

**Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants’ Initial Invalidity Contentions – Exhibit F-37**

Claim Chart Against U.S. Patent No. 8,506,649 (“’649 patent”)

Charted Reference: UK Patent Application No. 2,369,205 to Hayward (“Hayward”)

Hayward, filed on November 17, 2000 and published on May 22, 2002, qualifies as prior art to the ’649 patent under at least 35 U.S.C. § 102(b).

As set forth in the chart below, all asserted claims of the ’649 patent are anticipated and/or obvious over Hayward.¹

Except where specifically noted otherwise, this chart applies the apparent constructions of claim terms as used by Softex LLC (“Softex”) in its infringement contentions; such use, however, does not imply that Defendants adopt or agree with Softex’s constructions in any way.

To the extent the charted reference is held not to explicitly or inherently disclose any particular element below, such limitations were obvious for the reasons stated below and in Defendants’ Initial Invalidity Contentions, which are incorporated herein by reference.

Defendants are investigating this prior art and have not yet completed discovery from third parties who may have information concerning it. Defendants reserve the right to modify, amend, and/or supplement these contentions as information becomes available, and as discovery proceeds.

Evidence of Invalidity	
Claim Element	Claim 1
1.[pre] A mobile electronic device, comprising:	<i>To the extent that the preamble is limiting, it is disclosed or suggested by Hayward. For example:</i> A personal data device have a memory for storing personal data and a data storage and processing module for enabling operation of the device.” (Abstract).

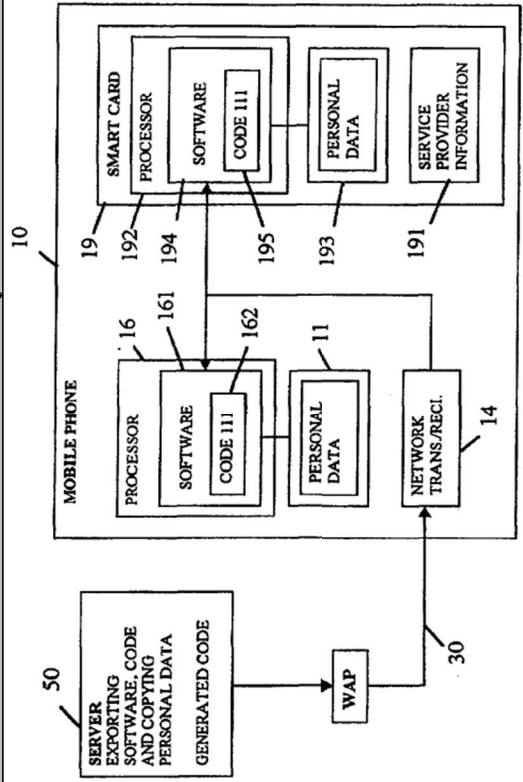
¹ The excerpts cited herein are exemplary. For any claim limitation, Defendants may rely on excerpts cited for any other limitation and/or additional excerpts not set forth fully herein to the extent necessary to provide a more comprehensive explanation for a reference’s disclosure of a limitation. Where an excerpt refers to or discusses a figure or figure items, that figure and any additional descriptions of that figure should be understood to be incorporated by reference as if set forth fully therein.

**Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants' Initial Invalidity Contentions – Exhibit F-37**

Claim Element	Evidence of Invalidity
	“Personal data devices, for example digital personal assistants, are known for storing personal data, for example, to act as personal organisers.” (1:5-6). “It is an object of the present invention to provide greater security of such stored personal data.” (1:22-23). “According to a first aspect of the invention there is provided a personal data device including data storage means for storing personal data, access authentication means for restricting access to the personal data stored in the data storage means to an authorised user, a data storage and processing module for enabling operation of the personal data device, data protection software and a synchronisation authentication code, at least a first element of the code being stored in the data storage means and at least a second element of the code being stored in the data storage and processing module, such that, when the at least a first element of the code stored in the data storage means and the at least a second element of the code stored in the module correspond, access is allowed by the data protection software to the personal data and, when the at least a first element of the code stored on the module and the at least a second element of the code stored in the data storage means do not correspond, the personal data and/or any electronic signatures stored in the data storage means are deleted by the data protection software.” (1:23-2:6). “The system of the invention as shown in Fig. 1 includes a web server 50 connected to the Internet 30 by a connection 306. The web server includes downloadable data protection software and a generator for generating downloadable authentication codes 520. Also connectable to the Internet are a number of devices, belonging to the same user, which may contain personal data. These include a mobile telephone or personal data device 10 connectable by a connection 302, a laptop computer 101 connectable by a connection 303, a PDA (personal data administrator) 102 connectable by connection 304, a home PC 60 connectable by a connection 301 and an office PC 600 connectable by a connection 305.” (9:19-28).

Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants’ Initial Invalidity Contentions – Exhibit F-37

Claim Element	Evidence of Invalidity
	“As shown in Fig. 2, the system of one aspect of the invention includes a personal data device 10 including a data store 11 accessible by a processor 16. Also connected to the processor is a short-range radio communications transmitter/receiver 12, connected to a first radio antenna 13, and a mobile telephone transmitter/receiver 14 connected to a second radio antenna 15. The mobile telephone transmitter/receiver 14 is adapted to use a mobile telephone network 20 over a radio link 21 to access an Internet network 30. It will be understood that the antennas 13 and 15 may be combined into a single antenna. Also connected to the processor is an authentication module 17, a display 18 and a reset facility 193.” (11:23-32). “Although the invention has been described in relation to a mobile telephone, it will be apparent that the invention has equal applicability to, and a similar mode of operation in, the protection of data on, for example, a personal data administrator (PDA), a laptop computer and a personal computer. In the case of, for example, a personal computer, it is possible in an embodiment of the invention, to nominate which files or folders are to be protected.” (15:28-16:2).

Claim Element	Evidence of Invalidity
	 The diagram, labeled Fig. 1A, illustrates a system architecture. On the left, a box labeled 50 represents a 'SERVER EXPORTING SOFTWARE CODE AND COPYING PERSONAL DATA GENERATED CODE'. An arrow points from this server to a box labeled 'WAP'. From the 'WAP', an arrow points to a box labeled 30, which is connected to a 'NETWORK TRANS./RECI.' block labeled 14. This network block is connected to a 'MOBILE PHONE' block labeled 10. Inside the mobile phone, there are two main sections. The top section contains a 'SMART CARD' (19) which includes a 'PROCESSOR' (192), 'SOFTWARE' (194), and 'CODE 111' (195). Below this, there is a 'PERSONAL DATA' block (193) and a 'SERVICE PROVIDER INFORMATION' block (191). The bottom section of the mobile phone contains a 'PROCESSOR' (16), 'SOFTWARE' (161), and 'CODE 111' (162). An arrow points from the 'CODE 111' (162) in the bottom section to the 'SOFTWARE' (194) in the top section. Another arrow points from the 'PERSONAL DATA' (11) block to the 'PERSONAL DATA' (193) block in the top section. Fig. 1A

Claim Element	Evidence of Invalidation
	The diagram illustrates a network architecture. At the top, a cloud labeled 'INTERNET 30' is connected to a 'Web Server 50'. The Web Server contains two components: 'Copy of personal data 511' and 'Downloadable data protection software and authentication code 520'. Below the Internet cloud, several devices are shown: 'Mobile phone 10' (containing 'Smart card 19'), 'Laptop 101', 'PDA 102', 'Home PC 60', and 'Office PC 600'. These devices are interconnected with the Internet cloud via various lines (solid and dashed) labeled with reference numerals 710 through 718. Specifically, the Mobile phone 10 is connected to the Internet via 717 and 716. The Laptop 101 is connected via 712 and 713. The PDA 102 is connected via 714 and 715. The Home PC 60 is connected via 710 and 711. The Office PC 600 is connected via 714 and 715. Additionally, there are direct connections from the devices to the Web Server: Mobile phone 10 to 511 (716), Laptop 101 to 511 (712), PDA 102 to 511 (714), Home PC 60 to 511 (710), and Office PC 600 to 511 (715). There are also connections from the devices to the Web Server via the Internet cloud: Mobile phone 10 to 520 (717), Laptop 101 to 520 (712), PDA 102 to 520 (714), Home PC 60 to 520 (711), and Office PC 600 to 520 (715). Fig. 1 <i>To the extent that the preamble is not fully disclosed or suggested by Hayward, the preamble would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidation Contentions.</i>

**Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants' Initial Invalidity Contentions – Exhibit F-37**

Claim Element	Evidence of Invalidity
1[a] a processor;	<i>This limitation is disclosed or suggested by Hayward. For example:</i> “A personal data device have a memory for storing personal data and a data storage and processing module for enabling operation of the device.” (Abstract). “As shown in Fig. 2, the system of one aspect of the invention includes a personal data device 10 including a data store 11 accessible by a processor 16. Also connected to the processor is a short-range radio communications transmitter/receiver 12, connected to a first radio antenna 13, and a mobile telephone transmitter/receiver 14 connected to a second radio antenna 15. The mobile telephone transmitter/receiver 14 is adapted to use a mobile telephone network 20 over a radio link 21 to access an Internet network 30. It will be understood that the antennas 13 and 15 may be combined into a single antenna. Also connected to the processor is an authentication module 17, a display 18 and a reset facility 193.” (11:23-32). “Although the invention has been described in relation to a mobile telephone, it will be apparent that the invention has equal applicability to, and a similar mode of operation in, the protection of data on, for example, a personal data administrator (PDA), a laptop computer and a personal computer. In the case of, for example, a personal computer, it is possible in an embodiment of the invention, to nominate which files or folders are to be protected.” (15:28-16:2). <i>To the extent that this limitation is not fully disclosed or suggested by Hayward, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i>
1[b] one or more non-transitory machine-readable storage media responsive to the processor; and	<i>This limitation is disclosed or suggested by Hayward. For example:</i> “A personal data device have a memory for storing personal data and a data storage and processing module for enabling operation of the device.” (Abstract).

**Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants' Initial Invalidation Contentions – Exhibit F-37**

Claim Element	Evidence of Invalidity
	“As shown in Fig. 2, the system of one aspect of the invention includes a personal data device 10 including a data store 11 accessible by a processor 16. Also connected to the processor is a short-range radio communications transmitter/receiver 12, connected to a first radio antenna 13, and a mobile telephone transmitter/receiver 14 connected to a second radio antenna 15. The mobile telephone transmitter/receiver 14 is adapted to use a mobile telephone network 20 over a radio link 21 to access an Internet network 30. It will be understood that the antennas 13 and 15 may be combined into a single antenna. Also connected to the processor is an authentication module 17, a display 18 and a reset facility 193.” (11:23-32). “Although the invention has been described in relation to a mobile telephone, it will be apparent that the invention has equal applicability to, and a similar mode of operation in, the protection of data on, for example, a personal data administrator (PDA), a laptop computer and a personal computer. In the case of, for example, a personal computer, it is possible in an embodiment of the invention, to nominate which files or folders are to be protected.” (15:28-16:2). <i>To the extent that this limitation is not fully disclosed or suggested by Hayward, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidation Contentions.</i>
1[c] a security application in at least one of the non-transitory machine-readable storage media, wherein the security application is operable to perform operations comprising:	<i>This limitation is disclosed or suggested by Hayward. For example:</i> “According to a first aspect of the invention there is provided a personal data device including data storage means for storing personal data, access authentication means for restricting access to the personal data stored in the data storage means to an authorised user, a data storage and processing module for enabling operation of the personal data device, data protection software and a synchronisation authentication code, at least a first element of the code being stored in the data storage means and at least a second element of the code being stored in the data storage and processing module, such that, when the at least a first element of the code stored in the data

**Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants' Initial Invalidity Contentions – Exhibit F-37**

Claim Element	Evidence of Invalidity
	storage means and the at least a second element of the code stored in the module correspond, access is allowed by the data protection software to the personal data and, when the at least a first element of the code stored on the module and the at least a second element of the code stored in the data storage means do not correspond, the personal data and/or any electronic signatures stored in the data storage means are deleted by the data protection software.” (1:23-2:6). “Authentication codes and data protection software can be downloaded from the web server 50 to any of the authorised user’s devices via the Internet 30. This means the data can be protected from misuse in a manner to be described and synchronisation can be restricted to devices belonging to the same user.” (10:25-28). <i>To the extent that this limitation is not fully disclosed or suggested by Hayward, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i>
1[c][i] enabling an owner of the mobile electronic device to register the mobile electronic device with a security service residing at least partially on one or more servers;	<i>This limitation is disclosed or suggested by Hayward. For example:</i> “The system of the invention as shown in Fig. 1 includes a web server 50 connected to the Internet 30 by a connection 306. The web server includes downloadable data protection software and a generator for generating downloadable authentication codes 520. Also connectable to the Internet are a number of devices, belonging to the same user, which may contain personal data. These include a mobile telephone or personal data device 10 connectable by a connection 302, a laptop computer 101 connectable by a connection 303, a PDA (personal data administrator) 102 connectable by connection 304, a home PC 60 connectable by a connection 301 and an office PC 600 connectable by a connection 305.” (9:19-28). “As shown in Fig. 2, associated with the personal data device 10 is a database server 50 having a database data store 51 in which can be stored a copy of the data to be stored in the personal data device. Preferably the database server includes

***Softex LLC v. Defendants*, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants’ Initial Invalidity Contentions – Exhibit F-37**

Claim Element	Evidence of Invalidity
	encryption/decryption facilities so that the personal data may be stored in an encrypted format. The database server 50 may conveniently be a server connected to the Internet 30. In this case it is possible for the personal data device to communicate with the server over a mobile telephone link 21 from the mobile telephone compatible transmitter/receiver 14 in the personal data device to access the Internet 30. On first logging into the personal data device 10, it is therefore necessary to log into and register the personal data device with the Internet database server 50. This registration, as well as submitting usual identification data includes transmitting to the database server the registered fingerprint or iris pattern or other authentication data registered in the personal data device for a purpose described below.” (14:9-22). “By means of the Internet 30, the personal data device 10 may be connected to an issuing authority web-site server 40 or a web-site database server 50. The database server 50 is provided with a data store 51. The database web-site server is also connectable by the Internet 30 to a personal computer 60 having a data store 61.” (12:1-5).

Claim Element	Evidence of Invalidity
1[c][ii] causing the mobile electronic device to automatically send identifying information from the mobile electronic device to the security service;	Fig. 2 <i>To the extent that this limitation is not fully disclosed or suggested by Hayward, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i> <i>This limitation is disclosed or suggested by Hayward. For example:</i> “As shown in Fig. 2, associated with the personal data device 10 is a database server 50 having a database data store 51 in which can be stored a copy of the data to be stored in the personal data device. Preferably the database server includes encryption/decryption facilities so that the personal data may be stored in an encrypted format. The database server 50 may conveniently be a server connected to the Internet 30. In this case it is possible for the personal data device to communicate with the server over a mobile telephone link 21 from the mobile telephone

**Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants' Initial Invalidation Contentions – Exhibit F-37**

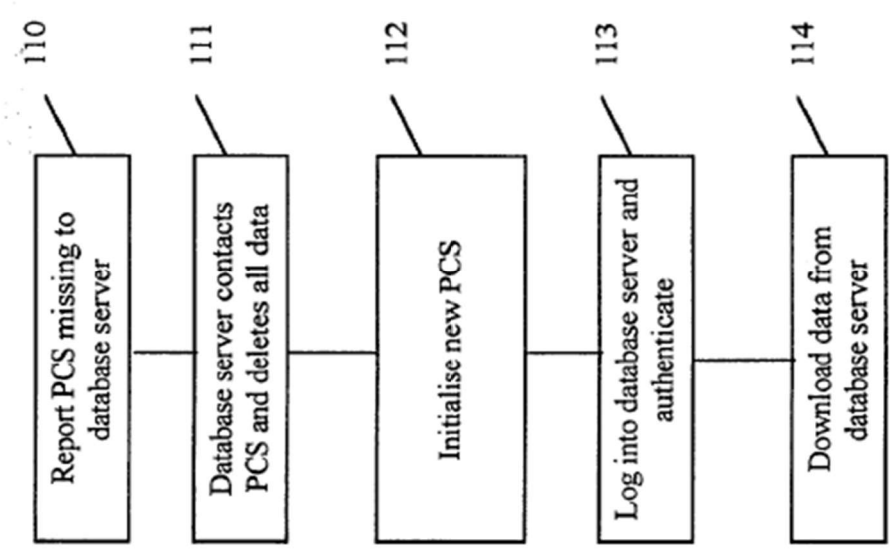
Claim Element	Evidence of Invalidity
	compatible transmitter/receiver 14 in the personal data device to access the Internet 30. On first logging into the personal data device 10, it is therefore necessary to log into and register the personal data device with the Internet database server 50. This registration, as well as submitting usual identification data includes transmitting to the database server the registered fingerprint or iris pattern or other authentication data registered in the personal data device for a purpose described below.” (14:9-22). <i>To the extent that this limitation is not fully disclosed or suggested by Hayward, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidation Contentions.</i>
1[c][iii] after the owner has registered the mobile electronic device with the security service, causing the mobile electronic device to periodically communicate with the security service, when the mobile electronic device is in a state other than a state in which the mobile electronic device is powered off;	<i>This limitation is disclosed or suggested by Hayward. For example:</i> “As indicated above, and referring again to Fig. 2, the personal data device is also connectable, for example using the Internet 30, to a database server 50 having a database data store 51 for storing a copy of the data stored in the data store 11 of the personal data device 10. The database server may thus be used to store a duplicate version of the data and software stored in the personal data device. It is therefore necessary for the personal data device to be logged into the database server from time to time to synchronise the data stored on the personal data device and on the database server. For example, the personal data device may contact the database server 50 over the internet 30 every time an amendment or addition is made to the personal data stored on the personal data device. Alternatively, updates may be made after, say, every three changes or at some other frequency chosen by the user. Facilities may be provided on the database server to compare the version of the personal data already stored with the current data in the personal data device and only to copy in either direction, as appropriate, any data which has changed or is new on either the device or the server, to create new current versions on both the device and the server.” (20:28-21:12).

Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants’ Initial Invalidity Contentions – Exhibit F-37

Claim Element	Evidence of Invalidity
	<i>To the extent that this limitation is not fully disclosed or suggested by Hayward, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i>
1[c][iv] after the owner has registered the mobile electronic device with the security service, accepting a notification at the mobile electronic device from the security service, wherein the notification comprises a message indicating that the owner of the mobile electronic device has reported a loss or requested disabling of the mobile electronic device;	<i>This limitation is disclosed or suggested by Hayward. For example:</i> “The database server also performs an important function when a personal data device is missing or replaced. Referring to Fig.12, if a personal data device 10 is reported missing, step 110, to the database server 50, the database server seeks to contact the missing device. The device may, for example, be reported missing by contacting the database server via the Internet or telephone. The database server preferably contacts the device in a manner undetectable to a user, 30 for example, by sending a SMS message. Either when the device is next switched on or, alternatively, the personal data device may be provided with sufficient functionality even when nominally powered off to receive the SMS message and act upon it. Such functionality may be powered by a main battery of the personal data device or by an auxiliary standby battery. The standby power also powers a reset 193 for a purpose to be described. An icon may be displayed on the personal data device display when the device is powered off to indicate that the data is protected by being duplicated on the database server. On being notified that the personal data device is no longer in the possession of the authorised user, the database server compares the data stored in the personal data device with that stored for that device in the database and, if appropriate, updates the version stored in the database using the data stored in the personal data device. The database server then signals the personal data device to delete, step 111, the data and/or any electronic signatures held in the personal data device so that the data cannot be used by an unauthorised user, for example, by using the reset facility 193 to reset all variables stored in the personal data device to default values. Moreover, the database server does not authorise subsequent registration of the personal data device with the database server, except by the authorised user. Therefore, even if an unauthorised user manages to bypass the fingerprint or other authentication facility incorporated in the personal data device, the device provides

Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants' Initial Invalidity Contentions – Exhibit F-37

Claim Element	Evidence of Invalidity
	only limited functionality to the unauthorised user. In addition, the data store 11 of the personal data device may be designed to be sufficiently volatile that should a thief remove the power supply to prevent a "silent call" deleting the stored data, the stored data and/or any stored electronic signatures will be automatically deleted and, for example, all variables reset to default values when the power supply is restored. The database server may also contact all issuing authorities to inform them that the device is missing, so that the issuing authorities may, if desired, issue new account numbers, codes or other details for subsequent use by the authorised user on a replacement personal data device. For this purpose, the issuing authority may, after suitable authentication, download the new data into the user's data on the database server to be subsequently downloaded to the user's replacement personal data device." (21:24-22:28).

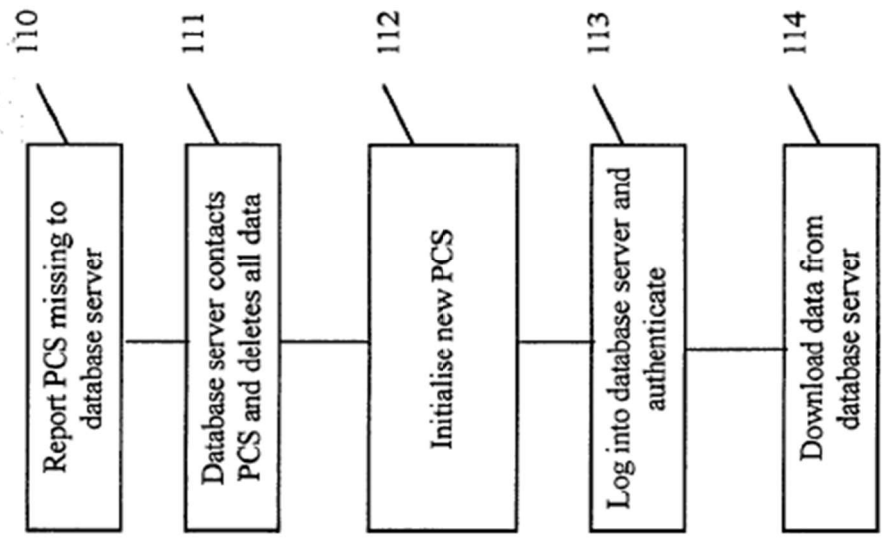
Claim Element	Evidence of Invalidity
	 <pre> graph TD 110[110 Report PCS missing to database server] --> 111[111 Database server contacts PCS and deletes all data] 111 --> 112[112 Initialise new PCS] 112 --> 113[113 Log into database server and authenticate] 113 --> 114[114 Download data from database server] </pre> <i>To the extent that this limitation is not fully disclosed or suggested by Hayward, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i>

Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants' Initial Invalidity Contentions – Exhibit F-37

Claim Element	Evidence of Invalidity
1[c][v] in response to receiving the notification, automatically disabling at least one user function of the mobile electronic device while still allowing the mobile electronic device to communicate with the security service; and	<i>This limitation is disclosed or suggested by Hayward. For example:</i> “The database server also performs an important function when a personal data device is missing or replaced. Referring to Fig. 12, if a personal data device 10 is reported missing, step 110, to the database server 50, the database server seeks to contact the missing device. The device may, for example, be reported missing by contacting the database server via the Internet or telephone. The database server preferably contacts the device in a manner undetectable to a user, 30 for example, by sending a SMS message. Either when the device is next switched on or, alternatively, the personal data device may be provided with sufficient functionality even when nominally powered off to receive the SMS message and act upon it. Such functionality may be powered by a main battery of the personal data device or by an auxiliary standby battery. The standby power also powers a reset 193 for a purpose to be described. An icon may be displayed on the personal data device display when the device is powered off to indicate that the data is protected by being duplicated on the database server. On being notified that the personal data device is no longer in the possession of the authorised user, the database server compares the data stored in the personal data device with that stored for that device in the database and, if appropriate, updates the version stored in the database using the data stored in the personal data device. The database server then signals the personal data device to delete, step 111, the data and/or any electronic signatures held in the personal data device so that the data cannot be used by an unauthorised user, for example, by using the reset facility 193 to reset all variables stored in the personal data device to default values. Moreover, the database server does not authorise subsequent registration of the personal data device with the database server, except by the authorised user. Therefore, even if an unauthorised user manages to bypass the fingerprint or other authentication facility incorporated in the personal data device, the device provides only limited functionality to the unauthorised user. In addition, the data store 11 of the personal data device may be designed to be sufficiently volatile that should a thief remove the power supply to prevent a "silent call" deleting the stored data, the stored data and/or any stored electronic signatures will be automatically deleted and, for example, all variables reset to default values when the power supply is restored. The

***Softex LLC v. Defendants*, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants’ Initial Invalidity Contentions – Exhibit F-37**

Claim Element	Evidence of Invalidity
	database server may also contact all issuing authorities to inform them that the device is missing, so that the issuing authorities may, if desired, issue new account numbers, codes or other details for subsequent use by the authorised user on a replacement personal data device. For this purpose, the issuing authority may, after suitable authentication, download the new data into the user's data on the database server to be subsequently downloaded to the user's replacement personal data device.” (21:24-22:28).

Claim Element	Evidence of Invalidity
	 <pre> graph TD 110[110 Report PCS missing to database server] --> 111[111 Database server contacts PCS and deletes all data] 111 --> 112[112 Initialise new PCS] 112 --> 113[113 Log into database server and authenticate] 113 --> 114[114 Download data from database server] </pre> <i>To the extent that this limitation is not fully disclosed or suggested by Hayward, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i>

Claim Element	Evidence of Invalidity
1[c][vi] automatically causing at least some user data to be copied from the mobile electronic device to at least one of the servers;	<i>This limitation is disclosed or suggested by Hayward. For example:</i> “The database server also performs an important function when a personal data device is missing or replaced. Referring to Fig. 12, if a personal data device 10 is reported missing, step 110, to the database server 50, the database server seeks to contact the missing device. The device may, for example, be reported missing by contacting the database server via the Internet or telephone. The database server preferably contacts the device in a manner undetectable to a user, 30 for example, by sending a SMS message. Either when the device is next switched on or, alternatively, the personal data device may be provided with sufficient functionality even when nominally powered off to receive the SMS message and act upon it. Such functionality may be powered by a main battery of the personal data device or by an auxiliary standby battery. The standby power also powers a reset 193 for a purpose to be described. An icon may be displayed on the personal data device display when the device is powered off to indicate that the data is protected by being duplicated on the database server. On being notified that the personal data device is no longer in the possession of the authorised user, the database server compares the data stored in the personal data device with that stored for that device in the database and, if appropriate, updates the version stored in the database using the data stored in the personal data device. The database server then signals the personal data device to delete, step 111, the data and/or any electronic signatures held in the personal data device so that the data cannot be used by an unauthorised user, for example, by using the reset facility 193 to reset all variables stored in the personal data device to default values. Moreover, the database server does not authorise subsequent registration of the personal data device with the database server, except by the authorised user. Therefore, even if an unauthorised user manages to bypass the fingerprint or other authentication facility incorporated in the personal data device, the device provides only limited functionality to the unauthorised user. In addition, the data store 11 of the personal data device may be designed to be sufficiently volatile that should a thief remove the power supply to prevent a "silent call" deleting the stored data, the stored data and/or any stored electronic signatures will be automatically deleted and, for example, all variables reset to default values when the power supply is restored. The

Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants’ Initial Invalidity Contentions – Exhibit F-37

Claim Element	Evidence of Invalidity
	database server may also contact all issuing authorities to inform them that the device is missing, so that the issuing authorities may, if desired, issue new account numbers, codes or other details for subsequent use by the authorised user on a replacement personal data device. For this purpose, the issuing authority may, after suitable authentication, download the new data into the user's data on the database server to be subsequently downloaded to the user's replacement personal data device.” (21:24-22:28). “As indicated above, and referring again to Fig. 2, the personal data device is also connectable, for example using the Internet 30, to a database server 50 having a database data store 51 for storing a copy of the data stored in the data store 11 of the personal data device 10. The database server may thus be used to store a duplicate version of the data and software stored in the personal data device. It is therefore necessary for the personal data device to be logged into the database server from time to time to synchronise the data stored on the personal data device and on the database server. For example, the personal data device may contact the database server 50 over the internet 30 every time an amendment or addition is made to the personal data stored on the personal data device. Alternatively, updates may be made after, say, every three changes or at some other frequency chosen by the user. Facilities may be provided on the database server to compare the version of the personal data already stored with the current data in the personal data device and only to copy in either direction, as appropriate, any data which has changed or is new on either the device or the server, to create new current versions on both the device and the server.” (20:28-21:12). “As shown in Fig. 11, in an embodiment of the invention, the device may be further protected by automatic deletion of the data stored in the personal data device on failure successfully to log into the personal data device after, for example, a second attempt. Thus, the user makes a first attempt to log into the device, step 1000, and if successful is presented, step 1010, with a device main menu. If unsuccessful, a second attempt, step 1020, may be made and if successful the main menu is presented, step 1010. However, if logging in is unsuccessful at the second attempt the

**Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants' Initial Invalidity Contentions – Exhibit F-37**

Claim Element	Evidence of Invalidity
	device deletes, step 1040, all the data and/or any electronic 25 signatures in the personal data device. Preferably, before deleting the data, the device contacts the database server 50 and uploads, step 1030, at least any data to the database server that is necessary to create a current backup. An authorised user may, subject to proper authentication, subsequently reload the data from the backup into the personal data device. In a similar manner, the data and/or any electronic signatures will be deleted if an attempt is made to read personal data using an incompatible authentication code.” (23:17-31). <i>To the extent that this limitation is not fully disclosed or suggested by Hayward, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i>
1[d] wherein the one or more non-transitory machine-readable storage media comprises non-volatile memory;	<i>This limitation is disclosed or suggested by Hayward. For example:</i> “A personal data device have a memory for storing personal data and a data storage and processing module for enabling operation of the device.” (Abstract). “Personal data devices, for example digital personal assistants, are known for storing personal data, for example, to act as personal organisers.” (1:5-6). “It is an object of the present invention to provide greater security of such stored personal data.” (1:22-23). “According to a first aspect of the invention there is provided a personal data device including data storage means for storing personal data, access authentication means for restricting access to the personal data stored in the data storage means to an authorised user, a data storage and processing module for enabling operation of the personal data device, data protection software and a synchronisation authentication code, at least a first element of the code being stored in the data storage means and at least a second element of the code being stored in the data storage and processing

Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants' Initial Invalidity Contentions – Exhibit F-37

Claim Element	Evidence of Invalidity
	module, such that, when the at least a first element of the code stored in the data storage means and the at least a second element of the code stored in the module correspond, access is allowed by the data protection software to the personal data and, when the at least a first element of the code stored on the module and the at least a second element of the code stored in the data storage means do not correspond, the personal data and/or any electronic signatures stored in the data storage means are deleted by the data protection software.” (1:23-2:6). “The system of the invention as shown in Fig. 1 includes a web server 50 connected to the Internet 30 by a connection 306. The web server includes downloadable data protection software and a generator for generating downloadable authentication codes 520. Also connectable to the Internet are a number of devices, belonging to the same user, which may contain personal data. These include a mobile telephone or personal data device 10 connectable by a connection 302, a laptop computer 101 connectable by a connection 303, a PDA (personal data administrator) 102 connectable by connection 304, a home PC 60 connectable by a connection 301 and an office PC 600 connectable by a connection 305.” (9:19-28). “As shown in Fig. 2, the system of one aspect of the invention includes a personal data device 10 including a data store 11 accessible by a processor 16. Also connected to the processor is a short-range radio communications transmitter/receiver 12, connected to a first radio antenna 13, and a mobile telephone transmitter/receiver 14 connected to a second radio antenna 15. The mobile telephone transmitter/receiver 14 is adapted to use a mobile telephone network 20 over a radio link 21 to access an Internet network 30. It will be understood that the antennas 13 and 15 may be combined into a single antenna. Also connected to the processor is an authentication module 17, a display 18 and a reset facility 193.” (11:23-32). “Although the invention has been described in relation to a mobile telephone, it will be apparent that the invention has equal applicability to, and a similar mode of operation in, the protection of data on, for example, a personal data administrator (PDA), a laptop computer and a personal computer. In the case of, for example, a

Claim Element	Evidence of Invalidity
	personal computer, it is possible in an embodiment of the invention, to nominate which files or folders are to be protected.” (15:28-16:2). “Moreover, the feature of protection of data by the use of an authentication code and protection software downloaded from a module such as a smart card, so that an element of the code is stored in the device memory and an element of the code stored on the smart card, to prevent operation of the device, or access to personal data or electronic signatures stored in the personal data device, unless the original smart card is installed, may be used without, or independently, of the feature of maintaining a copy of the personal data or electronic signature on another computer such as a PC or Internet server.” (24:12-18). <pre>graph TD 50[SERVER EXPORTING SOFTWARE, CODE AND COPYING PERSONAL DATA GENERATED CODE] --> 16[PROCESSOR] 50 --> 161[SOFTWARE] 50 --> 162[CODE 111] 50 --> 11[PERSONAL DATA] 50 --> 19[SMART CARD] 50 --> 192[PROCESSOR] 50 --> 194[SOFTWARE] 50 --> 195[CODE 111] 50 --> 193[PERSONAL DATA] 50 --> 191[SERVICE PROVIDER INFORMATION] 16 --> 14[NETWORK TRANS./RECI.] 19 --> 14 14 --> 30[WAP] 30 --> 14</pre> Fig. 1A <i>To the extent that this limitation is not fully disclosed or suggested by Hayward, this limitation would have been obvious to a person of ordinary skill in the art in combination with the</i>

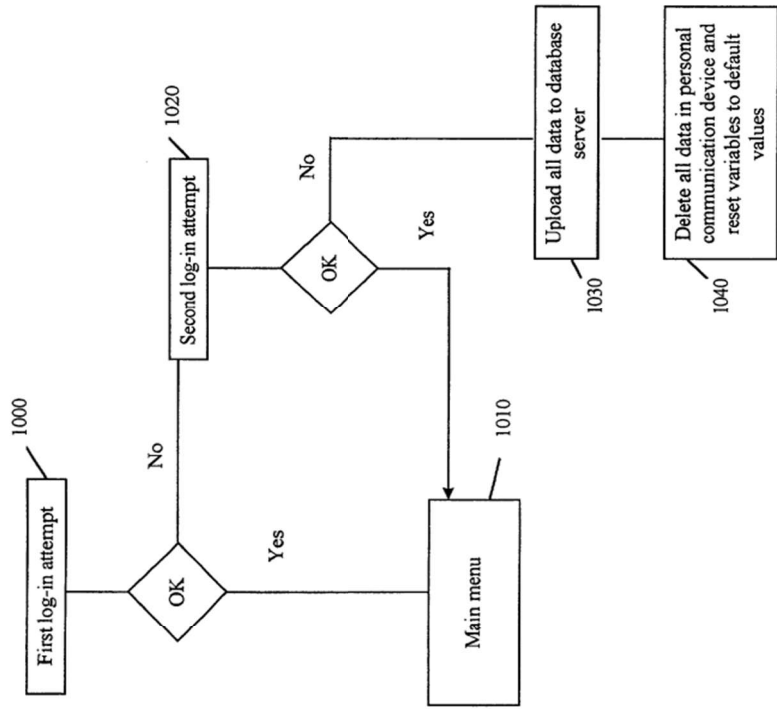
**Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants' Initial Invalidity Contentions – Exhibit F-37**

Claim Element	Evidence of Invalidity
1[e] wherein the non-volatile memory comprises a changeable area that can be modified by a user and a system area that cannot be modified by the user;	<i>general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i> <i>This limitation is disclosed or suggested by Hayward. For example:</i> “Moreover, the feature of protection of data by the use of an authentication code and protection software downloaded from a module such as a smart card, so that an element of the code is stored in the device memory and an element of the code stored on the smart card, to prevent operation of the device, or access to personal data or electronic signatures stored in the personal data device, unless the original smart card is installed, may be used without, or independently, of the feature of maintaining a copy of the personal data or electronic signature on another computer such as a PC or Internet server.” (24:12-18). <i>To the extent that this limitation is not fully disclosed or suggested by Hayward, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i>
1[f] wherein the security application utilizes code residing at least partially in the system area; and	<i>This limitation is disclosed or suggested by Hayward. For example:</i> “Moreover, the feature of protection of data by the use of an authentication code and protection software downloaded from a module such as a smart card, so that an element of the code is stored in the device memory and an element of the code stored on the smart card, to prevent operation of the device, or access to personal data or electronic signatures stored in the personal data device, unless the original smart card is installed, may be used without, or independently, of the feature of maintaining a copy of the personal data or electronic signature on another computer such as a PC or Internet server.” (24:12-18). <i>To the extent that this limitation is not fully disclosed or suggested by Hayward, this limitation would have been obvious to a person of ordinary skill in the art in combination with the</i>

Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants’ Initial Invalidation Contentions – Exhibit F-37

Claim Element	Evidence of Invalidity
1[g] wherein the security application receives the notification from at least one of the servers via the system area.	<i>general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidation Contentions.</i> <i>This limitation is disclosed or suggested by Hayward. For example:</i> “Moreover, the feature of protection of data by the use of an authentication code and protection software downloaded from a module such as a smart card, so that an element of the code is stored in the device memory and an element of the code stored on the smart card, to prevent operation of the device, or access to personal data or electronic signatures stored in the personal data device, unless the original smart card is installed, may be used without, or independently, of the feature of maintaining a copy of the personal data or electronic signature on another computer such as a PC or Internet server.” (24:12-18). <i>To the extent that this limitation is not fully disclosed or suggested by Hayward, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidation Contentions.</i>
Claim 2	
2. A mobile electronic device according to claim 1, wherein the notification includes no third-party certification.	<i>Because this claim recites a negative limitation, Hayward need not affirmatively state that the notification includes no third-party certification. Rather, Hayward discloses this limitation because its disclosures are complete and provide no indication that the disclosed “notification” (see cl. 1[c][iv] above) includes—or that there would be reason to include—a third-party certification.</i> <i>To the extent that this limitation is not fully disclosed or suggested by Hayward, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidation Contentions.</i>
Claim 7	

Claim Element	Evidence of Invalidity
7. A mobile device according to claim 1, wherein the operations the security application is operable to perform further comprise: after the at least some user data has been copied from the mobile electronic device to at least one of the servers, causing at least some of the user data to be deleted from the mobile electronic device.	<i>This limitation is disclosed or suggested by Hayward. For example:</i> “The database server also performs an important function when a personal data device is missing or replaced. Referring to Fig. 12, if a personal data device 10 is reported missing, step 110, to the database server 50, the database server seeks to contact the missing device. The device may, for example, be reported missing by contacting the database server via the Internet or telephone. The database server preferably contacts the device in a manner undetectable to a user, 30 for example, by sending a SMS message. Either when the device is next switched on or, alternatively, the personal data device may be provided with sufficient functionality even when nominally powered off to receive the SMS message and act upon it. Such functionality may be powered by a main battery of the personal data device or by an auxiliary standby battery. The standby power also powers a reset 193 for a purpose to be described. An icon may be displayed on the personal data device display when the device is powered off to indicate that the data is protected by being duplicated on the database server. On being notified that the personal data device is no longer in the possession of the authorised user, the database server compares the data stored in the personal data device with that stored for that device in the database and, if appropriate, updates the version stored in the database using the data stored in the personal data device. The database server then signals the personal data device to delete, step 111, the data and/or any electronic signatures held in the personal data device so that the data cannot be used by an unauthorised user, for example, by using the reset facility 193 to reset all variables stored in the personal data device to default values. Moreover, the database server does not authorise subsequent registration of the personal data device with the database server, except by the authorised user. Therefore, even if an unauthorised user manages to bypass the fingerprint or other authentication facility incorporated in the personal data device, the device provides only limited functionality to the unauthorised user. In addition, the data store 11 of the personal data device may be designed to be sufficiently volatile that should a thief remove the power supply to prevent a "silent call" deleting the stored data, the stored data and/or any stored electronic signatures will be automatically deleted and, for example, all variables reset to default values when the power supply is restored. The

Claim Element	Evidence of Invalidity
	database server may also contact all issuing authorities to inform them that the device is missing, so that the issuing authorities may, if desired, issue new account numbers, codes or other details for subsequent use by the authorised user on a replacement personal data device. For this purpose, the issuing authority may, after suitable authentication, download the new data into the user's data on the database server to be subsequently downloaded to the user's replacement personal data device.” (21:24-22:28). Fig. 11  <pre data-bbox="592 430 1364 1134">graph TD; 1000[First log-in attempt] --> OK1{OK}; OK1 -- Yes --> 1010[Main menu]; OK1 -- No --> 1020[Second log-in attempt]; 1020 --> OK2{OK}; OK2 -- Yes --> 1010; OK2 -- No --> 1030[Upload all data to database server]; 1030 --> 1040[Delete all data in personal communication device and reset variables to default values];</pre>

Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants’ Initial Invalidity Contentions – Exhibit F-37

Claim Element	Evidence of Invalidity
	<i>To the extent that this limitation is not fully disclosed or suggested by Hayward, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i>
9.[pre] A method for providing security for a mobile electronic device, the method comprising:	Claim 9 <i>To the extent that the preamble is limiting, it is disclosed or suggested by Hayward. For example:</i> “According to a fourth aspect of the present invention there is provided a method for storing and protecting personal data comprising the steps of: a) providing a personal data device including data storage means for storing personal data, first communication means for communicating over a communications network and a data processing and storage module for enabling operation, under control of data protection software, of the personal data device when a first element of a synchronization code stored on the module corresponds with a second element of a synchronisation authentication code stored in the personal data device storage means; b) storing personal data in the data storage means; c) providing a database server connectable to the communications network for receiving from the personal data device and storing a copy of the personal data stored in the personal data device such that the personal data in the personal data device and the database server may be mutually updated and synchronised; d) providing downloadable data protection software and a synchronization authentication code generator on the database server; e) downloading the data protection software and a synchronisation code from the database server to the personal data device and loading a first element of the synchronisation authentication code in the data storage and processing module and a second element in the data storage means of the personal data device such that operation of the personal data device is enabled; f) providing deletion means in the personal data device for deleting, under control of the data protection software, the personal data and/or electronic signatures

**Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants' Initial Invalidity Contentions – Exhibit F-37**

Claim Element	Evidence of Invalidity
	stored in the data storage means when the first element of the synchronisation code does not correspond with the second element of the synchronisation authentication code or on receipt of a deletion signal from the database server. According to a fifth aspect of the invention there is provided a computer program comprising code means for performing all the steps of the method described above when the program is run on one or more computers.” (7:11-8:8). <i>To the extent that the preamble is not fully disclosed or suggested by Hayward, the preamble would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i>
9[a] receiving, at a mobile electronic device, a request from an owner of the mobile electronic device to register the mobile electronic device with a security service residing at least partially on one or more servers;	<i>This limitation is disclosed or suggested by Hayward. For example:</i> See claim 1[c][i]. <i>To the extent that this limitation is not fully disclosed or suggested by Hayward, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i>
9[b] in response to the request from that owner, registering the mobile electronic device with the security service;	<i>This limitation is disclosed or suggested by Hayward. For example:</i> See claim 1[c][i]. <i>To the extent that this limitation is not fully disclosed or suggested by Hayward, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i>
9[c] automatically sending identifying information for the mobile	<i>This limitation is disclosed or suggested by Hayward. For example:</i>

Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants’ Initial Invalidity Contentions – Exhibit F-37

Claim Element	Evidence of Invalidity
electronic device from the mobile electronic device to the security service;	See claim 1[c][ii]. <i>To the extent that this limitation is not fully disclosed or suggested by Hayward, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i>
9[d] after the owner has registered the mobile electronic device with the security service, periodically communicating with the security service, when the mobile electronic device is in a state other than a state in which the mobile electronic device is powered off;	<i>This limitation is disclosed or suggested by Hayward. For example:</i> See claim 1[c][iii]. <i>To the extent that this limitation is not fully disclosed or suggested by Hayward, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i>
9[e] after the owner has registered the mobile electronic device with the security service, wherein the notification comprises a message indicating that the owner of the mobile electronic device has reported a loss or requested disabling of the mobile electronic device;	<i>This limitation is disclosed or suggested by Hayward. For example:</i> See claim 1[c][iv]. <i>To the extent that this limitation is not fully disclosed or suggested by Hayward, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i>
9[f] in response to accepting the notification, automatically disabling at least one user function of the mobile electronic device while still allowing the mobile electronic device to communicate with the security service; and	<i>This limitation is disclosed or suggested by Hayward. For example:</i> See claim 1[c][v]. <i>To the extent that this limitation is not fully disclosed or suggested by Hayward, this limitation would have been obvious to a person of ordinary skill in the art in combination with the</i>

Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants' Initial Invalidity Contentions – Exhibit F-37

Claim Element	Evidence of Invalidity
9[g] automatically causing at least some user data to be copied from the mobile electronic device to at least one of the servers;	<i>general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i> <i>This limitation is disclosed or suggested by Hayward. For example:</i> <i>See claim 1[c][vi].</i> <i>To the extent that this limitation is not fully disclosed or suggested by Hayward, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i>
9[h] wherein the mobile electronic device comprises non-volatile memory;	<i>This limitation is disclosed or suggested by Hayward. For example:</i> <i>See claim 1[d].</i> <i>To the extent that this limitation is not fully disclosed or suggested by Hayward, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i>
9[i] wherein the non-volatile memory comprises a changeable area that can be modified by a user and system area that cannot be modified by the user;	<i>This limitation is disclosed or suggested by Hayward. For example:</i> <i>See claim 1[e].</i> <i>To the extent that this limitation is not fully disclosed or suggested by Hayward, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i>

**Softex LLC v. Defendants, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants' Initial Invalidation Contentions – Exhibit F-37**

Claim Element	Evidence of Invalidity
9[j] wherein the security application utilizes code residing at least partially in the system area; and	<i>This limitation is disclosed or suggested by Hayward. For example:</i> See claim 1[f]. <i>To the extent that this limitation is not fully disclosed or suggested by Hayward, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidation Contentions.</i>
9[k] wherein the operation of accepting the notification from the security service comprises receiving the notification from at least one of the servers via the system area.	<i>This limitation is disclosed or suggested by Hayward. For example:</i> See claim 1[g]. <i>To the extent that this limitation is not fully disclosed or suggested by Hayward, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidation Contentions.</i>
Claim 10	
10. A mobile electronic device according to claim 9, wherein the notification includes no third-party certification.	<i>This limitation is disclosed or suggested by Hayward. For example:</i> See claim 2. <i>To the extent that this limitation is not fully disclosed or suggested by Hayward, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidation Contentions.</i>
Claim 15	
15. A mobile device according to claim 9, wherein the operations the security application is operable to	<i>This limitation is disclosed or suggested by Hayward. For example:</i> See claim 7.

***Softex LLC v. Defendants*, 1:22-cv-01308, 1:22-cv-01309, 1:22-cv-01311 (W.D. Tex.)
Defendants’ Initial Invalidity Contentions – Exhibit F-37**

Claim Element	Evidence of Invalidity
perform further comprise: after the at least some user data has been copied from the mobile electronic device to at least one of the servers, causing at least some of the user data to be deleted from the mobile electronic device.	<i>To the extent that this limitation is not fully disclosed or suggested by Hayward, this limitation would have been obvious to a person of ordinary skill in the art in combination with the general knowledge in the field, common sense, and/or with any of the references identified in the Initial Invalidity Contentions.</i>