IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

SOFTEX LLC **Plaintiff,** **v.** **HP INC.,** **Defendant.**	**Civil Action No. 1:22-cv-01311-DAE** **JURY TRIAL DEMANDED**

JOINT CLAIM CONSTRUCTION STATEMENT

Pursuant to this Court's Docket Control Order (Dkt. 58), Plaintiff Softex LLC ("Softex" and Defendant HP ("HP" or "Defendant") submit the attached Joint Claim Construction Statement.

Dated: December 18, 2023

Respectfully submitted,

By: */s/ Blair M. Jacobs*
Blair M. Jacobs (DC Bar No. 32010)
bjacobs@McKoolSmith.com
Christina A. Ondrick (DC Bar No. 494625)
condrick@McKoolSmith.com
John S. Holley (SBN 24078678)
jholley@McKoolSmith.com
MCKOOL SMITH, P.C.
1999 K Street, NW Suite 600
Washington, D.C. 20006
Telephone: (202) 370-8300
Facsimile: (202) 370-8344

John B. Campbell (SBN 24036314)
jcampbell@McKoolSmith.com
MCKOOL SMITH, P.C.
303 Colorado Street, Suite 2100
Austin, TX 78701
Telephone: (512) 692-8700
Facsimile: (512) 692-8744

Casey L. Shomaker (SBN 24110359)
cshomaker@McKoolSmith.com
Matthew Folks (SBN 24116368)
mfolks@McKoolSmith.com
MCKOOL SMITH, P.C.
300 Crescent Court, Suite 1500
Dallas, TX 75201
Telephone: (214) 978-4218
Facsimile: (214) 978-4044

ATTORNEYS FOR PLAINTIFF SOFTEX LLC

By: */s/ Heidi Keefe*
Heidi L. Keefe (CA Bar 178960)
hkeefe@cooley.com
Reuben H. Chen (CA Bar 228725)
rchen@cooley.com
Alexandra Leeper (admitted *pro hac vice*)
aleeper@cooley.com
3175 Hanover Street
Palo Alto, CA 94304
Telephone: (650) 843-5000
Fax: (650) 849-7400
Orion Armon (admitted *pro hac vice*)
oarmon@cooley.com
1144 15th Street, Suite 2300
Denver, CO 80202
Telephone: (720) 566-4000
Fax: (720) 566-4099
Dustin M. Knight (admitted *pro hac vice*)
dknight@cooley.com
11951 Freedom Drive, 16th Floor
Reston, VA 20190
Telephone: (703) 456-8000
Fax: (703) 456-8100
Samuel K. Whitt (admitted *pro hac vice*)
swhitt@cooley.com
1299 Pennsylvania Avenue, NW Suite 700
Washington, DC 20004
Telephone: (202) 842-7800
Fax: (202) 842-7899

ATTORNEYS FOR DEFENDANT HP INC.

MICROSOFT CORP. EXHIBIT 1033
IPR2023-01185
Page 3 of 49

I. Agreed Upon Terms

Term	Patent/Claim(s)	Agreed upon constructions
"periodically communicate with the security service" / "periodically communicating with the security service"	'649 patent claims 1, 7, 9, and 15	Plain and ordinary meaning
"erasure of a non-volatile storage device" / "non-volatile storage device is . . . erased" / "erase the non-volatile storage device"	'710 patent claims 1-8, 11-21, 23	No construction necessary
"disabled" / "disabling"	'837 patent claims 10-14, and 16-19; '603 patent claim 4, 14, and 20; '649 patent claims 1, 7, 9, and 15; '410 patent claims 1-4, 7, and 17	Plain and ordinary meaning
"connected to"	'235 patent claims 1-21; '892 patent claims 1-19; '710 patent claims 1-8, 11-21, 23	No construction necessary - plain and ordinary meaning
"administering the security service for the electronic device"	'892 patent claims 8-10	No construction necessary, plain and ordinary meaning.
"valid"	'410 patent claims 1-4, 7-11, and 14-20	No construction necessary, plain and ordinary meaning.
"bypass operation of the application component"	'410 patent claims 4, 11, and 20	No construction necessary, plain and ordinary meaning.

"operating system (OS) environment" / "OS environment" / "operating system environment"	'837 patent claims 1-3, 8-14, 18-24; '235 patent claims 1-21; '892 patent claims 1-19	No construction necessary - plain and ordinary.
"non-transitory machine-readable medium" / "non-transitory machine-readable storage medium" / "non-transitory machine-readable storage media"	'235 patent claims 15-21; '892 patent claims 15-18; '603 patent claims 12-14, and 18-20; '649 patent claims 1, 7; '410 patent claims 8-11, 14; '710 patent claims 19-21, 23	Plain and ordinary meaning, which is a machine-readable medium that is not a transitory wave.

II. DISPUTED TERMS

Term(s) / Claim(s)	Softex's Proposed Construction	Defendants' Proposed Construction	Court's Construction
"basic input/output system (BIOS)" / "BIOS" / "Basic Input/Output System (BIOS)" • '837 patent claims 1-3, 8-14, 18; • '235 patent claims 1-21; '892 patent claims 1-19; • '603 patent claims 1-4, 10, 12-14, and 18-20; • '410 patent claims 15-20; • '710 patent claims 1-8, 11-21, 23	Plain and ordinary meaning, which is electronic device firmware that is used to start the computer system after it is powered on.	the set of essential software routines that tests hardware at startup, starts the operating system, supports the transfer of data among hardware devices, and is stored in read-only memory (ROM) so that it can be executed when the computer is turned on	

MICROSOFT CORP. EXHIBIT 1033
IPR2023-01185
Page 5 of 49

Term / Claims	Softex's Proposed Construction	Defendants' Proposed Construction	Court's Construction
power on self test (POST) • '410 patent claims 1-4, 7-11, and 14-20	No construction necessary, plain and ordinary meaning.	"A set of routines stored in a computer's read-only memory (ROM) that tests various system components such as RAM, the disk drives, and the keyboard to see whether they are properly connected and operating and, if problems are found, alert the user or, if problems are not found, pass control to the system's bootstrap loader to load the operating system"	
Term(s) / Claim(s)	**Softex's Proposed Construction**	**Defendants' Proposed Construction**	**Court's Construction**
hidden partition • '837 patent claim 23; • '410 patent claims 1-4, 7-11, 14-20	No construction necessary - plain and ordinary meaning	Indefinite Alternatively, if not indefinite: "a hard drive partition that is hidden to all users"	
Term(s) / Claim(s)	**Softex's Proposed Construction**	**Defendants' Proposed Construction**	**Court's Construction**
operating correctly / operated correctly | • '410 patent claims 1-4, 7-11, and 14-20; • '603 patent claims 1-4, 10, 12-14, and 18-20	Plain and ordinary meaning, which is operating/operated as expected.	Indefinite	

MICROSOFT CORP. EXHIBIT 1033
IPR2023-01185
Page 6 of 49

Term(s) / Claim(s)	Softex's Proposed Construction	Defendants' Proposed Construction	Court's Construction
"wherein integrating the ESTSM ROM image into the BIOS of the electronic device configures the electronic device for having a non-viewable component, an application component connected to the non-viewable component and capable of executing within an operating system environment and of communicating with the non-viewable component, and a BIOS component connected to the non-viewable component" / "wherein integrating the ESTSM ROM image into the BIOS of the electronic device configures the electronic device for having a non-viewable component, an application component that is connected to the non-viewable component, that is capable of communicating with the non-viewable component, and that executes within an operating system environment" • '235 patent claims 1-7, 15-21	No construction necessary, plain and ordinary meaning.	Indefinite	

MICROSOFT CORP. EXHIBIT 1033
IPR2023-01185
Page 7 of 49

Term(s) / Claim(s)	Softex's Proposed Construction	Defendants' Proposed Construction	Court's Construction
primary server • '603 patent claims 2-4, 13-14, and 19-20	No construction necessary, plain and ordinary meaning.	"a particular server that is the first server with which the user's device attempts to communicate"	
Term(s) / Claim(s)	**Softex's Proposed Construction**	**Defendants' Proposed Construction**	**Court's Construction**
central server • '710 patent claim 1	No construction necessary, plain and ordinary meaning.	"a particular server located within the premises of the administrator of the electronic device security system"	
Term(s) / Claim(s)	**Softex's Proposed Construction**	**Defendants' Proposed Construction**	**Court's Construction**
If §112, sixth paragraph, does not apply			
application component • '837 claims 1-3, 5-14, and 16-27; • '235 claims 1-21; '892 claims 1-19; • '603 claims 1-4, 10-14, and 18-20; • '410 claims 1-4, 7-11, and 14-20; • '710 claims 1-8, 11-21, 23	Not subject to § 112, ¶ 6, no construction necessary.	Indefinite under § 112, ¶ 1	
If §112, sixth paragraph does apply			
'837 Patent | Claim 1 (if §112, sixth paragraph does apply)			
application component	Not subject to § 112, ¶ 6, but if construed under §112, ¶ 6: **<u>Claim 1 (function):</u>**	**Invokes 35 U.S.C. § 112, ¶ 6:** **<u>Function</u>**: "provide security and tracking for an electronic	

	• configured to cause the electronic device to send, to the server system, a message that contains location information for the electronic device; • to determine whether the electronic device has been reported stolen, based on information received from the server system; • to notify the BIOS security component that the electronic device has been reported stolen, in response to determining that the electronic device has been reported stolen. **<u>Claim 1 (structure):</u>** a computer application configured to to perform the sending, determining and notifying disclosed in Figs. 40, 42, 44-50, 55, 71, 72; 8:27-40; 15:25-37; 15:63-67; 16:15-17; 18:66-19:2; 19:20-25; 19:29-31; 20:17-27; 17:55-61; 24:33-44; 25:63-67; 26:57-64; 33:26-	device; communicate through a secure medium with a server to automatically determine if an electronic device has been reported stolen; if the device has been reported stolen, work with the server to determine what services the user has registered for and take the appropriate action (e.g., disable the device, communicate identifying information to the server, erase the storage device, recover data, encrypt data, etc.); notify a BIOS security component that the device has been reported stolen; notify a BIOS component that the device has been reported stolen; communicate with a non-viewable security component through a communications area; communicate with a non-viewable component; determine the device's location; send location information for the device to a server system; record that the device has been reported stolen; and erase a non-volatile storage device in response to an instruction from the server"	

	29.	**Structure**: Indefinite (no structure disclosed)	
'837 Patent | Claims 12, 20 (if §112, sixth paragraph does apply)			
application component	Not subject to § 112, ¶ 6, but if construed under §112, ¶ 6: **Claims 12, 20 (function):** • configured to cause the electronic device to send, to the server system, a message that contains location information for the electronic device, and • capable of determining whether the electronic device has been reported stolen, based on information received from the server system **Claims 12, 20 (structure):** a computer application configured to perform the sending and determining disclosed in Figs. 40, 42, 44-50, 55, 71, 72; 8:27-40; 15:25-37; 15:63-67; 16:15-17; 19:20-25; 19:29-31; 20:17-27; 17:55-61; 24:33-44; 25:63-67.	**Invokes 35 U.S.C. § 112, ¶ 6:** **Function**: "provide security and tracking for an electronic device; communicate through a secure medium with a server to automatically determine if an electronic device has been reported stolen; if the device has been reported stolen, work with the server to determine what services the user has registered for and take the appropriate action (e.g., disable the device, communicate identifying information to the server, erase the storage device, recover data, encrypt data, etc.); notify a BIOS security component that the device has been reported stolen; notify a BIOS component that the device has been reported stolen; communicate with a non-viewable security component through a communications area; communicate with a non-viewable component; determine the device's location; send location	

MICROSOFT CORP. EXHIBIT 1033
IPR2023-01185
Page 10 of 49

		information for the device to a server system; record that the device has been reported stolen; and erase a non-volatile storage device in response to an instruction from the server" **Structure**: Indefinite (no structure disclosed)	
'235 Patent | Claims 1, 4 (if §112, sixth paragraph does apply)			
application component	Not subject to § 112, ¶ 6, but if construed under §112, ¶ 6: **Claim 1, 4 (function):** • capable of communicating with the non-viewable component, • send, to the server system, a message that contains information of a location of the electronic device, and • configured to determine whether the electronic device has been reported stolen, based on information received from the server system. **Claims 1, 4 (structure):**	**Invokes 35 U.S.C. § 112, ¶ 6:** **Function**: "provide security and tracking for an electronic device; communicate through a secure medium with a server to automatically determine if an electronic device has been reported stolen; if the device has been reported stolen, work with the server to determine what services the user has registered for and take the appropriate action (e.g., disable the device, communicate identifying information to the server, erase the storage device, recover data, encrypt data, etc.); notify a BIOS security component that the device has been reported stolen; notify a BIOS component that the device has been reported stolen;	

MICROSOFT CORP. EXHIBIT 1033
IPR2023-01185
Page 11 of 49

	a computer application configured to perform the communicating, sending and determining disclosed in Figs. 40, 42, 44-50, 55, 71, 72; 8:27-40; 15:25-37; 15:63-67; 16:15-17; 18:66-19:2; 19:20-25; 19:29-31; 20:17-27; 17:55-61; 24:33-44; 25:63-67; 26:57-64; 33:26-29.	communicate with a non-viewable security component through a communications area; communicate with a non-viewable component; determine the device's location; send location information for the device to a server system; record that the device has been reported stolen; and erase a non-volatile storage device in response to an instruction from the server" **<u>Structure</u>**: Indefinite (no structure disclosed)	
'235 Patent | Claim 6 (if §112, sixth paragraph does apply)			
application component	Not subject to § 112, ¶ 6, but if construed under §112, ¶ 6: **<u>Claims 4, 11, 18 (function):</u>** • to cause the electronic device to send, to the server system, a message that contains information of a location of the electronic device, and • to determine whether the electronic device has been reported stolen, based on	**Invokes 35 U.S.C. § 112, ¶ 6:** **<u>Function</u>**: "provide security and tracking for an electronic device; communicate through a secure medium with a server to automatically determine if an electronic device has been reported stolen; if the device has been reported stolen, work with the server to determine what services the user has registered for and take the appropriate action (e.g., disable the device, communicate identifying information to the	

MICROSOFT CORP. EXHIBIT 1033
IPR2023-01185
Page 12 of 49

	information received from the server system. **<u>Claims 4, 11, 18 (structure):</u>** a computer application configured to perform the sending and determining disclosed in Figs. 40, 42, 44-50, 55, 71, 72; 8:27-40; 15:25-37; 15:63-67; 16:15-17; 19:20-25; 19:29-31; 20:17-27; 17:55-61; 24:33-44; 25:63-67.	server, erase the storage device, recover data, encrypt data, etc.); notify a BIOS security component that the device has been reported stolen; notify a BIOS component that the device has been reported stolen; communicate with a non-viewable security component through a communications area; communicate with a non-viewable component; determine the device's location; send location information for the device to a server system; record that the device has been reported stolen; and erase a non-volatile storage device in response to an instruction from the server" **<u>Structure</u>**: Indefinite (no structure disclosed)	
'235 Patent | Claim 7 (if §112, sixth paragraph does apply)			
application component	Not subject to § 112, ¶ 6, but if construed under §112, ¶ 6: **<u>Claim 7 (function):</u>** • configured to notify the BIOS component that the electronic device has been reported stolen, in response to	**Invokes 35 U.S.C. § 112, ¶ 6:** **<u>Function</u>**: "provide security and tracking for an electronic device; communicate through a secure medium with a server to automatically determine if an electronic device has been reported stolen; if the device	

MICROSOFT CORP. EXHIBIT 1033
IPR2023-01185
Page 13 of 49

	determining that the electronic device has been reported stolen. **<u>Claim 7 (structure):</u>** a computer application configured to perform the notifying disclosed in Figs. 40, 42, 44-50, 55, 71, 72; 18:66-19:2; 25:63-67; 26:57-64;	has been reported stolen, work with the server to determine what services the user has registered for and take the appropriate action (e.g., disable the device, communicate identifying information to the server, erase the storage device, recover data, encrypt data, etc.); notify a BIOS security component that the device has been reported stolen; notify a BIOS component that the device has been reported stolen; communicate with a non-viewable security component through a communications area; communicate with a non-viewable component; determine the device's location; send location information for the device to a server system; record that the device has been reported stolen; and erase a non-volatile storage device in response to an instruction from the server" **<u>Structure</u>**: Indefinite (no structure disclosed)	
'235 Patent | Claims 8, 15 (if §112, sixth paragraph does apply)			
application component	Not subject to § 112, ¶ 6, but if construed under §112, ¶ 6:	**Invokes 35 U.S.C. § 112, ¶ 6:**	

	Claims 8, 15 (function): • communicating with the non-viewable component **Claims 8, 15 (structure):** a computer application configured to perform the communicating disclosed in Figs. 40, 42, 44-50, 55, 71, 72; 17:39-42; 18:41-46; 18:66-19:2; 25:63-67; 26:57-64;	**Function**: "provide security and tracking for an electronic device; communicate through a secure medium with a server to automatically determine if an electronic device has been reported stolen; if the device has been reported stolen, work with the server to determine what services the user has registered for and take the appropriate action (e.g., disable the device, communicate identifying information to the server, erase the storage device, recover data, encrypt data, etc.); notify a BIOS security component that the device has been reported stolen; notify a BIOS component that the device has been reported stolen; communicate with a non-viewable security component through a communications area; communicate with a non-viewable component; determine the device's location; send location information for the device to a server system; record that the device has been reported stolen; and erase a non-volatile storage device in response to an	

		instruction from the server" **<u>Structure</u>**: Indefinite (no structure disclosed)	
'235 Patent | Claims 14, 21 (if §112, sixth paragraph does apply)			
application component	Not subject to § 112, ¶ 6, but if construed under §112, ¶ 6: **<u>Claims 14, 21 (function):</u>** • to notify the BIOS component that the electronic device has been reported stolen, in response to determining that the electronic device has been reported stolen. **<u>Claims 14, 21 (structure):</u>** a computer application configured to perform the notifying disclosed in Figs. 40, 42, 44-50, 55, 71, 72; 18:66-19:2; 19:34-40; 19:62-67; 21:50-55; 25:37-41; 26:17-22.	**Invokes 35 U.S.C. § 112, ¶ 6:** **<u>Function</u>**: "provide security and tracking for an electronic device; communicate through a secure medium with a server to automatically determine if an electronic device has been reported stolen; if the device has been reported stolen, work with the server to determine what services the user has registered for and take the appropriate action (e.g., disable the device, communicate identifying information to the server, erase the storage device, recover data, encrypt data, etc.); notify a BIOS security component that the device has been reported stolen; notify a BIOS component that the device has been reported stolen; communicate with a non-viewable security component through a communications area; communicate with a non-viewable component;	

		determine the device's location; send location information for the device to a server system; record that the device has been reported stolen; and erase a non-volatile storage device in response to an instruction from the server" **<u>Structure</u>**: Indefinite (no structure disclosed)	
'892 Patent | Claims 1, 11, 12, 15 (if §112, sixth paragraph does apply)			
application component	Not subject to § 112, ¶ 6, but if construed under §112, ¶ 6: **<u>Claims 1, 11, 12, 15 (function):</u>** • communicating with the non-viewable component, and • that is capable of communicating through a secure medium with a server system **<u>Claims 1, 11, 12, 15 (structure):</u>** a computer application configured to perform the communicating disclosed in Figs. 40, 42, 44-50, 55, 71, 72; 8:27-40; 15:25-37; 15:63-67; 16:15-17; 18:66-19:2; 19:20-	**Invokes 35 U.S.C. § 112, ¶ 6:** **<u>Function</u>**: "provide security and tracking for an electronic device; communicate through a secure medium with a server to automatically determine if an electronic device has been reported stolen; if the device has been reported stolen, work with the server to determine what services the user has registered for and take the appropriate action (e.g., disable the device, communicate identifying information to the server, erase the storage device, recover data, encrypt data, etc.); notify a BIOS security component that the device has been reported stolen; notify a	

	25; 19:29-31; 20:17-27; 17:55-61; 24:33-44; 25:63-67; 26:57-64; 33:26-29.	BIOS component that the device has been reported stolen; communicate with a non-viewable security component through a communications area; communicate with a non-viewable component; determine the device's location; send location information for the device to a server system; record that the device has been reported stolen; and erase a non-volatile storage device in response to an instruction from the server" **Structure**: Indefinite (no structure disclosed)	
'603 Patent | Claims 1, 12, 18 (if §112, sixth paragraph does apply)			
application component	Not subject to § 112, ¶ 6, but if construed under §112, ¶ 6: **Claims 1, 12, 18 (function):** • to automatically ascertain whether the electronic device has been reported stolen, based on information received from a server system. **Claims 1, 12, 18 (structure):**	**Invokes 35 U.S.C. § 112, ¶ 6:** **Function**: "provide security and tracking for an electronic device; communicate through a secure medium with a server to automatically determine if an electronic device has been reported stolen; if the device has been reported stolen, work with the server to determine what services the user has registered for and take the appropriate action (e.g., disable	

	a computer application configured to perform automatic ascertaining disclosed in Figs. 40; 42; 44; 45; 46; 47; 48; 49; 55, 71; 72; 15:25-30; 15:61-66; 33:65-34:4; 34:13-20; 34:58-67.	the device, communicate identifying information to the server, erase the storage device, recover data, encrypt data, etc.); notify a BIOS security component that the device has been reported stolen; notify a BIOS component that the device has been reported stolen; communicate with a non-viewable security component through a communications area; communicate with a non-viewable component; determine the device's location; send location information for the device to a server system; record that the device has been reported stolen; and erase a non-volatile storage device in response to an instruction from the server" **Structure**: Indefinite (no structure disclosed)	
'410 Patent | Claims 1, 8, 15 (if §112, sixth paragraph does apply)			
application component	Not subject to § 112, ¶ 6, but if construed under §112, ¶ 6: **Claims 1, 8, 15 (function):** • associated with tracking and locating the electronic device	**Invokes 35 U.S.C. § 112, ¶ 6:** **Function**: "provide security and tracking for an electronic device; communicate through a secure medium with a server to automatically determine if an	

MICROSOFT CORP. EXHIBIT 1033
IPR2023-01185
Page 19 of 49

	Claims 1, 8, 15 (structure): a computer application configured to perform automatic ascertaining disclosed in Figs. 40, 42, 44-50, 55, 71, 72; 8:27-40; 11:4-9; 15:25-37; 15:63-67; 16:15-17; 17:65-17:1; 19:20-25; 19:29-31; 20:17-27; 24:33-44.	electronic device has been reported stolen; if the device has been reported stolen, work with the server to determine what services the user has registered for and take the appropriate action (e.g., disable the device, communicate identifying information to the server, erase the storage device, recover data, encrypt data, etc.); notify a BIOS security component that the device has been reported stolen; notify a BIOS component that the device has been reported stolen; communicate with a non-viewable security component through a communications area; communicate with a non-viewable component; determine the device's location; send location information for the device to a server system; record that the device has been reported stolen; and erase a non-volatile storage device in response to an instruction from the server" **Structure**: Indefinite (no structure disclosed)	

'710 Patent | Claims 1, 2, 19 (if §112, sixth paragraph does apply)			
application component	Not subject to § 112, ¶ 6, but if construed under §112, ¶ 6: **<u>Claims 1, 2, 19 (function):</u>** • capable of communicating with the non-viewable component **<u>Claims 1, 2, 19 (structure):</u>** a computer application configured to perform the communicating disclosed in Figs. 40, 42, 44-50, 55, 71, 72; 17:39-42; 18:41-46; 18:66-19:2; 25:63-67; 26:57-64	**Invokes 35 U.S.C. § 112, ¶ 6:** **<u>Function</u>**: "provide security and tracking for an electronic device; communicate through a secure medium with a server to automatically determine if an electronic device has been reported stolen; if the device has been reported stolen, work with the server to determine what services the user has registered for and take the appropriate action (e.g., disable the device, communicate identifying information to the server, erase the storage device, recover data, encrypt data, etc.); notify a BIOS security component that the device has been reported stolen; notify a BIOS component that the device has been reported stolen; communicate with a non-viewable security component through a communications area; communicate with a non-viewable component; determine the device's location; send location information for the device to a server system; record that the	

MICROSOFT CORP. EXHIBIT 1033
IPR2023-01185
Page 21 of 49

		device has been reported stolen; and erase a non-volatile storage device in response to an instruction from the server" **<u>Structure</u>**: Indefinite (no structure disclosed)	
'710 Patent | Claim 13 (if §112, sixth paragraph does apply)			
application component	Not subject to § 112, ¶ 6, but if construed under §112, ¶ 6: **<u>Claim 13 (function):</u>** • record that the electronic device has been reported stolen, after the report that the electronic device has been stolen has been received **<u>Claim 13 (structure):</u>** a computer application configured to perform the recording disclosed disclosed in Figs. 40; 42; 44; 45; 46; 47; 48; 49; 55, 71; 72; 15:25-30; 15:61-66; 33:65-34:4; 34:13-20; 34:58-67.	**Invokes 35 U.S.C. § 112, ¶ 6:** **<u>Function</u>**: "provide security and tracking for an electronic device; communicate through a secure medium with a server to automatically determine if an electronic device has been reported stolen; if the device has been reported stolen, work with the server to determine what services the user has registered for and take the appropriate action (e.g., disable the device, communicate identifying information to the server, erase the storage device, recover data, encrypt data, etc.); notify a BIOS security component that the device has been reported stolen; notify a BIOS component that the device has been reported stolen; communicate with a non-viewable security component	

MICROSOFT CORP. EXHIBIT 1033
IPR2023-01185
Page 22 of 49

		through a communications area; communicate with a non-viewable component; determine the device's location; send location information for the device to a server system; record that the device has been reported stolen; and erase a non-volatile storage device in response to an instruction from the server" **Structure**: Indefinite (no structure disclosed)	
'710 Patent | Claim 15 (if §112, sixth paragraph does apply)			
application component	Not subject to § 112, ¶ 6, but if construed under §112, ¶ 6: **Claim 15 (function):** • erase the non-volatile storage device in response to an instruction from the server system **Claim 15 (structure):** a computer application configured to perform the recording disclosed in Figs. 42, 44, 45, 55; 2:28-34; 8:41-47; 14:21-25; 15:59-63; 16:2-5; 17:55-61; 23:35-38; 26:57-61.	**Invokes 35 U.S.C. § 112, ¶ 6:** **Function**: "provide security and tracking for an electronic device; communicate through a secure medium with a server to automatically determine if an electronic device has been reported stolen; if the device has been reported stolen, work with the server to determine what services the user has registered for and take the appropriate action (e.g., disable the device, communicate identifying information to the server, erase the storage device, recover data, encrypt data,	

MICROSOFT CORP. EXHIBIT 1033
IPR2023-01185
Page 23 of 49

		etc.); notify a BIOS security component that the device has been reported stolen; notify a BIOS component that the device has been reported stolen; communicate with a non-viewable security component through a communications area; communicate with a non-viewable component; determine the device's location; send location information for the device to a server system; record that the device has been reported stolen; and erase a non-volatile storage device in response to an instruction from the server" **Structure**: Indefinite (no structure disclosed)	
Term(s) / Claim(s)	**Softex's Proposed Construction**	**Defendants' Proposed Construction**	**Court's Construction**
If §112, sixth paragraph does not apply			
non-viewable component • '235 patent claims 1-21; • '892 patent claims 1-19; • '410 patent claims 1-4, 7-11, 14-20; • '710 patent claims 1-8, 11-21, 23	"a part of a computer program, the contents of which are not viewable to a typical or normal user."	Indefinite under § 112, ¶ 1	

MICROSOFT CORP. EXHIBIT 1033
IPR2023-01185
Page 24 of 49

Term(s) / Claim(s)	Softex's Proposed Construction	Defendants' Proposed Construction	Court's Construction
If §112, sixth paragraph does not apply			
non-viewable security component • '837 patent claims 1-3, 5-14, and 16-27	"a part of a security-related computer program, the contents of which are not viewable to a typical or normal user."	Indefinite under § 112, ¶ 1	
If §112, sixth paragraph does apply			
'235 Patent | Claims 1, 5, 8, 12, 15, and 19 (if §112, sixth paragraph, applies)			
non-viewable component	Not subject to § 112, ¶ 6, but if construed under § 112, ¶ 6: **<u>Claims 1, 5, 8, 12, 15, and 19 (function):</u>** determine whether the application component is present and whether the application component has been tampered with **<u>Claims 1, 5, 8, 12, 15, and 19 (structure):</u>** a computer application configured to perform the determining disclosed in Figs. 53; 54; 3:1-8; 3:28-31; 18:4-8; 19:44-48; 26:65-27:3.	**Invokes 35 U.S.C. § 112, ¶ 6:** **Function**: "track an electronic device; locate the device; determine whether an application component is present and whether the application component has been tampered with; automatically determine whether the application component operated correctly during last power-up of the device; in response to a determination that the application component did not operate correctly during last power-up of the device, automatically restore the application component from a backup fileset; automatically place the device under control of power on self test (POST) to proceed with powering-up the	

MICROSOFT CORP. EXHIBIT 1033
IPR2023-01185
Page 25 of 49

		device in response to a determination that the application component operated correctly during last power-up of the device; and include a validator module capable of determining whether the application component is present and whether the application component has been tampered with" **Structure**: Indefinite (no structure disclosed) Alternatively, if not indefinite under ¶ 6: **Structure**: "a program and/or data residing on a hidden partition or Host Protected Area (HPA) of a hard disk drive"	
'892 Patent | Claims 1, 11, 12, 15 (if §112, sixth paragraph, applies)			
non-viewable component	Not subject to § 112, ¶ 6, but if construed under § 112, ¶ 6: **<u>Claims 1, 11, 12, 15 (function):</u>** determine whether the application component is present and whether the application component has been tampered with	**Invokes 35 U.S.C. § 112, ¶ 6:** **Function**: "track an electronic device; locate the device; determine whether an application component is present and whether the application component has been tampered with; automatically determine whether the application component operated correctly	

	Claims 1, 11, 12, 15 (structure): a computer application configured to perform the determining disclosed in Figs. 53; 54; 3:1-8; 3:28-31; 18:4-8; 19:44-48; 26:65-27:3.	during last power-up of the device; in response to a determination that the application component did not operate correctly during last power-up of the device, automatically restore the application component from a backup fileset; automatically place the device under control of power on self test (POST) to proceed with powering-up the device in response to a determination that the application component operated correctly during last power-up of the device; and include a validator module capable of determining whether the application component is present and whether the application component has been tampered with" **Structure**: Indefinite (no structure disclosed) Alternatively, if not indefinite under ¶ 6: **Structure**: "a program and/or data residing on a hidden partition or Host Protected Area (HPA) of a hard disk drive"	

'410 Patent | Claims 1, 8 (if §112, sixth paragraph, applies)			
non-viewable component	Not subject to § 112, ¶ 6, but if construed under § 112, ¶ 6: **<u>Claims 1, 8, (function):</u>** • automatically determining whether the application component operated correctly during last power-up of the electronic device; • in response to a determination that the application component did not operate correctly during last power-up of the electronic device, automatically restoring the application component from a backup fileset; and • automatically placing the electronic device under control of power on self test (POST) to proceed with powering-up the electronic device in response to a determination that the application component operated correctly	**Invokes 35 U.S.C. § 112, ¶ 6:** **Function**: "track an electronic device; locate the device; determine whether an application component is present and whether the application component has been tampered with; automatically determine whether the application component operated correctly during last power-up of the device; in response to a determination that the application component did not operate correctly during last power-up of the device, automatically restore the application component from a backup fileset; automatically place the device under control of power on self test (POST) to proceed with powering-up the device in response to a determination that the application component operated correctly during last power-up of the device; and include a validator module capable of determining whether the application component is present and whether the	

	during last power-up of the electronic device. **<u>Claims 1, 8 (structure):</u>** a computer application configured to perform the determining disclosed in Figs. 54, 55; 2:49-52; 19:35-40; 25:31-49; 25:63-26:3; 26:12-22.	application component has been tampered with" **Structure**: Indefinite (no structure disclosed) Alternatively, if not indefinite under ¶ 6: **Structure**: "a program and/or data residing on a hidden partition or Host Protected Area (HPA) of a hard disk drive"	
'410 Patent | Claim 15 (if §112, sixth paragraph, applies)			
non-viewable component	Not subject to § 112, ¶ 6, but if construed under § 112, ¶ 6: **<u>Claim 15 (function):</u>** • associated with tracking and locating the electronic device **<u>Claim 15 (structure):</u>** a computer application configured to perform the determining disclosed in Figs. 40, 42, 44-50, 55, 71, 72; 8:27-40; 11:4-9; 15:25-37; 15:63-67; 16:15-17; 17:65-17:1; 19:20-25; 19:29-31; 20:17-27; 24:33-44.	**Invokes 35 U.S.C. § 112, ¶ 6:** **Function**: "track an electronic device; locate the device; determine whether an application component is present and whether the application component has been tampered with; automatically determine whether the application component operated correctly during last power-up of the device; in response to a determination that the application component did not operate correctly during last power-up of the device, automatically restore the application component from a backup fileset; automatically	

MICROSOFT CORP. EXHIBIT 1033
IPR2023-01185
Page 29 of 49

		place the device under control of power on self test (POST) to proceed with powering-up the device in response to a determination that the application component operated correctly during last power-up of the device; and include a validator module capable of determining whether the application component is present and whether the application component has been tampered with" **Structure**: Indefinite (no structure disclosed) Alternatively, if not indefinite under ¶ 6: **Structure**: "a program and/or data residing on a hidden partition or Host Protected Area (HPA) of a hard disk drive"	
'837 Patent | Claims 1-3, 8-14, 18-24 (if §112, sixth paragraph, applies)			
non-viewable security component	Not subject to § 112, ¶ 6, but if construed under § 112, ¶ 6: **<u>Claims 1, 5, 8, 12, 15, and 19 (function):</u>** determining whether the application component is present and whether the	**Invokes 35 U.S.C. § 112, ¶ 6:** **Function**: "provide security and tracking for an electronic device and contain a validator module capable of determining whether an application component is present and whether the application	

	application component has been tampered with **<u>Claims 1, 5, 8, 12, 15, and 19 (structure):</u>** A computer application configured to perform the determining disclosed in Figs. 53; 54; 3:1-8; 3:28-31; 18:4-8; 19:44-48; 26:65-27:3.	component has been tampered with" **Structure**: Indefinite (no structure disclosed) Alternatively, if not indefinite under ¶ 6: **Structure**: "a program and/or data residing on a hidden partition or Host Protected Area (HPA) of a hard disk drive"	
Term(s) / Claim(s)	**Softex's Proposed Construction**	**Defendants' Proposed Construction**	**Court's Construction**
If §112, sixth paragraph does not apply			
validator module • '837 patent claims 1-3, 8-14, 18-24; '235 patent claims 5, 12, and 19	Not subject to § 112, ¶ 6, plain and ordinary meaning, which is "a computer application that validates"	No construction offered	
If §112, sixth paragraph does apply			
'837 Patent | Claims 1, 12, 20 (if §112, sixth paragraph, applies)			
validator module	Not subject to § 112, ¶ 6, but if construed under § 112, ¶ 6: **<u>Claims 1, 12, and 20 (function):</u>** • determining whether the application component is present and whether the	**Invokes 35 U.S.C. § 112, ¶ 6:** **Function**: "determine whether an application component is present and whether the application component has been tampered with" **Structure**: Indefinite (no structure disclosed)	

	application component has been tampered with **<u>Claims 1, 12, and 20 (structure):</u>** a computer application configured to perform the determining disclosed in Figs. 53; 54; 3:1-8; 3:28-31; 18:4-8; 19:44-48; 26:65-27:3.	Alternatively, if not indefinite under ¶ 6: **Structure**: "a program that implements the steps shown in Figure 54"	
'235 Patent | Claims 5, 12, 19 (if §112, sixth paragraph, applies)			
validator module	Not subject to § 112, ¶ 6, but if construed under § 112, ¶ 6: **<u>Claims 5, 12, and 19 (function):</u>** determine whether the application component is present and whether the application component has been tampered with **<u>Claims 5, 12, and 19 (structure):</u>** a computer application configured to perform the determining disclosed in Figs. 53; 54; 3:1-8; 3:28-31; 18:4-8; 19:44-48; 26:65-27:3.	**Invokes 35 U.S.C. § 112, ¶ 6:** **Function**: "determine whether an application component is present and whether the application component has been tampered with" **Structure**: Indefinite (no structure disclosed) Alternatively, if not indefinite under ¶ 6: **Structure**: "a program that implements the steps shown in Figure 54"	
Term(s) / Claim(s)	**Softex's Proposed Construction**	**Defendants' Proposed Construction**	**Court's Construction**

If §112, sixth paragraph does not apply			
"BIOS component" / "basic input/output system (BIOS) component" • '235 patent claims 1-21; • '892 patent claims 1-19; • '603 patent claims 1-4, 10, 12-14, and 18-20; • '410 patent claims 15-20; • '710 patent claims 1-8, 11-21, 23	Not subject to § 112, ¶ 6, plain and ordinary meaning, which is "component of electronic device firmware that is used to start the computer system after it is powered on."	Indefinite under § 112, ¶ 1 Alternatively, if not indefinite under ¶ 1: "an option ROM BIOS image in an extension ROM BIOS"	
Basic input/output system (BIOS) security component" / "BIOS security component" • '837 patent claims 1-3, 8-14, 18-24 • '892 patent claims 11-14	Not subject to § 112, ¶ 6, plain and ordinary meaning, which is "security component of electronic device firmware that is used to start the computer system after it is powered on."	Indefinite under § 112, ¶ 1 Alternatively, if not indefinite under ¶ 1: "an option ROM BIOS image in an extension ROM BIOS"	
If §112, sixth paragraph does apply			
'235 Patent | Claims 1, 8, 15 (if §,112 sixth paragraph, applies)			
BIOS component terms	Not subject to § 112, ¶ 6, but if construed under §112, ¶ 6: **<u>Claims 1, 8, 15 (function):</u>** • determine whether the non-viewable component is present and whether the non-viewable component has been tampered with,	**Invokes 35 U.S.C. § 112, ¶ 6:** **Function**: "track an electronic device; locate the device; determine whether a non-viewable component is present and whether the non-viewable component has been tampered with; check integrity of an application component during a boot process for the device;	

	• check integrity of the application component during a boot process for the electronic device, • automatically cause the electronic device to restore the integrity of the application component in response to a negative integrity check of the application component **<u>Claims 1, 8, 15 (structure):</u>** a computer application configured to perform the determining, checking and causing disclosed in Figures 53, 54, 55, 71; 3:1-16; 18:4-8; 18:37-46; 19:43-48; 20:13-23; 26:13-50.	automatically cause the device to restore the integrity of the application component, in response to a negative integrity check of the application component; automatically determine whether the application component operated correctly during last power-up of the device; in response to a determination that the application component did not operate correctly during last power-up of the device, automatically restore the application component from a backup fileset; automatically place the device under control of power on self test (POST) to proceed with powering-up the device in response to a determination that the application component operated correctly during last power-up of the device; find information from the application component indicating that the application component was operating correctly; and prevent the device from booting to an operating system of the device, in response to receiving	

MICROSOFT CORP. EXHIBIT 1033
IPR2023-01185
Page 34 of 49

		notification that the device has been reported stolen" **Structure**: Indefinite (no structure disclosed) Alternatively, if not indefinite under ¶ 6: **Structure**: "an option ROM BIOS image in an extension ROM BIOS, as shown in Figure 49 and as described in associated portions of the specification, performing operations, as shown in Figure 53 and described in associated portions of the specification and as shown in Figure 54 and described in associated portions of the specification"	
'235 Patent | Claims 13, 20			
BIOS component terms	Not subject to § 112, ¶ 6, but if construed under §112, ¶ 6: **<u>Claims 13, 20 (function):</u>** • prevent the electronic device from booting to an operating system of the electronic device, in response to receiving notification that the electronic device has been reported stolen	**Invokes 35 U.S.C. § 112, ¶ 6:** **Function**: "track an electronic device; locate the device; determine whether a non-viewable component is present and whether the non-viewable component has been tampered with; check integrity of an application component during a boot process for the device; automatically cause the device to restore the integrity of the	

	Claims 13, 20 (structure): a computer application configured to perform the preventing in Figures 53, 54, 55, 71; 3:32-35; 18:59-61; 18:65-19:5; 19:23-30; 19:34-48; 19:43-48; 20:13-23; 26:13-50.	application component, in response to a negative integrity check of the application component; automatically determine whether the application component operated correctly during last power-up of the device; in response to a determination that the application component did not operate correctly during last power-up of the device, automatically restore the application component from a backup fileset; automatically place the device under control of power on self test (POST) to proceed with powering-up the device in response to a determination that the application component operated correctly during last power-up of the device; find information from the application component indicating that the application component was operating correctly; and prevent the device from booting to an operating system of the device, in response to receiving notification that the device has been reported stolen"	

MICROSOFT CORP. EXHIBIT 1033
IPR2023-01185
Page 36 of 49

		Structure: Indefinite (no structure disclosed) Alternatively, if not indefinite under ¶ 6: **Structure**: "an option ROM BIOS image in an extension ROM BIOS, as shown in Figure 49 and as described in associated portions of the specification, performing operations, as shown in Figure 53 and described in associated portions of the specification and as shown in Figure 54 and described in associated portions of the specification"	
'892 Patent | Claims 1, 11, 12, 15			
BIOS component terms	Not subject to § 112, ¶ 6, but if construed under §112, ¶ 6: **<u>Claims 1, 11, 12, 15 (function):</u>** • determine whether the non-viewable component is present and whether the non-viewable component has been tampered with, • check integrity of the application component during a boot process	**Invokes 35 U.S.C. § 112, ¶ 6:** **Function**: "track an electronic device; locate the device; determine whether a non-viewable component is present and whether the non-viewable component has been tampered with; check integrity of an application component during a boot process for the device; automatically cause the device to restore the integrity of the application component, in response to a negative integrity	

MICROSOFT CORP. EXHIBIT 1033
IPR2023-01185
Page 37 of 49

	for the electronic device, • automatically cause the electronic device to restore the integrity of the application component, in response to a negative integrity check of the application component **<u>Claims 1, 11, 12, 15 (structure):</u>** a computer application configured to perform the determining, checking and causing disclosed in Figures 53, 54, 55, 71; 3:1-16; 18:4-8; 18:37-46; 19:43-48; 20:13-23; 26:13-50.	check of the application component; automatically determine whether the application component operated correctly during last power-up of the device; in response to a determination that the application component did not operate correctly during last power-up of the device, automatically restore the application component from a backup fileset; automatically place the device under control of power on self test (POST) to proceed with powering-up the device in response to a determination that the application component operated correctly during last power-up of the device; find information from the application component indicating that the application component was operating correctly; and prevent the device from booting to an operating system of the device, in response to receiving notification that the device has been reported stolen"	

MICROSOFT CORP. EXHIBIT 1033
IPR2023-01185
Page 38 of 49

		Structure: Indefinite (no structure disclosed) Alternatively, if not indefinite under ¶ 6: **Structure**: "an option ROM BIOS image in an extension ROM BIOS, as shown in Figure 49 and as described in associated portions of the specification, performing operations, as shown in Figure 53 and described in associated portions of the specification and as shown in Figure 54 and described in associated portions of the specification"	
'603 Patent | Claims 1, 12, 18			
BIOS component terms	Not subject to § 112, ¶ 6, but if construed under §112, ¶ 6: **<u>Claims 1, 12, 18 (function):</u>** • automatically preventing the electronic device from completing the boot process if the BIOS component does not find the information from the application component indicating that the application	**Invokes 35 U.S.C. § 112, ¶ 6:** **Function**: "track an electronic device; locate the device; determine whether a non-viewable component is present and whether the non-viewable component has been tampered with; check integrity of an application component during a boot process for the device; automatically cause the device to restore the integrity of the application component, in response to a negative integrity check of the application	

MICROSOFT CORP. EXHIBIT 1033
IPR2023-01185
Page 39 of 49

	component was operating correctly **<u>Claims 1, 12, 18 (structure):</u>** a computer application configured to perform the preventing in Figures 53, 54, 55, 71; 3:32-35; 18:59-61; 18:65-19:5; 19:23-30; 19:34-48; 19:43-48; 20:13-23; 26:13-50.	component; automatically determine whether the application component operated correctly during last power-up of the device; in response to a determination that the application component did not operate correctly during last power-up of the device, automatically restore the application component from a backup fileset; automatically place the device under control of power on self test (POST) to proceed with powering-up the device in response to a determination that the application component operated correctly during last power-up of the device; find information from the application component indicating that the application component was operating correctly; and prevent the device from booting to an operating system of the device, in response to receiving notification that the device has been reported stolen" **Structure**: Indefinite (no structure disclosed)	

		Alternatively, if not indefinite under ¶ 6: **Structure**: "an option ROM BIOS image in an extension ROM BIOS, as shown in Figure 49 and as described in associated portions of the specification, performing operations, as shown in Figure 53 and described in associated portions of the specification and as shown in Figure 54 and described in associated portions of the specification"	
'410 Patent | Claim 15			
BIOS component terms	Not subject to § 112, ¶ 6, but if construed under §112, ¶ 6: **<u>Claims 15 (function):</u>** • automatically determining whether the application component operated correctly during last power-up of the electronic device; • in response to a determination that the application component did not operate correctly during last power-up of the	**Invokes 35 U.S.C. § 112, ¶ 6:** **Function**: "track an electronic device; locate the device; determine whether a non-viewable component is present and whether the non-viewable component has been tampered with; check integrity of an application component during a boot process for the device; automatically cause the device to restore the integrity of the application component, in response to a negative integrity check of the application component; automatically determine whether the	

	electronic device, automatically restoring the application component from a backup fileset; and • automatically placing the electronic device under control of power on self test (POST) to proceed with powering-up the device in response to a determination that the application component operated correctly during last power-up of the electronic device. **<u>Claim 15 (structure):</u>** a computer application configured to perform the determining, restoring and placing disclosed in Figures 53, 53, 54, 55, 71; 3:1-16; 17:61-18:12; 18:37-46; 18:59-61; 19:43-48; 20:13-23; 24:62-67; 25:41-62; 26:13-50.	application component operated correctly during last power-up of the device; in response to a determination that the application component did not operate correctly during last power-up of the device, automatically restore the application component from a backup fileset; automatically place the device under control of power on self test (POST) to proceed with powering-up the device in response to a determination that the application component operated correctly during last power-up of the device; find information from the application component indicating that the application component was operating correctly; and prevent the device from booting to an operating system of the device, in response to receiving notification that the device has been reported stolen" **Structure**: Indefinite (no structure disclosed) Alternatively, if not indefinite under ¶ 6:	

		Structure: "an option ROM BIOS image in an extension ROM BIOS, as shown in Figure 49 and as described in associated portions of the specification, performing operations, as shown in Figure 53 and described in associated portions of the specification and as shown in Figure 54 and described in associated portions of the specification"	
'710 Patent | Claims 1, 2, 19			
BIOS component terms	Not subject to § 112, ¶ 6, but if construed under §112, ¶ 6: **<u>Claims 1, 2, 19 (function):</u>** • determine whether the non-viewable component is present and whether the non-viewable component has been tampered with, • check integrity of the application component during a boot process for the electronic device, • automatically cause the electronic device to restore the integrity of the application	**Invokes 35 U.S.C. § 112, ¶ 6:** **Function**: "track an electronic device; locate the device; determine whether a non-viewable component is present and whether the non-viewable component has been tampered with; check integrity of an application component during a boot process for the device; automatically cause the device to restore the integrity of the application component, in response to a negative integrity check of the application component; automatically determine whether the application component operated correctly during last	

MICROSOFT CORP. EXHIBIT 1033
IPR2023-01185
Page 43 of 49

	component, in response to a negative integrity check of the application component **<u>Claims 1, 2, 19 (structure):</u>** a computer application configured to perform the determining, checking and causing disclosed in Figures 53, 54, 55, 71; 3:1-16; 18:4-8; 18:37-46; 19:43-48; 20:13-23; 26:13-50.	power-up of the device; in response to a determination that the application component did not operate correctly during last power-up of the device, automatically restore the application component from a backup fileset; automatically place the device under control of power on self test (POST) to proceed with powering-up the device in response to a determination that the application component operated correctly during last power-up of the device; find information from the application component indicating that the application component was operating correctly; and prevent the device from booting to an operating system of the device, in response to receiving notification that the device has been reported stolen" **Structure**: Indefinite (no structure disclosed) Alternatively, if not indefinite under ¶ 6:	

MICROSOFT CORP. EXHIBIT 1033
IPR2023-01185
Page 44 of 49

		Structure: "an option ROM BIOS image in an extension ROM BIOS, as shown in Figure 49 and as described in associated portions of the specification, performing operations, as shown in Figure 53 and described in associated portions of the specification and as shown in Figure 54 and described in associated portions of the specification"	
'837 Patent | Claims 1, 12			
BIOS Security Component Terms	Not subject to § 112, ¶ 6, but if construed under §112, ¶ 6: **<u>Claims 1, 12 (function):</u>** • check integrity of the application component during a boot process for the electronic device; • determine whether the non-viewable security component is present and whether the non-viewable security component has been tampered with; • automatically cause the electronic device to restore the integrity of the application	**Invokes 35 U.S.C. § 112, ¶ 6:** **Function**: "provide security and tracking for the electronic device; check integrity of an application component during a boot process for the device; determine whether a non-viewable security component is present and whether it has been tampered with; automatically cause the device to restore the integrity of the application component, in response to a negative integrity check for the application component; automatically cause the device to reinstall the application component from a hidden partition of a hard disk drive, in	

MICROSOFT CORP. EXHIBIT 1033
IPR2023-01185
Page 45 of 49

	component, in response to a negative integrity check for the application component; • prevent the electronic device from booting to the OS, in response to receiving notification that the electronic device has been reported stolen; **<u>Claims 1, 12 (structure):</u>** a computer application configured to perform the checking, determining, causing, and preventing disclosed in Figures 53, 54, 55, 71; 3:1-16; 3:32-35; 18:4-8; 18:37-46; 19:23-30; 19:34-48; 19:43-48; 20:13-23; 26:13-50; 26:65-27:3.	response to a negative integrity check for the application component; prevent the device from booting to an OS, in response to receiving notification that the device has been reported stolen; prevent the device from booting to the OS, in response to receiving notification that the device is to be disabled; cause the device to respond to a negative integrity check for the application component by using a backup copy of the application component to restore the integrity of the application component; locate the device; disable the device; and track the device until the device is disabled" **Structure**: Indefinite (no structure disclosed) Alternatively, if not indefinite under ¶ 6: **Structure**: "an option ROM BIOS image in an extension ROM BIOS, as shown in Figure 49 and as described in associated portions of the	

MICROSOFT CORP. EXHIBIT 1033
IPR2023-01185
Page 46 of 49

		specification, performing operations, as shown in Figure 53 and described in associated portions of the specification and as shown in Figure 54 and described in associated portions of the specification"	
'837 Patent | Claim 20			
BIOS Security Component Terms	Not subject to § 112, ¶ 6, but if construed under §112, ¶ 6: **<u>Claims 20 (function):</u>** • check integrity of the application component during a boot process for the electronic device; • automatically cause the electronic device to restore the integrity of the application component, in response to a negative integrity check for the application component; • determine whether the non-viewable security component is present and whether the non-viewable security component has been tampered with	**Invokes 35 U.S.C. § 112, ¶ 6:** **Function**: "provide security and tracking for the electronic device; check integrity of an application component during a boot process for the device; determine whether a non-viewable security component is present and whether it has been tampered with; automatically cause the device to restore the integrity of the application component, in response to a negative integrity check for the application component; automatically cause the device to reinstall the application component from a hidden partition of a hard disk drive, in response to a negative integrity check for the application component; prevent the device from booting to an OS, in response to receiving	

MICROSOFT CORP. EXHIBIT 1033
IPR2023-01185
Page 47 of 49

	Claims 20 (structure): a computer application configured to perform the checking, causing, and determining disclosed in Figures 53, 54, 55, 71; 3:1-16; 18:4-8; 18:37-46; 18:59-61; 18:65-19:5; 19:43-48; 20:13-23; 26:13-50.	notification that the device has been reported stolen; prevent the device from booting to the OS, in response to receiving notification that the device is to be disabled; cause the device to respond to a negative integrity check for the application component by using a backup copy of the application component to restore the integrity of the application component; locate the device; disable the device; and track the device until the device is disabled" **Structure**: Indefinite (no structure disclosed) Alternatively, if not indefinite under ¶ 6: **Structure**: "an option ROM BIOS image in an extension ROM BIOS, as shown in Figure 49 and as described in associated portions of the specification, performing operations, as shown in Figure 53 and described in associated portions of the specification and as shown in Figure 54 and	

		described in associated portions of the specification"	
'892 Patent | Claims 11, 12			
BIOS Security Component Terms	Not subject to § 112, ¶ 6, but if construed under §112, ¶ 6: **<u>Claims 11, 12 (function):</u>** • determine whether the non-viewable component is present and whether the non-viewable component has been tampered with, • check integrity of the application component during a boot process for the electronic device, and • automatically cause the electronic device to restore the integrity of the application component, in response to a negative integrity check of the application component, **<u>Claims 11, 12 (structure):</u>** a computer application configured to perform the checking, causing, and determining disclosed in Figures 53, 54, 55, 71; 3:1-16;	**Invokes 35 U.S.C. § 112, ¶ 6:** **Function**: "provide security and tracking for the electronic device; check integrity of an application component during a boot process for the device; determine whether a non-viewable security component is present and whether it has been tampered with; automatically cause the device to restore the integrity of the application component, in response to a negative integrity check for the application component; automatically cause the device to reinstall the application component from a hidden partition of a hard disk drive, in response to a negative integrity check for the application component; prevent the device from booting to an OS, in response to receiving notification that the device has been reported stolen; prevent the device from booting to the OS, in response to receiving notification that the device is to	

MICROSOFT CORP. EXHIBIT 1033
IPR2023-01185
Page 49 of 49

	18:4-8; 18:37-46; 19:43-48; 20:13-23; 26:13-50.	be disabled; cause the device to respond to a negative integrity check for the application component by using a backup copy of the application component to restore the integrity of the application component; locate the device; disable the device; and track the device until the device is disabled" **Structure**: Indefinite (no structure disclosed) Alternatively, if not indefinite under ¶ 6: **Structure**: "an option ROM BIOS image in an extension ROM BIOS, as shown in Figure 49 and as described in associated portions of the specification, performing operations, as shown in Figure 53 and described in associated portions of the specification and as shown in Figure 54 and described in associated portions of the specification"	