products. Apple supplies Accused Apple Products and actively encourages the use, sale, offer for sale, and importation of the same in the United States through the promotion and provision of marketing literature, promotion, and user guides, which induces and results in direct infringement. Apple has known or should have known that these actions would cause direct infringement of the ‘737 patent and did so with specific intent to encourage direct infringement, at least as of 2007, when Apple and Motorola participated in talks regarding the licensing of Motorola's patent portfolio. On information and belief, in connection with those negotiations, Apple has reviewed said portfolio, including Motorola's ‘737 Patent. Moreover, Apple has known of the ‘737 patent since at least October 6, 2010, when Motorola filed its Complaint, attaching the ‘737 patent as an exhibit. Despite knowing of the ‘737 patent, Apple continues to make, use, offer to sell, and sell its products and has continued to circulate marketing literature and user guides encouraging users of the Accused Apple Products to infringe. Additionally, the identified features of the Accused Apple Products are material parts of the inventions of the asserted claims and have no substantial non-infringing uses.

<b>‘737 Patent Claim</b>	<b>Accused Apple Products<sup>9</sup></b>
--------------------------	---


<sup>8</sup> The term "13-inch Apple MacBook Pro with Retina Display" means Apple's new 13-inch MacBook Pro computer announced by Apple on October 23, 2012. See <http://www.apple.com/pr/library/2012/10/23Apple-Introduces-13-inch-MacBook-Pro-with-Retina-Display.html>.

<sup>9</sup> This chart provides Motorola’s infringement analysis for the Accused Apple Products. Upon information and belief, the analysis set forth in this chart for applies equally to all of the Accused Apple Products.

**EXHIBIT D**

<b>'737 Patent Claim</b>	<b>Accused Apple Products<sup>9</sup></b>
9. A portable communication device in a communication system having a fixed portion, the portable communication device comprising:	Upon information and belief, Apple imports, manufactures, sells, offers to sell, and uses the Accused Apple Products, which are portable communication devices. Moreover, the Accused Apple Products operate in the normal course of use in a communication system having a fixed portion, which is the authentication system used in one or more of Apple's iTunes, Apple's App Store, and Apple's enterprise application system.  <i>See, e.g.,</i> iPhone 4 Technical Specifications, ( <a href="http://www.apple.com/iphone/specs.html">http://www.apple.com/iphone/specs.html</a> ), accessed on May 12, 2011, MOTO-APPLE-0006037953_126659:

**EXHIBIT D**

'737 Patent Claim	Accused Apple Products <sup>9</sup>
	<p><b>Size and weight<sup>1</sup></b></p> <p>Height: <b>4.5 inches</b> (115.2 mm) Width: <b>2.31 inches</b> (58.6 mm) Depth: <b>0.37 inch</b> (9.3 mm) Weight: <b>4.8 ounces</b> (137 grams)</p>  <p><b>Cellular and wireless</b></p> <ul style="list-style-type: none"><li>■ UMTS/HSDPA/HSUPA (850, 900, 1900, 2100 MHz)</li><li>■ GSM/EDGE (850, 900, 1800, 1900 MHz)</li><li>■ 802.11b/g/n Wi-Fi (802.11n 2.4GHz only)</li><li>■ Bluetooth 2.1 + EDR wireless technology</li></ul> <p>See also, iPhone 5 Technical Specifications, (<a href="http://www.apple.com/iphone/specs.html">http://www.apple.com/iphone/specs.html</a>), accessed on 11/06/2012, MOTO-SDFL-0000016104.</p>

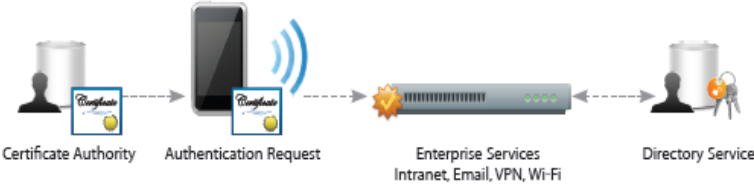
**EXHIBIT D**

‘737 Patent Claim	Accused Apple Products <sup>9</sup>
	<p>Cellular and Wireless</p> <ul style="list-style-type: none"> <li>• GSM model A1428*: UMTS/HSPA+/DC-HSDPA (850, 900, 1900, 2100 MHz); GSM/EDGE (850, 900, 1800, 1900 MHz); LTE (Bands 4 and 17)</li> <li>• CDMA model A1429*: CDMA EV-DO Rev. A and Rev. B (800, 1900, 2100 MHz); UMTS/HSPA+/DC-HSDPA (850, 900, 1900, 2100 MHz); GSM/EDGE (850, 900, 1800, 1900 MHz); LTE (Bands 1, 3, 5, 13, 25)</li> <li>• GSM model A1429*: UMTS/HSPA+/DC-HSDPA (850, 900, 1900, 2100 MHz); GSM/EDGE (850, 900, 1800, 1900 MHz); LTE (Bands 1, 3, 5)</li> <li>• 802.11a/b/g/n Wi-Fi (802.11n 2.4GHz and 5GHz)</li> <li>• Bluetooth 4.0 wireless technology</li> </ul> <p>See also e.g., Apple iPad Technical Specifications, (<a href="http://www.apple.com/ipad/specs">www.apple.com/ipad/specs</a>), accessed on April 12, 2011, MOTO-APPLE-0005383110_35376:</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>Wireless and Cellular</p> <ul style="list-style-type: none"> <li>■ Wi-Fi (802.11a/b/g/n)</li> <li>■ Bluetooth 2.1 + EDR technology</li> </ul> <ul style="list-style-type: none"> <li>■ Wi-Fi + 3G model: UMTS/HSDPA/HSUPA (850, 900, 1900, 2100 MHz); GSM/EDGE (850, 900, 1800, 1900 MHz)</li> <li>■ Wi-Fi + 3G for Verizon model: CDMA EV-DO Rev. A (800, 1900 MHz)</li> <li>■ Data only*</li> <li>■ Wi-Fi (802.11 a/b/g/n)</li> <li>■ Bluetooth 2.1 + EDR technology</li> </ul> <p style="text-align: right;"><a href="#">Learn more about Wi-Fi + 3G ▶</a></p> </div> <p>See also, e.g., MacBook Pro 15" Core 2 Duo Model A1211 Teardown, (<a href="http://www.ifixit.com/Teardown/MacBook-Pro-15-Inch-Core-2-Duo-Model-A1211-Teardown/593/1">http://www.ifixit.com/Teardown/MacBook-Pro-15-Inch-Core-2-Duo-Model-A1211-Teardown/593/1</a>), accessed on May 14, 2011, MOTO-APPLE-0006037953_127250:</p>

**EXHIBIT D**

‘737 Patent Claim	Accused Apple Products <sup>9</sup>
	<div data-bbox="619 248 1312 592"> </div> <p data-bbox="604 613 1917 1120">In addition, Apple has performed each and every step of this claim, and, through its design of the Accused Apple Products, Apple also contributes to the infringement of the '737 patent by users of the device. Apple and Motorola have been in talks since 2007 regarding the licensing of Motorola's patent portfolio, and, on information and belief, in accordance with those negotiations, Apple has reviewed said portfolio, including Motorola's '737 Patent. Thus, at least as early as 2007, Apple knew that offering to sell or selling the Accused Apple Products would contribute to direct infringement of the '737 Patent. Apple knew that the Accused Apple Products contain two specific components for sending and receiving authorization requests and responses. Apple knew that these components could be combined and had no substantial non-infringing use, and that the combination, for which the two components were especially made, was both patented and infringing. Moreover, Accused Apple Products users have, in fact, combined these components into an infringing device. Apple further contributes to the direct infringement of the users of the Accused Apple Products, including but not limited to by describing infringing combinations in its advertisements, promotional materials, and user manuals. <i>See e.g.</i>, iPhone in Business: Security Overview, MOTO-APPLE-0006037953_126666.</p> <p data-bbox="619 1149 877 1174"><b>Mandatory Code Signing</b></p> <p data-bbox="619 1179 1465 1328">All iPhone applications must be signed. The applications provided with the device are signed by Apple. Third-party applications are signed by the developer using an Apple-issued certificate. This ensures that applications haven't been tampered with or altered. Additionally, runtime checks are made to ensure that an application hasn't become untrusted since it was last used.</p> <p data-bbox="604 1356 1732 1388"><i>See also</i> iPhone in Business: Digital Certificates, MOTO-APPLE-0006037953_126669:</p>

**EXHIBIT D**

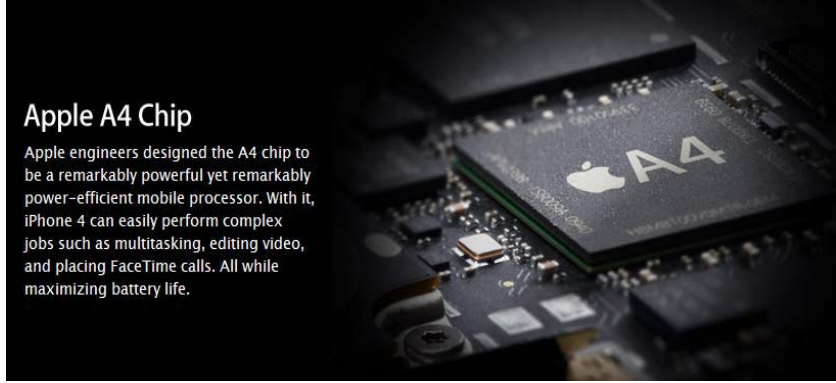

‘737 Patent Claim	Accused Apple Products <sup>9</sup>
	<p><b>Digital certificates</b></p> <p>Digital certificates can be used to securely authenticate users to corporate services without the need for user names, passwords or soft tokens. On iPhone, certificate-based authentication is supported for access to Microsoft Exchange ActiveSync, VPN, and Wi-Fi networks.</p>  <p>The diagram illustrates the process of digital certificate authentication. On the left, a 'Certificate Authority' (represented by a server icon) issues a 'Certificate' (represented by a document icon) to an iPhone. The iPhone then sends an 'Authentication Request' (represented by a document icon with a signal wave) to 'Enterprise Services' (represented by a server rack icon), which includes 'Intranet, Email, VPN, Wi-Fi'. Finally, the Enterprise Services connect to a 'Directory Service' (represented by a server icon with a key icon).</p> <p><i>See also id.:</i></p> <p>iPhone supports digital certificates, giving business users secure, streamlined access to corporate services. A digital certificate is composed of a public key, information about the user, and the certificate authority that issued the certificate. Digital certificates are a form of identification that enables streamlined authentication, data integrity, and encryption.</p> <p>On iPhone, certificates can be used in a variety of ways. Signing data with a digital certificate helps to ensure that information cannot be altered. Certificates can also be used to guarantee the identity of the author or “signer.” Additionally, they can be used to encrypt configuration profiles and network communications to further protect confidential or private information.</p> <p><i>See also</i> Distributing Enterprise Apps for iOS 4 Devices, (<a href="http://developer.apple.com/library/ios/#featuredarticles/FA_Wireless_Enterprise_App_Distribution/Introduction/Introduction.html">http://developer.apple.com/library/ios/#featuredarticles/FA_Wireless_Enterprise_App_Distribution/Introduction/Introduction.html</a>), accessed on May 12, 2011, MOTO-APPLE-0006037953_126598:</p> <p><b>"Certificate Validation.</b> The first time an application is opened on a device, the distribution certificate is validated by contacting Apple's OCSP server. Unless the certificate has been revoked, the app is allowed to run. Inability to contact or get a response from the OCSP server is not interpreted as a revocation. To verify the status, the device must be able to reach ocsf.apple.com. See 'Network Configuration Requirements.'</p>



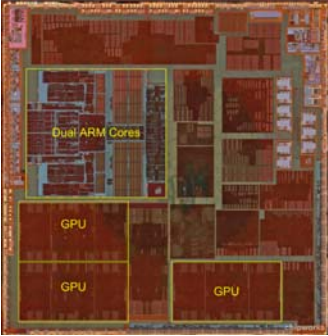

**EXHIBIT D**

‘737 Patent Claim	Accused Apple Products <sup>9</sup>
	<p>The OCSF response is cached on the device for the period of time specified by the OCSF server; currently between 3 and 7 days. The validity of the certificate will not be checked again until the device has restarted and the cached response has expired. If a revocation is received at that time, the app will be prevented from running. Note that revoking a distribution certificate will invalidate all of the applications you have distributed.</p> <p>An app will not run if the distribution certificate has expired. Currently, distribution certificates are valid for one year. A few weeks before your certificate expires request a new distribution certificate from the Dev Center, use it create new distribution provisioning profiles, then recompile and distribute the updated apps to your users. See 'Providing Updated Apps.'</p> <p><i>See also</i> Developer Library—Authentication and Authorization, (<a href="http://developer.apple.com/library/ios/#documentation/Security/Conceptual/Security_Overview/AuthenticationAndAuthorization/AuthenticationAndAuthorization.html#//apple_ref/doc/uid/TP30000976-CH2-SW1">http://developer.apple.com/library/ios/#documentation/Security/Conceptual/Security_Overview/AuthenticationAndAuthorization/AuthenticationAndAuthorization.html#//apple_ref/doc/uid/TP30000976-CH2-SW1</a>), accessed on 11/06/2012, MOTO-SDFL-0000018762:</p> <p>The details of authorization depend on the platform you are using: <b>In iOS</b>, the user can set a passcode (which by default is a four-digit personal identification number) to prevent unauthorized use of the device. After entering this passcode, the user of the device is presumed to be authorized to use the device. In addition, each app is digitally signed and can therefore be authenticated by the operating system. Therefore, there are no user authentication or authorization APIs in iOS.</p> <p><b>In OS X</b>, there are several layers of authorization:</p> <ul style="list-style-type: none"> <li>• If FileVault 2 (full-disk encryption) is enabled, the computer requires a password to decrypt the boot volume.</li> <li>• If automatic login is disabled, OS X displays a login screen after booting.</li> <li>• OS X also displays a login screen when the user logs out.</li> <li>• If the appropriate checkbox in the Security system preferences pane is checked, OS X displays a login screen when waking from sleep or when leaving a screen saver.</li> <li>• When an app or tool requests access to a locked keychain, a password is required.</li> <li>• If an app or tool needs elevated privileges, an administrator password is required.</li> <li>• Some apps may restrict access to parts of their functionality through the Authorization Services API.</li> </ul> <p>In addition, on both OS X and iOS, some apps may require you to log in to a remote server, which in turn performs authentication and authorization.</p>

**EXHIBIT D**

<b>'737 Patent Claim</b>	<b>Accused Apple Products<sup>9</sup></b>
a processor;	<p>Upon information and belief, the Apple Phones contain a variety of different processors, such as an Apple A4 processor, and Apple Computers contain a variety of different processors, such as the 2.4GHz Intel Core 2 Duo processor.</p> <p><i>See, e.g.,</i> (<a href="http://www.apple.com/channel/iphone/iphone-4/best-buy/design.html">http://www.apple.com/channel/iphone/iphone-4/best-buy/design.html</a>), accessed May 12, 2011, MOTO-APPLE-0006037953_127201:</p> <div data-bbox="606 461 1436 841"><p><b>Apple A4 Chip</b></p><p>Apple engineers designed the A4 chip to be a remarkably powerful yet remarkably power-efficient mobile processor. With it, iPhone 4 can easily perform complex jobs such as multitasking, editing video, and placing FaceTime calls. All while maximizing battery life.</p></div> <p><i>See also e.g.,</i> Apple iPad Technical Specifications, (<a href="http://www.apple.com/ipad/specs">www.apple.com/ipad/specs</a>), accessed on April 12, 2011, MOTO-APPLE-0005383110_35376:</p> <div data-bbox="606 948 1335 1101"><p>Chip</p><p>1GHz dual-core Apple A5 custom-designed, high-performance, low-power system-on-a-chip</p></div> <p><i>See also,</i> iPhone 5 teardown analysis –A6 processor (<a href="http://www.ifixit.com/Teardown/Apple-A6-Teardown/10528/2">http://www.ifixit.com/Teardown/Apple-A6-Teardown/10528/2</a>), accessed on 11/06/2012, MOTO-SDFL-0000016113:</p>

**EXHIBIT D**

‘737 Patent Claim	Accused Apple Products <sup>9</sup>
	 <p data-bbox="611 621 1703 724"><i>See also, e.g.,</i> MacBook Pro 15" Core 2 Duo Model A1211 Teardown, (<a href="http://www.ifixit.com/Teardown/MacBook-Pro-15-Inch-Core-2-Duo-Model-A1211-Teardown/593/1">http://www.ifixit.com/Teardown/MacBook-Pro-15-Inch-Core-2-Duo-Model-A1211-Teardown/593/1</a>), accessed on May 14, 2011, MOTO-APPLE-0006037953_127248:</p>  <p data-bbox="632 1149 1094 1214"><b>MacBook Pro 15" Core 2 Duo Model A1211</b></p> <p data-bbox="632 1230 1010 1255">2.16 or 2.33 GHz Core 2 Duo processor</p>
<p>an authorization element coupled to the processor for obtaining usage authorization for utilizing software in the</p>	<p>Upon information and belief, the Accused Apple Products contain an authorization element coupled to the processor for obtaining usage authorization for utilizing software in the Apple product:</p>

**EXHIBIT D**

‘737 Patent Claim	Accused Apple Products <sup>9</sup>
portable communication device,	<p><b>Mandatory Code Signing</b>            All iPhone applications must be signed. The applications provided with the device are signed by Apple. Third-party applications are signed by the developer using an Apple-issued certificate. This ensures that applications haven't been tampered with or altered. Additionally, runtime checks are made to ensure that an application hasn't become untrusted since it was last used.</p> <p>iPhone in Business: Security Overview, MOTO-APPLE-0006037953_126666.  <i>See also</i> iPhone in Business: Digital Certificates, MOTO-APPLE-0006037953_126669:</p> <p><b>Digital certificates</b>            Digital certificates can be used to securely authenticate users to corporate services without the need for user names, passwords or soft tokens. On iPhone, certificate-based authentication is supported for access to Microsoft Exchange ActiveSync, VPN, and Wi-Fi networks.</p>  <p><i>See also id.:</i></p> <p>iPhone supports digital certificates, giving business users secure, streamlined access to corporate services. A digital certificate is composed of a public key, information about the user, and the certificate authority that issued the certificate. Digital certificates are a form of identification that enables streamlined authentication, data integrity, and encryption.</p> <p>On iPhone, certificates can be used in a variety of ways. Signing data with a digital certificate helps to ensure that information cannot be altered. Certificates can also be used to guarantee the identity of the author or "signer." Additionally, they can be used to encrypt configuration profiles and network communications to further protect confidential or private information.</p> <p><i>See also</i> Distributing Enterprise Apps for iOS 4 Devices,  <a href="http://developer.apple.com/library/ios/#featuredarticles/FA_Wireless_Enterprise_App_Distribution/I">http://developer.apple.com/library/ios/#featuredarticles/FA_Wireless_Enterprise_App_Distribution/I</a></p>

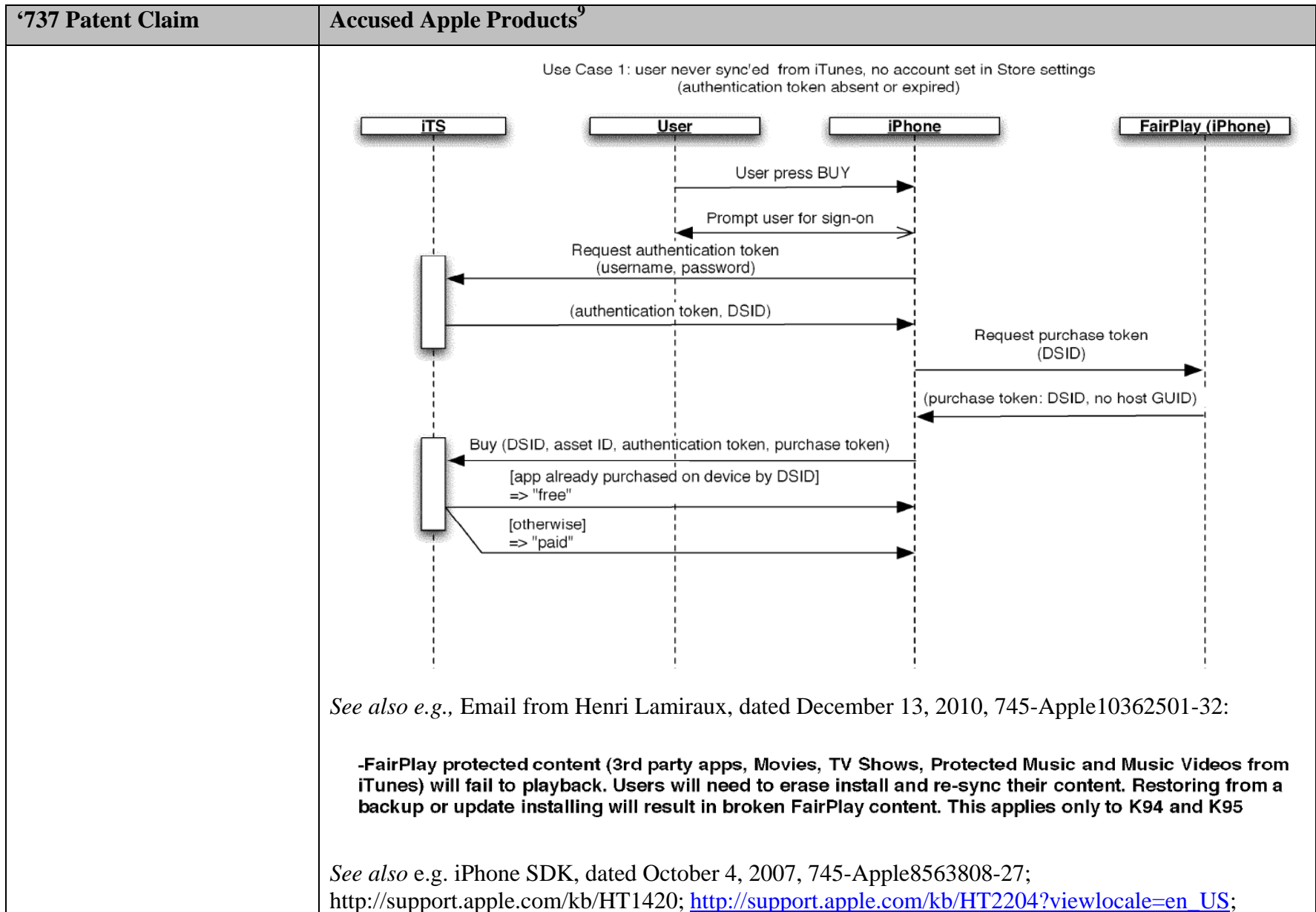
**EXHIBIT D**

<b>'737 Patent Claim</b>	<b>Accused Apple Products<sup>9</sup></b>
	<p><a href="#">ntroduction/Introduction.html</a>), accessed on May 12, 2011, MOTO-APPLE-0006037953_126598:</p> <p><b>"Certificate Validation.</b> The first time an application is opened on a device, the distribution certificate is validated by contacting Apple's OCSP server. Unless the certificate has been revoked, the app is allowed to run. Inability to contact or get a response from the OCSP server is not interpreted as a revocation. To verify the status, the device must be able to reach ocsf.apple.com. See 'Network Configuration Requirements.'</p> <p>The OCSP response is cached on the device for the period of time specified by the OCSP server; currently between 3 and 7 days. The validity of the certificate will not be checked again until the device has restarted and the cached response has expired. If a revocation is received at that time, the app will be prevented from running. Note that revoking a distribution certificate will invalidate all of the applications you have distributed.</p> <p>An app will not run if the distribution certificate has expired. Currently, distribution certificates are valid for one year. A few weeks before your certificate expires request a new distribution certificate from the Dev Center, use it create new distribution provisioning profiles, then recompile and distribute the updated apps to your users. See 'Providing Updated Apps.'"</p> <p><i>See also</i> Developer Library—Authentication and Authorization, (<a href="http://developer.apple.com/library/ios/#documentation/Security/Conceptual/Security_Overview/AuthenticationAndAuthorization/AuthenticationAndAuthorization.html#//apple_ref/doc/uid/TP30000976-CH2-SW1">http://developer.apple.com/library/ios/#documentation/Security/Conceptual/Security_Overview/AuthenticationAndAuthorization/AuthenticationAndAuthorization.html#//apple_ref/doc/uid/TP30000976-CH2-SW1</a>), accessed on 11/06/2012, MOTO-SDFL-0000018762 (emphasis added):</p> <p>The details of authorization depend on the platform you are using: <b>In iOS</b>, the user can set a passcode (which by default is a four-digit personal identification number) to prevent unauthorized use of the device. After entering this passcode, the user of the device is presumed to be authorized to use the device. In addition, <u>each app is digitally signed and can therefore be authenticated by the operating system.</u> Therefore, there are no user authentication or authorization APIs in iOS.</p>

**EXHIBIT D**

<b>'737 Patent Claim</b>	<b>Accused Apple Products<sup>9</sup></b>
	<p><u>Communications with the Apple App store</u>. In connection with a request to use or download software onto an Accused Apple Product, an authorization element coupled to the processor of that Accused Apple Product requests usage authorization for utilizing that software in the Accused Apple Product.</p> <p><i>See also e.g.</i>, Email from Dallas De Atley, dated December 14, 2010, 745-Apple10360097-98:</p> <ul style="list-style-type: none"><li>&gt; The ability to run applications on a device is controlled by two mechanisms:</li><li>&gt;</li><li>&gt; 1) Code signing enforced by the kernel</li><li>&gt;</li><li>&gt; All applications must be signed by Apple before the kernel will run them.</li><li>&gt;</li><li>&gt; 2) Encryption enforced by FairPlay</li><li>&gt;</li><li>&gt; All applications are also encrypted with FairPlay, and decoded in the kernel by the FairPlay engine.</li><li>&gt; The use of FairPlay allows us to tie the application to a particular user more than a particular device.</li></ul> <p><i>See also e.g.</i>, iTunes Authentication Use Case Chart, 745-Apple5374978-81:</p>

**EXHIBIT D**

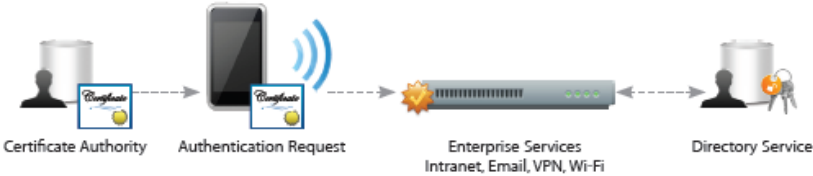


**EXHIBIT D**

‘737 Patent Claim	Accused Apple Products <sup>9</sup>
	<p><a href="http://support.apple.com/kb/HE37">http://support.apple.com/kb/HE37</a></p>
<p>in which the authorization element generates an external authorization request, and</p>	<p>Upon information and belief, the authorization element in the Accused Apple Products generates an external authorization request sent to Apple's iTunes, Apple's App Store authentication servers and / or Apple's enterprise application system. For example, the digital certificate is validated by contacting an external OCSP server (external authorization request) upon initial opening, and by a runtime check (external authorization request) at each time of use.</p> <p>See Distributing Enterprise Apps for iOS 4 Devices, (<a href="http://developer.apple.com/library/ios/#featuredarticles/FA_Wireless_Enterprise_App_Distribution/Introduction/Introduction.html">http://developer.apple.com/library/ios/#featuredarticles/FA_Wireless_Enterprise_App_Distribution/Introduction/Introduction.html</a>), accessed on May 12, 2011, MOTO-APPLE-0006037953_126598:</p> <p><b>"Certificate Validation.</b> The first time an application is opened on a device, the distribution certificate is validated by contacting Apple's OCSP server. Unless the certificate has been revoked, the app is allowed to run. Inability to contact or get a response from the OCSP server is not interpreted as a revocation. To verify the status, the device must be able to reach <a href="http://ocsp.apple.com">ocsp.apple.com</a>. See 'Network Configuration Requirements.'</p> <p>The OCSP response is cached on the device for the period of time specified by the OCSP server; currently between 3 and 7 days. The validity of the certificate will not be checked again until the device has restarted and the cached response has expired. If a revocation is received at that time, the app will be prevented from running. Note that revoking a distribution certificate will invalidate all of the applications you have distributed.</p> <p>An app will not run if the distribution certificate has expired. Currently, distribution certificates are valid for one year. A few weeks before your certificate expires request a new distribution certificate from the Dev Center, use it create new distribution provisioning profiles, then recompile and distribute the updated apps to your users. See 'Providing Updated Apps.'"</p> <p>See also iPhone in Business: Security Overview, MOTO-APPLE-0006037953_126666:</p>



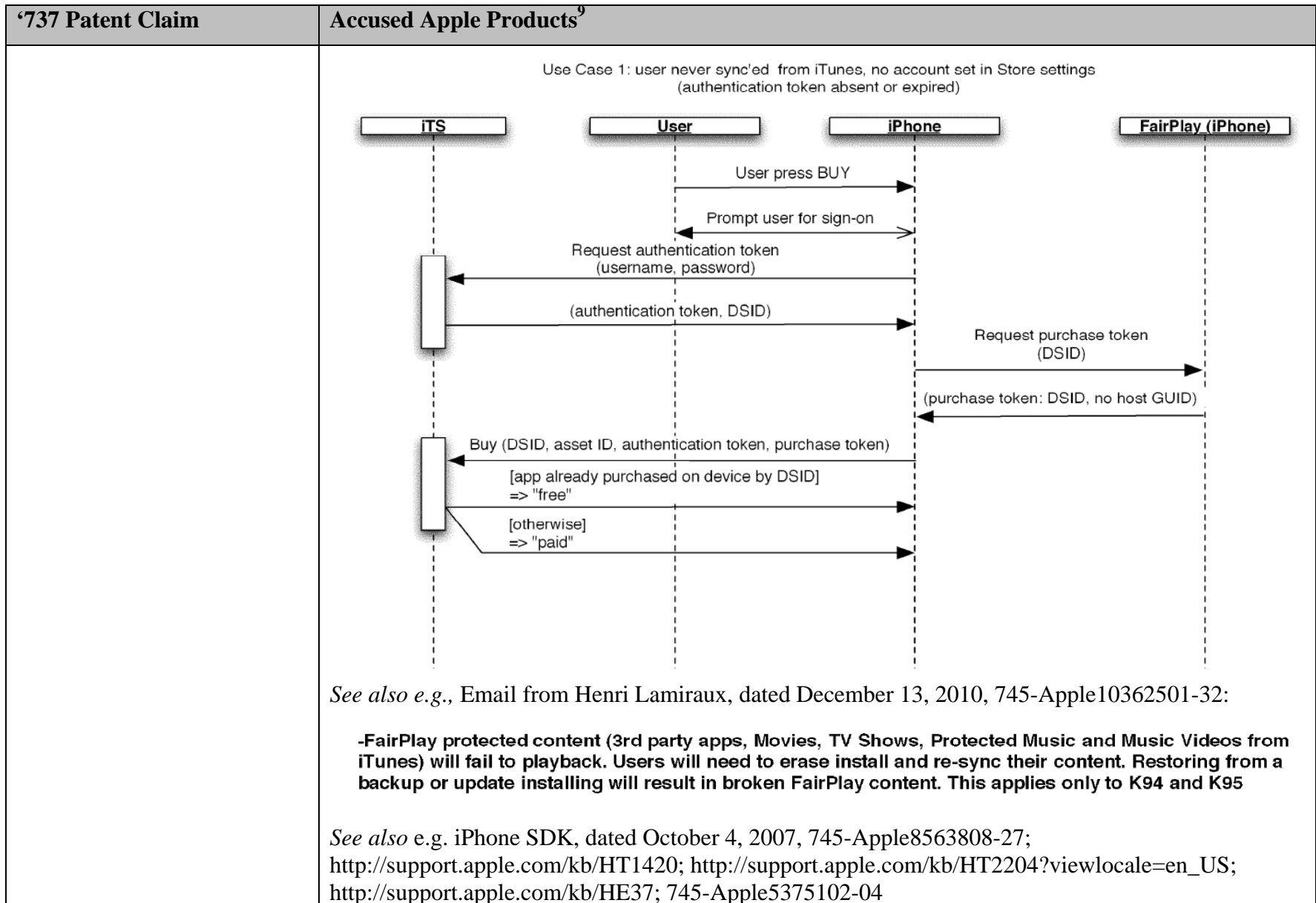
**EXHIBIT D**

‘737 Patent Claim	Accused Apple Products <sup>9</sup>
	<p><b>Mandatory Code Signing</b>            All iPhone applications must be signed. The applications provided with the device are signed by Apple. Third-party applications are signed by the developer using an Apple-issued certificate. This ensures that applications haven't been tampered with or altered. Additionally, runtime checks are made to ensure that an application hasn't become untrusted since it was last used.</p> <p><i>See also</i> iPhone in Business: Digital Certificates, MOTO-APPLE-0006037953_126669:</p> <p><b>Digital certificates</b>            Digital certificates can be used to securely authenticate users to corporate services without the need for user names, passwords or soft tokens. On iPhone, certificate-based authentication is supported for access to Microsoft Exchange ActiveSync, VPN, and Wi-Fi networks.</p>  <p>The diagram illustrates the authentication process. On the left, a 'Certificate Authority' (represented by a server icon) issues a 'Certificate' (represented by a document icon) to an iPhone. The iPhone then sends an 'Authentication Request' (represented by a document icon with a signal wave) to 'Enterprise Services' (represented by a server rack icon). Below this icon are the labels 'Intranet, Email, VPN, Wi-Fi'. Finally, the Enterprise Services connect to a 'Directory Service' (represented by a server icon with a key icon).</p> <p><u>Communications with the Apple App store.</u> In connection with a request to use software on or download software onto an Accused Apple Product, an authorization element coupled to the processor of that Accused Apple Product requests usage authorization for utilizing that software in the Accused Apple Product. The authorization element within the Accused Apple Product generates an external authorization request in order to secure this authorization.</p> <p><i>See also e.g.</i>, Email from Dallas De Atley, dated December 14, 2010, 745-Apple10360097-98:</p>

**EXHIBIT D**

<b>'737 Patent Claim</b>	<b>Accused Apple Products<sup>9</sup></b>
	<ul style="list-style-type: none"><li>&gt; The ability to run applications on a device is controlled by two mechanisms:</li><li>&gt;</li><li>&gt; 1) Code signing enforced by the kernel</li><li>&gt;</li><li>&gt; All applications must be signed by Apple before the kernel will run them.</li><li>&gt;</li><li>&gt; 2) Encryption enforced by FairPlay</li><li>&gt;</li><li>&gt; All applications are also encrypted with FairPlay, and decoded in the kernel by the FairPlay engine.</li><li>&gt; The use of FairPlay allows us to tie the application to a particular user more than a particular device.</li></ul> <p><i>See also e.g., iTunes Authentication Use Case Chart, 745-Apple5374978-81:</i></p>

**EXHIBIT D**



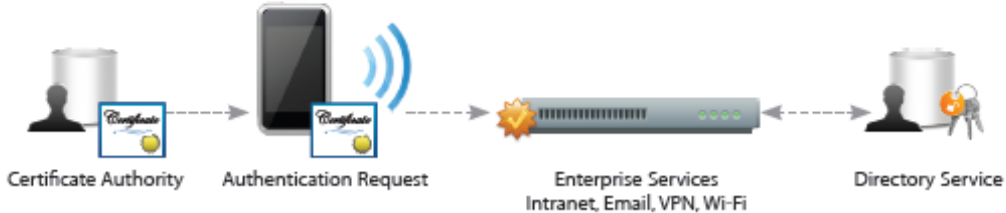
**EXHIBIT D**

‘737 Patent Claim	Accused Apple Products <sup>9</sup>
	<p>See also Developer Library—Authentication and Authorization, (<a href="http://developer.apple.com/library/ios/#documentation/Security/Conceptual/Security_Overview/AuthenticationAndAuthorization/AuthenticationAndAuthorization.html#//apple_ref/doc/uid/TP30000976-CH2-SW1">http://developer.apple.com/library/ios/#documentation/Security/Conceptual/Security_Overview/AuthenticationAndAuthorization/AuthenticationAndAuthorization.html#//apple_ref/doc/uid/TP30000976-CH2-SW1</a>), accessed on 11/06/2012, MOTO-SDFL-0000018762 (emphasis added):</p> <p>The details of authorization depend on the platform you are using: <b>In iOS</b>, the user can set a passcode (which by default is a four-digit personal identification number) to prevent unauthorized use of the device. After entering this passcode, the user of the device is presumed to be authorized to use the device. In addition, <u>each app is digitally signed and can therefore be authenticated by the operating system.</u> Therefore, there are no user authentication or authorization APIs in iOS.</p> <p><b>In OS X</b>, there are several layers of authorization:</p> <ul style="list-style-type: none"> <li>• If FileVault 2 (full-disk encryption) is enabled, the computer requires a password to decrypt the boot volume.</li> <li>• If automatic login is disabled, OS X displays a login screen after booting.</li> <li>• OS X also displays a login screen when the user logs out.</li> <li>• If the appropriate checkbox in the Security system preferences pane is checked, OS X displays a login screen when waking from sleep or when leaving a screen saver.</li> <li>• When an app or tool requests access to a locked keychain, a password is required.</li> <li>• <u>If an app or tool needs elevated privileges, an administrator password is required.</u></li> <li>• <u>Some apps may restrict access to parts of their functionality through the Authorization Services API.</u></li> </ul> <p>In addition, on <u>both OS X and iOS</u>, some apps may require you to log in to a remote server, which in turn performs authentication and authorization.</p>
<p>in which the authorization element communicates with the fixed portion to obtain the usage authorization in response to the external authorization request, and</p>	<p>Upon information and belief, the authorization element in the Accused Apple Products communicates with the fixed portion (<i>i.e.</i>, the authentication server for Apple's iTunes, Apple's App Store and / or Apple's enterprise application system) to obtain the usage authorization in response to the external authorization request. For example, the digital certificate (authorization element) is validated by contacting an external OCSP server (communication to fixed portion to obtain usage authorization) upon initial opening, and by a runtime check (external authorization request) at each time of use.</p> <p>See, e.g., Distributing Enterprise Apps for iOS 4 Devices, (<a href="http://developer.apple.com/library/ios/#featuredarticles/FA_Wireless_Enterprise_App_Distribution/Introduction/Introduction.html">http://developer.apple.com/library/ios/#featuredarticles/FA_Wireless_Enterprise_App_Distribution/Introduction/Introduction.html</a>), accessed on May 12, 2011, MOTO-APPLE-0006037953_126598:</p> <p><b>"Certificate Validation.</b> The first time an application is opened on a device, the distribution certificate is validated by contacting Apple's OCSP server. Unless the certificate has been revoked, the app is allowed to run. Inability to contact or get a</p>

**EXHIBIT D**

‘737 Patent Claim	Accused Apple Products <sup>9</sup>
	<p>response from the OCSP server is not interpreted as a revocation. To verify the status, the device must be able to reach ocsf.apple.com. See 'Network Configuration Requirements.'</p> <p>The OCSP response is cached on the device for the period of time specified by the OCSP server; currently between 3 and 7 days. The validity of the certificate will not be checked again until the device has restarted and the cached response has expired. If a revocation is received at that time, the app will be prevented from running. Note that revoking a distribution certificate will invalidate all of the applications you have distributed.</p> <p>An app will not run if the distribution certificate has expired. Currently, distribution certificates are valid for one year. A few weeks before your certificate expires request a new distribution certificate from the Dev Center, use it create new distribution provisioning profiles, then recompile and distribute the updated apps to your users. See 'Providing Updated Apps.'</p> <p><i>See also iPhone in Business: Security Overview, MOTO-APPLE-0006037953_126666:</i></p> <p><b>Mandatory Code Signing</b>  All iPhone applications must be signed. The applications provided with the device are signed by Apple. Third-party applications are signed by the developer using an Apple-issued certificate. This ensures that applications haven't been tampered with or altered. Additionally, runtime checks are made to ensure that an application hasn't become untrusted since it was last used.</p> <p><i>See also iPhone in Business: Digital Certificates, MOTO-APPLE-0006037953_126669:</i></p>

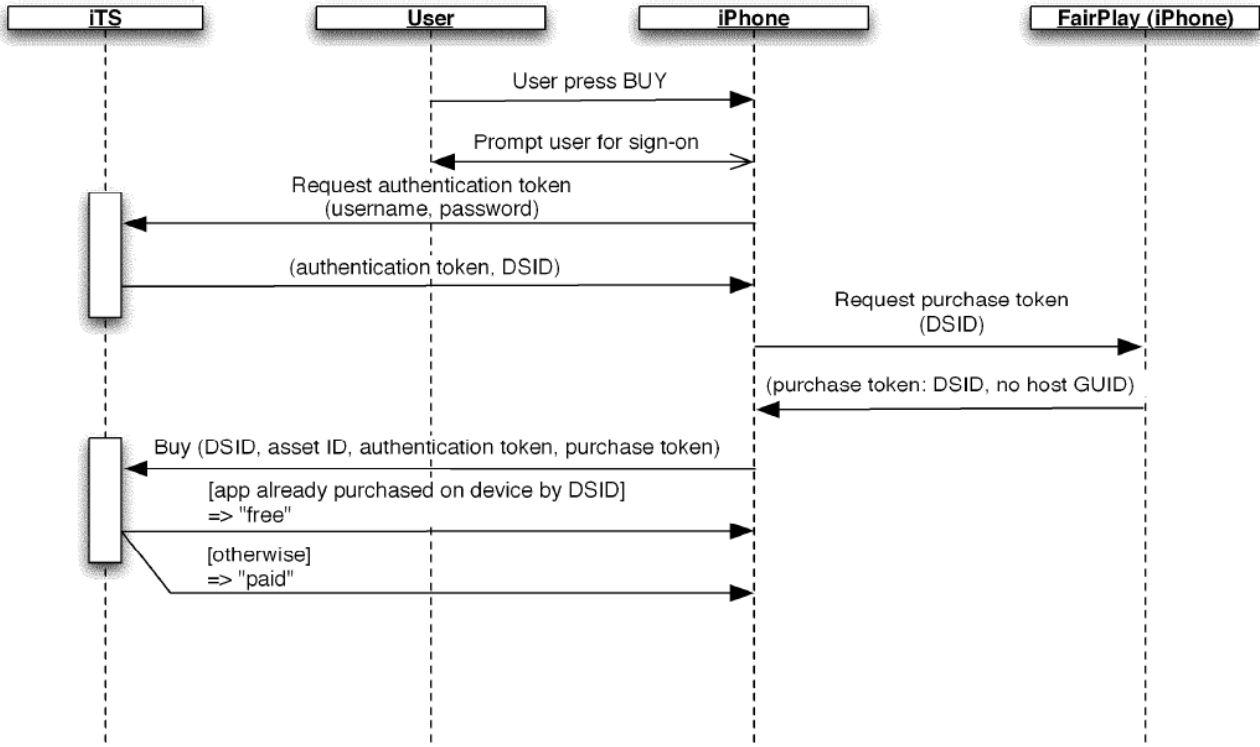
**EXHIBIT D**

‘737 Patent Claim	Accused Apple Products <sup>9</sup>
	<p><b>Digital certificates</b></p> <p>Digital certificates can be used to securely authenticate users to corporate services without the need for user names, passwords or soft tokens. On iPhone, certificate-based authentication is supported for access to Microsoft Exchange ActiveSync, VPN, and Wi-Fi networks.</p>  <p>The diagram illustrates the authentication process. On the left, a 'Certificate Authority' (represented by a server icon) issues a digital certificate (represented by a document icon) to a smartphone. The smartphone then sends an 'Authentication Request' (represented by a document icon) to 'Enterprise Services' (represented by a server rack icon), which includes 'Intranet, Email, VPN, Wi-Fi'. Finally, the Enterprise Services communicate with a 'Directory Service' (represented by a server icon and a key icon).</p> <p><u>Communications with the Apple App store.</u> In connection with a request to use software on or download software onto an Accused Apple Product, an authorization element coupled to the processor of that Accused Apple Product requests usage authorization for utilizing that software in the Accused Apple Product. The authorization element within the Accused Apple Product generates an external authorization request in order to secure this authorization. The authorization element communicates with Apple servers to obtain the usage authorization in response to the external authorization request.</p> <p><i>See also e.g.,</i> Email from Dallas De Atley, dated December 14, 2010, 745-Apple10360097-98:</p>

**EXHIBIT D**

<b>'737 Patent Claim</b>	<b>Accused Apple Products<sup>9</sup></b>
	<ul style="list-style-type: none"><li>&gt; The ability to run applications on a device is controlled by two mechanisms:</li><li>&gt;</li><li>&gt; 1) Code signing enforced by the kernel</li><li>&gt;</li><li>&gt; All applications must be signed by Apple before the kernel will run them.</li><li>&gt;</li><li>&gt; 2) Encryption enforced by FairPlay</li><li>&gt;</li><li>&gt; All applications are also encrypted with FairPlay, and decoded in the kernel by the FairPlay engine.</li><li>&gt; The use of FairPlay allows us to tie the application to a particular user more than a particular device.</li></ul> <p><i>See also e.g., iTunes Authentication Use Case Chart, 745-Apple5374978-81:</i></p>

**EXHIBIT D**

‘737 Patent Claim	Accused Apple Products <sup>9</sup>
	<p style="text-align: center;">Use Case 1: user never sync'ed from iTunes, no account set in Store settings (authentication token absent or expired)</p>  <pre> sequenceDiagram     participant ITS     participant User     participant iPhone     participant FairPlay as FairPlay (iPhone)      User-&gt;&gt;iPhone: User press BUY     iPhone-&gt;&gt;User: Prompt user for sign-on     iPhone-&gt;&gt;ITS: Request authentication token (username, password)     ITS-&gt;&gt;iPhone: (authentication token, DSID)     iPhone-&gt;&gt;FairPlay: Request purchase token (DSID)     FairPlay-&gt;&gt;iPhone: (purchase token: DSID, no host GUID)     iPhone-&gt;&gt;ITS: Buy (DSID, asset ID, authentication token, purchase token)     ITS--&gt;&gt;iPhone: [app already purchased on device by DSID =&gt; "free"]     ITS--&gt;&gt;iPhone: [otherwise =&gt; "paid"]     </pre> <p><i>See also e.g.,</i> Email from Henri Lamiraux, dated December 13, 2010, 745-Apple10362501-32</p> <p><b>-FairPlay protected content (3rd party apps, Movies, TV Shows, Protected Music and Music Videos from iTunes) will fail to playback. Users will need to erase install and re-sync their content. Restoring from a backup or update installing will result in broken FairPlay content. This applies only to K94 and K95</b></p> <p><i>See also e.g.</i> iPhone SDK, dated October 4, 2007, 745-Apple8563808-27;</p>



**EXHIBIT D**

‘737 Patent Claim	Accused Apple Products <sup>9</sup>
	<p>http://support.apple.com/kb/HT1420; <a href="http://support.apple.com/kb/HT2204?viewlocale=en_US">http://support.apple.com/kb/HT2204?viewlocale=en_US</a>; http://support.apple.com/kb/HE37; 745-Apple5375102-04.</p> <p>See also Developer Library—Authentication and Authorization, (<a href="http://developer.apple.com/library/ios/#documentation/Security/Conceptual/Security_Overview/AuthenticationAndAuthorization/AuthenticationAndAuthorization.html#//apple_ref/doc/uid/TP30000976-CH2-SW1">http://developer.apple.com/library/ios/#documentation/Security/Conceptual/Security_Overview/AuthenticationAndAuthorization/AuthenticationAndAuthorization.html#//apple_ref/doc/uid/TP30000976-CH2-SW1</a>), accessed on 11/06/2012, MOTO-SDFL-0000018762 (emphasis added):</p> <p>The details of authorization depend on the platform you are using: <b>In iOS</b>, the user can set a passcode (which by default is a four-digit personal identification number) to prevent unauthorized use of the device. After entering this passcode, the user of the device is presumed to be authorized to use the device. In addition, <u>each app is digitally signed and can therefore be authenticated by the operating system.</u> Therefore, there are no user authentication or authorization APIs in iOS.</p> <p><b>In OS X</b>, there are several layers of authorization:</p> <ul style="list-style-type: none"> <li>• If FileVault 2 (full-disk encryption) is enabled, the computer requires a password to decrypt the boot volume.</li> <li>• If automatic login is disabled, OS X displays a login screen after booting.</li> <li>• OS X also displays a login screen when the user logs out.</li> <li>• If the appropriate checkbox in the Security system preferences pane is checked, OS X displays a login screen when waking from sleep or when leaving a screen saver.</li> <li>• When an app or tool requests access to a locked keychain, a password is required.</li> <li>• <u>If an app or tool needs elevated privileges, an administrator password is required.</u></li> <li>• <u>Some apps may restrict access to parts of their functionality through the Authorization Services API.</u></li> </ul> <p>In addition, <u>on both OS X and iOS, some apps may require you to log in to a remote server, which in turn performs authentication and authorization.</u></p>
<p>in which the external authorization request includes at least one of: an address identifying the portable communication device, a software name and a size of the software; and</p>	<p>Upon information and belief, the external authorization request includes at least one of: an address identifying the portable communication device, a software name and a size of the software.</p> <p>For example, an X.509 digital certificate for an iPhone 4 “enforces a trust policy referred to as the S/MIME policy, which specifies that in order to be trusted to verify a digitally signed email, a certificate must contain an email address that matches the address of the sender of the email.” Security Concepts, (<a href="http://developer.apple.com/library/ios/#documentation/Security/Conceptual/Security_Overview/Concepts/Concepts.html">http://developer.apple.com/library/ios/#documentation/Security/Conceptual/Security_Overview/Concepts/Concepts.html</a>), accessed on May 13, 2011, MOTO-APPLE-0006037953_126611.</p>

**EXHIBIT D**

‘737 Patent Claim	Accused Apple Products <sup>9</sup>
	<p><i>See id.</i> at MOTO-APPLE-0006037953_126608:</p> <p>"A digital certificate is a collection of data used to verify the identity of the holder or sender of the certificate: For example, an X.509 certificate contains such information as:</p> <ul style="list-style-type: none"> <li>• Version</li> <li>• Serial number</li> <li>• Certificate issuer</li> <li>• Certificate holder</li> <li>• Validity period (the certificate is not valid before or after this period)</li> <li>• Attributes, known as certificate extension, that contain additional information such as allowable uses for this certificate</li> <li>• Digital signature from the certification authority to ensure that the certificate has not been altered and to indicate the identity of the issuer</li> <li>• Public key of the owner of the certificate</li> <li>• Message digest algorithm used to create the signature."</li> </ul> <p><i>See also</i> Distributing Enterprise Apps for iOS 4 Devices, (<a href="http://developer.apple.com/library/ios/#featuredarticles/FA_Wireless_Enterprise_App_Distribution/Introduction/Introduction.html">http://developer.apple.com/library/ios/#featuredarticles/FA_Wireless_Enterprise_App_Distribution/Introduction/Introduction.html</a>), accessed on May 12, 2011, MOTO-APPLE-0006037953_126598:</p> <p><b>"Certificate Validation.</b> The first time an application is opened on a device, the distribution certificate is validated by contacting Apple's OCSP server. Unless the certificate has been revoked, the app is allowed to run. Inability to contact or get a response from the OCSP server is not interpreted as a revocation. To verify the status, the device must be able to reach ocsf.apple.com. See 'Network Configuration Requirements.'</p> <p>The OCSP response is cached on the device for the period of time specified by the OCSP server; currently between 3 and 7 days. The validity of the certificate will not be checked again until the device has restarted and the cached response has expired. If a</p>

**EXHIBIT D**

‘737 Patent Claim	Accused Apple Products <sup>9</sup>
	<p>revocation is received at that time, the app will be prevented from running. Note that revoking a distribution certificate will invalidate all of the applications you have distributed.</p> <p>An app will not run if the distribution certificate has expired. Currently, distribution certificates are valid for one year. A few weeks before your certificate expires request a new distribution certificate from the Dev Center, use it create new distribution provisioning profiles, then recompile and distribute the updated apps to your users. See 'Providing Updated Apps.'</p>
<p>second authorization element coupled to the processor for allowing utilization of the software, in response to usage authorization being obtained from the fixed portion.</p>	<p>Upon information and belief, the Accused Apple Products contain a second authorization element coupled to the processor for allowing utilization of the software, in response to an authorization being obtained from the fixed portion.</p> <p>For example, the iPhone 4 software application is allowed to run (second authorization element) once the digital certificate is authorized (usage authorization obtained from fixed portion).</p> <p><i>See, e.g.,</i> Distributing Enterprise Apps for iOS 4 Devices, (<a href="http://developer.apple.com/library/ios/#featuredarticles/FA_Wireless_Enterprise_App_Distribution/Introduction/Introduction.html">http://developer.apple.com/library/ios/#featuredarticles/FA_Wireless_Enterprise_App_Distribution/Introduction/Introduction.html</a>), accessed on May 12, 2011, MOTO-APPLE-0006037953_126598:</p> <p><b>"Certificate Validation.</b> The first time an application is opened on a device, the distribution certificate is validated by contacting Apple's OCSP server. Unless the certificate has been revoked, the app is allowed to run. Inability to contact or get a response from the OCSP server is not interpreted as a revocation. To verify the status, the device must be able to reach ocsf.apple.com. See 'Network Configuration Requirements.'</p> <p>The OCSP response is cached on the device for the period of time specified by the OCSP server; currently between 3 and 7 days. The validity of the certificate will not be checked again until the device has restarted and the cached response has expired. If a revocation is received at that time, the app will be prevented from running. Note that revoking a distribution certificate will invalidate all of the applications you have</p>

**EXHIBIT D**

<b>'737 Patent Claim</b>	<b>Accused Apple Products<sup>9</sup></b>
	<p>distributed.</p> <p>An app will not run if the distribution certificate has expired. Currently, distribution certificates are valid for one year. A few weeks before your certificate expires request a new distribution certificate from the Dev Center, use it create new distribution provisioning profiles, then recompile and distribute the updated apps to your users. See 'Providing Updated Apps.'</p>