Exhibit D

UNITED STATES PATENT NO. 6,008,737

PRELIMINARY INFRINGEMENT CONTENTIONS[1]

Accused Apple Products:[2] Apple iPhone 3G, 3GS, and 4G , Apple iPad, Apple iPad with 3G, Apple iPad 2, Apple iPad 2 with 3G, Apple iPod Touch (collectively, "Apple Phones"), Apple MacBook, Apple MacBook Pro, Apple MacBook Air, Apple iMac, Apple Mac Mini, and Apple Mac Pro (collectively, "Apple Computers").

'737 Patent Claim	**Accused Apple Products**
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 area portable communication devices. Moreover, the Accused Apple Products operate in the normal course of use in a communication system having a fixed portion. *See, e.g.*, iPhone 4 Technical Specifications, (http://www.apple.com/iphone/specs.html), accessed on May 12, 2011, MOTO-APPLE-0006037953_126659:

[1] Motorola Mobility's investigation is ongoing and discovery and claim construction are not yet complete. Mobility reserves the right to supplement or amend these contentions with contentions arising under the doctrine of equivalents in response to any proposed or ordered claim construction, subsequent discovery response or production, or subsequent disclosure made pursuant to FRCP 26.

[2] This list of Accused Apple Products was created based on publicly available information. Motorola Mobility reserves the right to supplement this list of Accused Apple Products.

Exhibit D

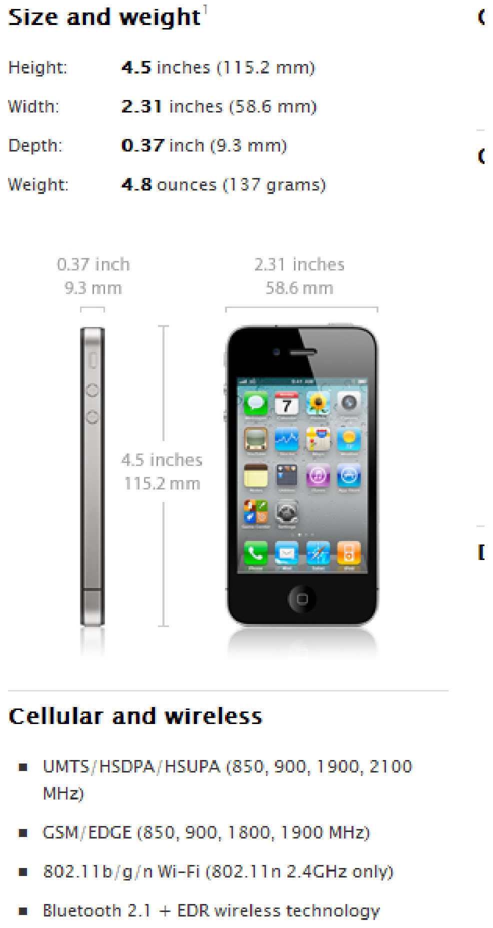
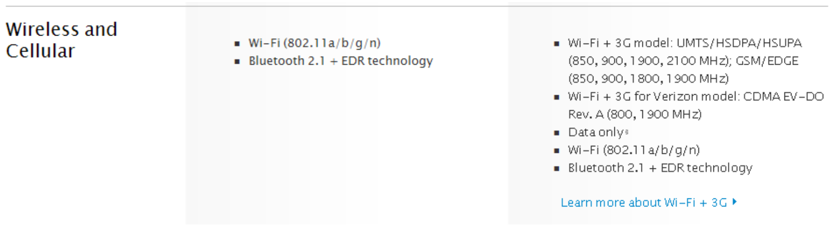
‘737 Patent Claim	Accused Apple Products
	 0.37 inch 9.3 mm 2.31 inches 58.6 mm 4.5 inches 115.2 mm **Size and weight**[1] Height: **4.5** inches (115.2 mm) Width: **2.31** inches (58.6 mm) Depth: **0.37** inch (9.3 mm) Weight: **4.8** ounces (137 grams) **Cellular and wireless** ▪ UMTS/HSDPA/HSUPA (850, 900, 1900, 2100 MHz) ▪ GSM/EDGE (850, 900, 1800, 1900 MHz) ▪ 802.11b/g/n Wi-Fi (802.11n 2.4GHz only) ▪ Bluetooth 2.1 + EDR wireless technology *See also e.g.*, Apple iPad Technical Specifications, (www.apple.com/ipad/specs), accessed on April 12, 2011, MOTO-APPLE-0005383110_35376:  Wireless and Cellular ▪ Wi-Fi (802.11a/b/g/n) ▪ Bluetooth 2.1 + EDR technology ▪ Wi-Fi + 3G model: UMTS/HSDPA/HSUPA (850, 900, 1900, 2100 MHz); GSM/EDGE (850, 900, 1800, 1900 MHz) ▪ Wi-Fi + 3G for Verizon model: CDMA EV-DO Rev. A (800, 1900 MHz) ▪ Data only[8] ▪ Wi-Fi (802.11a/b/g/n) ▪ Bluetooth 2.1 + EDR technology Learn more about Wi-Fi + 3G ▸ *See also, e.g.*, MacBook Pro 15" Core 2 Duo Model A1211 Teardown, (http://www.ifixit.com/Teardown/MacBook-Pro-15-Inch-Core-2-Duo-Model-A1211-Teardown/593/1), accessed on May 14, 2011, MOTO-APPLE-0006037953_127250:

Exhibit D

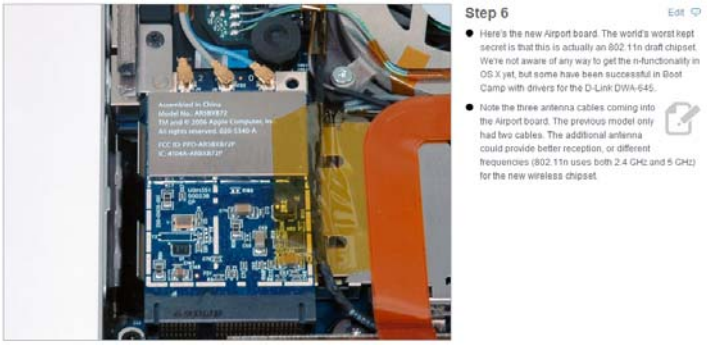
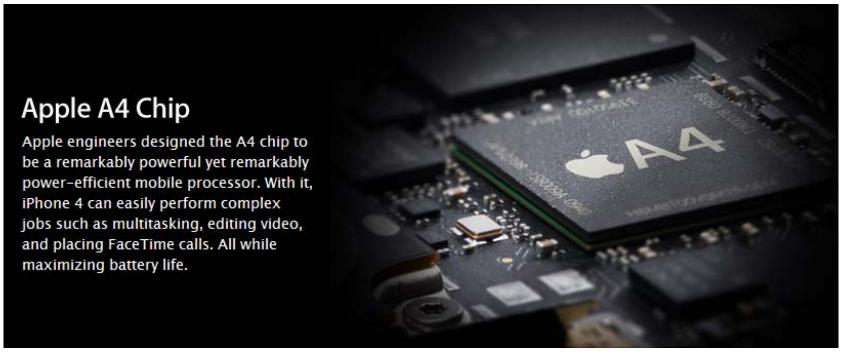
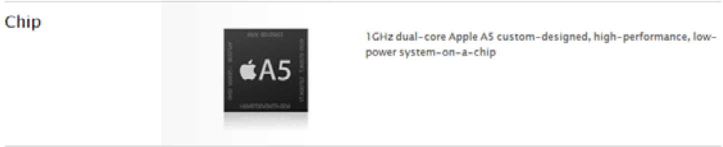
‘737 Patent Claim	Accused Apple Products
	 Step 6 - Here's the new Airport board. The world's worst kept secret is that this is actually an 802.11n draft chipset. We're not aware of any way to get the n-functionality in OS X yet, but some have been successful in Boot Camp with drivers for the D-Link DWA-645. - Note the three antenna cables coming into the Airport board. The previous model only had two cables. The additional antenna could provide better reception, or different frequencies (802.11n uses both 2.4 GHz and 5 GHz) for the new wireless chipset.
a processor;	Upon information and belief, the Apple Phones contain a variety of different processors, such a an Apple A4 processor, and Apple Computers contain a variety of different processors, such as the 2.4GHz Intel Core 2 Duo processor. *See*, *e.g.*, (http://www.apple.com/channel/iphone/iphone-4/best-buy/design.html), accessed May 12, 2011, MOTO-APPLE-0006037953_127201:  Apple A4 Chip 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. *See also e.g.*, Apple iPad Technical Specifications, (www.apple.com/ipad/specs), accessed on April 12, 2011, MOTO-APPLE-0005383110_35376:  Chip 1GHz dual-core Apple A5 custom-designed, high-performance, low-power system-on-a-chip *See also*, *e.g.*, MacBook Pro 15" Core 2 Duo Model A1211 Teardown, (http://www.ifixit.com/Teardown/MacBook-Pro-15-Inch-Core-2-Duo-Model-A1211-Teardown/593/1), accessed on May 14, 2011, MOTO-APPLE-0006037953_127248:

Exhibit D

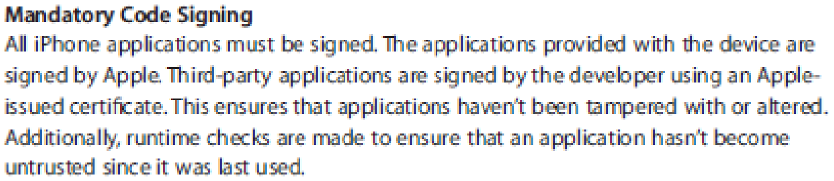
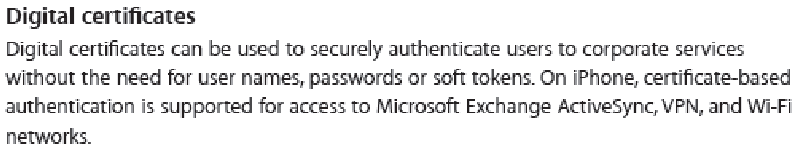
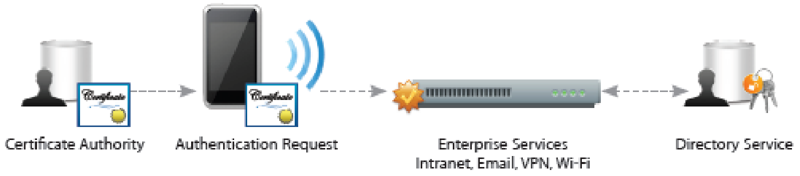
‘737 Patent Claim	Accused Apple Products
	 MacBook Pro 15" Core 2 Duo Model A1211 2.16 or 2.33 GHz Core 2 Duo processor
an authorization element coupled to the processor for obtaining usage authorization for utilizing software in the portable communication device,	Upon information and belief, the Accused Apple Products contain an authorization element coupled to the processor for obtaining usage authorization for utilizing software:  **Mandatory Code Signing** 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. iPhone in Business: Security Overview, MOTO-APPLE-0006037953_126666. *See also* iPhone in Business: Digital Certificates, MOTO-APPLE-0006037953_126669:  **Digital certificates** 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.  Certificate Certificate Certificate Authority Authentication Request Enterprise Services Intranet, Email, VPN, Wi-Fi Directory Service

Exhibit D

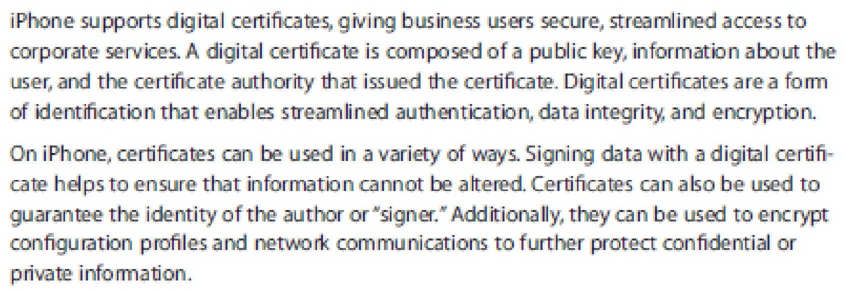
‘737 Patent Claim	Accused Apple Products
	See also id.:  iPhone supports digital certificates, giving business users secure, streamlined access to corporate services. A digital certificate is composed of a public key, information about the user, and the certificate authority that issued the certificate. Digital certificates are a form of identification that enables streamlined authentication, data integrity, and encryption. 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. *See also* Distributing Enterprise Apps for iOS 4 Devices, (http://developer.apple.com/library/ios/#featuredarticles/FA_Wireless_Enterprise_App_Distribution/Introduction/Introduction.html), accessed on May 12, 2011, MOTO-APPLE-0006037953_126598: "**Certificate Validation**. 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 ocsp.apple.com. See 'Network Configuration Requirements.' 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. 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.'" *See e.g.*, Communications with the Apple App store.
in which the authorization	Upon information and belief, the authorization element in the

Exhibit D

‘737 Patent Claim	Accused Apple Products
element generates an external authorization request, and	Accused Apple Products generates an external authorization request. For example, the digital certificate (authorization element) 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. *See* Distributing Enterprise Apps for iOS 4 Devices, (http://developer.apple.com/library/ios/#featuredarticles/FA_Wireless_Enterprise_App_Distribution/Introduction/Introduction.html), accessed on May 12, 2011, MOTO-APPLE-0006037953_126598: "**Certificate Validation**. 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 ocsp.apple.com. See 'Network Configuration Requirements.' 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. 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.'" *See also* iPhone in Business: Security Overview, MOTO-APPLE-0006037953_126666:

Exhibit D

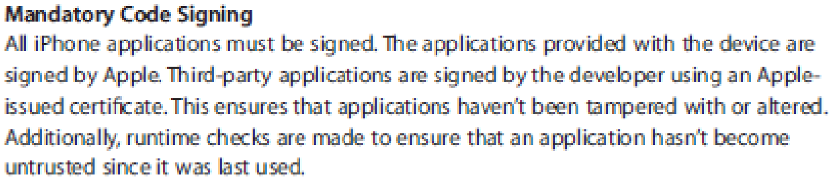
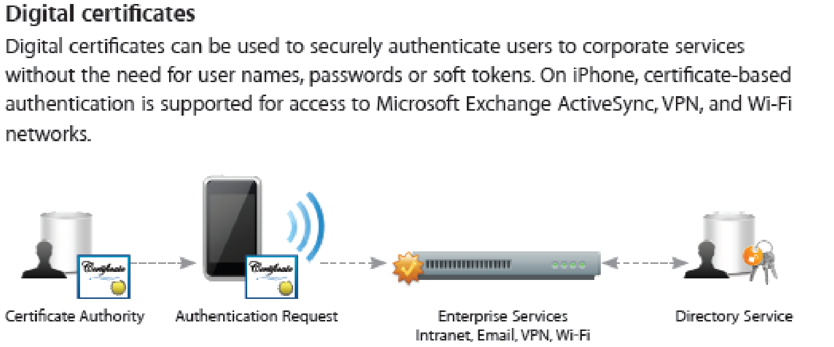
'737 Patent Claim	Accused Apple Products
	 **Mandatory Code Signing** All iPhone applications must be signed. The applications provided with the device are signed by Apple. Third-party applications are signed by the developer using an Apple-issued certificate. This ensures that applications haven't been tampered with or altered. Additionally, runtime checks are made to ensure that an application hasn't become untrusted since it was last used. *See also* iPhone in Business: Digital Certificates, MOTO-APPLE-0006037953_126669:  **Digital certificates** 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. Certificate Authority Authentication Request Enterprise Services Intranet, Email, VPN, Wi-Fi Directory Service
in which the authorization element communicates with the fixed portion to obtain the usage authorization in response to the external authorization request, and	Upon information and belief, the authorization element in the Accused Apple Products communicates with the fixed portion 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. *See, e.g.*, Distributing Enterprise Apps for iOS 4 Devices, (http://developer.apple.com/library/ios/#featuredarticles/FA_Wireless_Enterprise_App_Distribution/Introduction/Introduction.html), accessed on May 12, 2011, MOTO-APPLE-0006037953_126598: "**Certificate Validation**. 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 ocsp.apple.com. See 'Network Configuration Requirements.'

Exhibit D

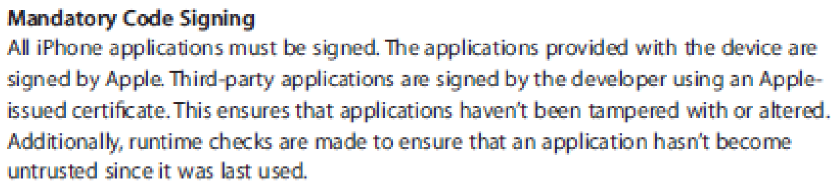
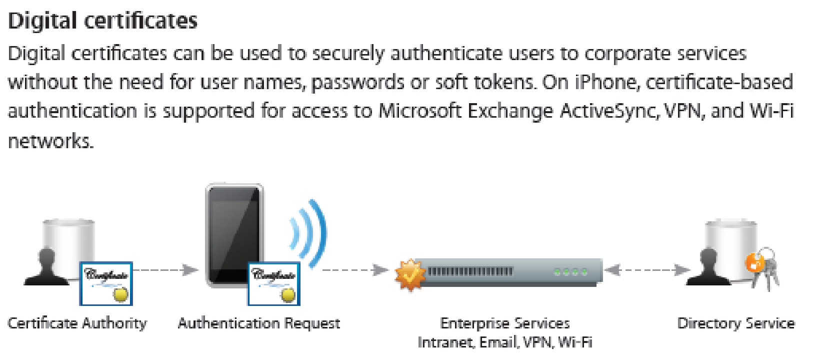
‘737 Patent Claim	Accused Apple Products
	The OCSP response is cached on the device for the period of time specified by the OCSP server; currently between 3 and 7 days. The validity of the certificate will not be checked again until the device has restarted and the cached response has expired. If a revocation 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. 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.'" *See also* iPhone in Business: Security Overview, MOTO-APPLE-0006037953_126666:  **Mandatory Code Signing** 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. *See also* iPhone in Business: Digital Certificates, MOTO-APPLE-0006037953_126669:  **Digital certificates** 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. Certificate Authority Authentication Request Enterprise Services Intranet, Email, VPN, Wi-Fi Directory Service
in which the external authorization request includes at least one of: an address identifying the	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.

Exhibit D

‘737 Patent Claim	Accused Apple Products
portable communication device, a software name and a size of the software; and	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, (http://developer.apple.com/library/ios/#documentation/Security/Conceptual/Security_Overview/Concepts/Concepts.html), accessed on May 13, 2011, MOTO-APPLE-0006037953_126611. *See id.* at MOTO-APPLE-0006037953_126608: "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: • Version • Serial number • Certificate issuer • Certificate holder • Validity period (the certificate is not valid before or after this period) • Attributes, known as certificate extension, that contain additional information such as allowable uses for this certificate • Digital signature from the certification authority to ensure that the certificate has not been altered and to indicate the identity of the issuer • Public key of the owner of the certificate • Message digest algorithm used to create the signature." *See also* Distributing Enterprise Apps for iOS 4 Devices, (http://developer.apple.com/library/ios/#featuredarticles/FA_Wireless_Enterprise_App_Distribution/Introduction/Introduction.html), accessed on May 12, 2011, MOTO-APPLE-0006037953_126598: "**Certificate Validation**. 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 ocsp.apple.com. See 'Network

Exhibit D

‘737 Patent Claim	**Accused Apple Products**
	Configuration Requirements.' 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. 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.'"
second authorization element coupled to the processor for allowing utilization of the software, in response to usage authorization being obtained from the fixed portion.	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. 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. *See*, *e.g.*, Distributing Enterprise Apps for iOS 4 Devices, (http://developer.apple.com/library/ios/#featuredarticles/FA_Wireless_Enterprise_App_Distribution/Introduction/Introduction.html), accessed on May 12, 2011, MOTO-APPLE-0006037953_126598: "**Certificate Validation**. 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 ocsp.apple.com. See 'Network Configuration Requirements.' 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

Exhibit D

‘737 Patent Claim	Accused Apple Products
	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. 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.'"