15866
071106
U.S. PTO

PTO/SB/05 (09-04)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office. U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.	SOFP:115US
First Inventor	Apurva M. Bhansali
Title	Electronic Device Security ...
Express Mail Label No.	EQ112282385US

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

1. [✓] **Fee Transmittal Form** (e.g., PTO/SB/17)
   (Submit an original and a duplicate for fee processing)
2. [✓] **Applicant claims small entity status.** See 37 CFR 1.27.
3. [✓] **Specification** [*Total Pages* 66]
   Both the claims and abstract must start on a new page
   (For information on the preferred arrangement, see MPEP 608.01(a))
4. [✓] **Drawing(s)** (*35 U.S.C. 113*) [*Total Sheets* 79]
5. **Oath or Declaration** [*Total Sheets* 6]
   a. [ ] Newly executed (original or copy)
   b. [✓] A copy from a prior application (37 CFR 1.63(d))
   (for continuation/divisional with Box 18 completed)
   i. [ ] DELETION OF INVENTOR(S)
   Signed statement attached deleting inventor(s) name in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).
6. [ ] **Application Data Sheet.** See 37 CFR 1.76
7. [ ] **CD-ROM or CD-R** in duplicate, large table or Computer Program *(Appendix)*
   [ ] Landscape Table on CD
8. **Nucleotide and/or Amino Acid Sequence Submission**
   (if applicable, items a. – c. are required)
   a. [ ] Computer Readable Form (CRF)
   b. Specification Sequence Listing on:
      i. [ ] CD-ROM or CD-R (2 copies); or
      ii. [ ] Paper
   c. [ ] Statements verifying identity of above copies

ADDRESS TO: **Commissioner for Patents**
P.O. Box 1450
Alexandria VA 22313-1450

ACCOMPANYING APPLICATION PARTS

9. [ ] **Assignment Papers** (cover sheet & document(s))
   Name of Assignee _____
10. [ ] **37 CFR 3.73(b) Statement** *(when there is an assignee)* [✓] **Power of Attorney**
11. [ ] **English Translation Document** *(if applicable)*
12. [✓] **Information Disclosure Statement** (PTO/SB/08 or PTO-1449)
    [ ] Copies of citations attached
13. [ ] **Preliminary Amendment**
14. [✓] **Return Receipt Postcard** (MPEP 503)
    (Should be specifically itemized)
15. [ ] **Certified Copy of Priority Document(s)**
    (if foreign priority is claimed)
16. [ ] **Nonpublication Request** under 35 U.S.C. 122(b)(2)(B)(i). Applicant must attach form PTO/SB/35 or equivalent.
17. [ ] Other: _____

113007 U.S.PTO
11/484100
071106

18. If a CONTINUING APPLICATION, *check appropriate box, and supply the requisite information below and in the first sentence of the specification following the title, or in an Application Data Sheet under 37 CFR 1.76:*

[ ] Continuation [✓] Divisional [ ] Continuation-in-part (CIP) of prior application No.: 10/925,161

Prior application information: *Examiner* Tolentino, Roderick *Art Unit:* 2134

19. CORRESPONDENCE ADDRESS

[ ] The address associated with Customer Number: [ ] ***OR*** [ ] Correspondence address below

Name	Apurva M. Bhansali				
Address	Softex, Inc. 9300 Jollyville Rd., Suite 201				
City	Austin	State	TX	Zip Code	78759
Country	U.S.A.	Telephone	(281) 207-5327	Fax	(281) 207-5327

Signature	Indranil Chowdhury	Date	July 11, 2006
Name (Print/Type)	Indranil Chowdhury	Registration No. (Attorney/Agent)	47,490

This collection of information is required by 37 CFR 1.53(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

071106 15866 U.S.PTO

PTO/SB/17 (01-06)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995 no persons are required to respond to a collection of information unless it displays a valid OMB control number

Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).

FEE TRANSMITTAL
For FY 2006

☑ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 1925

Complete if Known	
Application Number	TBA
Filing Date	July 11, 2006
First Named Inventor	Apurva M. Bhansali
Examiner Name	TBA
Art Unit	TBA
Attorney Docket No.	SOFP:115US

METHOD OF PAYMENT (check all that apply)

☐ Check ☑ Credit Card ☐ Money Order ☐ None ☐ Other (please identify): _____

☑ Deposit Account Deposit Account Number: 503361 Deposit Account Name: Indranil Chowdhury, P.C.

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☐ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, except for the filing fee

☑ Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17 ☑ Credit any overpayments

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION (All the fees below are due upon filing or may be subject to a surcharge.)

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

	FILING FEES		SEARCH FEES		EXAMINATION FEES		
		Small Entity		Small Entity		Small Entity	
Application Type	Fee ($)	Fee ($)	Fee ($)	Fee ($)	Fee ($)	Fee ($)	Fees Paid ($)
Utility	300	150	500	250	200	100	500
Design	200	100	100	50	130	65	
Plant	200	100	300	150	160	80	
Reissue	300	150	500	250	600	300	
Provisional	200	100	0	0	0	0	

2. EXCESS CLAIM FEES

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20 (including Reissues)	50	25
Each independent claim over 3 (including Reissues)	200	100
Multiple dependent claims	360	180

Total Claims	Extra Claims	Fee ($)	Fee Paid ($)
52 - 20 or HP =	32	x 25	= 800

HP = highest number of total claims paid for, if greater than 20.

Indep. Claims	Extra Claims	Fee ($)	Fee Paid ($)
8 - 3 or HP =	5	x 100	= 500

HP = highest number of independent claims paid for, if greater than 3.

Multiple Dependent Claims	
Fee ($)	Fee Paid ($)

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets	Extra Sheets	Number of each additional 50 or fraction thereof	Fee ($)	Fee Paid ($)
145 - 100 =	45	/ 50 = 1 (round up to a whole number) x	125	= 125

4. OTHER FEE(S)

	Fees Paid ($)
Non-English Specification, $130 fee (no small entity discount)	
Other (e.g., late filing surcharge):	

SUBMITTED BY

Signature	Indranil Chowdhury	Registration No. (Attorney/Agent) 47,490	Telephone (281) 207-5327
Name (Print/Type)	Indranil Chowdhury		Date July 11, 2006

This collection of information is required by 37 CFR 1.136. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

(OUR REF: SOFP:115US)

APPLICATION

FOR

UNITED STATES LETTERS PATENT

TITLE: ELECTRONIC DEVICE SECURITY AND TRACKING SYSTEM AND METHOD

APPLICANTS: Apurva M. Bhansali, Manoj K. Jain, Gayathri Rangarajan, Mehul R. Patel, Rayesh K. Raikar, Ranjit Kapila, Kamal M. Dhanani, Shradha Dube, Elza A. Varghese, and Thomas D. Tucker

Express Mail No.: EQ112282385US
Date: July 11, 2006

ELECTRONIC DEVICE SECURITY AND TRACKING SYSTEM AND METHOD

CROSS REFERENCE TO RELATED APPLICATION

[0001] This application is a divisional of U.S. Application No. 10/925,161, filed on August 23, 2004, incorporated herein by reference, which in turn claims priority under 35 USC §119(e)(1) to Provisional Application No. 60/497,182, filed August 23, 2003, incorporated herein by reference.

BACKGROUND

[0002] Theft of electronic devices containing costly hardware and software has become increasingly common. Such thefts may occur because of the value of the electronic device hardware or for access to information contained on the electronic device's storage accessories such as credit card information, confidential and proprietary business information, and so on. Another use of the stolen device may be to gain access to servers containing confidential information through the electronic device.

[0003] Physical attachment of the electronic device to the user or an immovable object is one way of preventing theft. Password protection schemes may also be used to discourage theft or at least stop the thief from accessing the information stored on the electronic device. Motion sensors or alarms placed on the electronic device may be another impediment to the would be thief. However, such techniques do not always prevent theft, are costly and once the electronic device is stolen, do not allow tracking or recovery.

SUMMARY

[0004] The problems noted above are solved in large part by the electronic device security and tracking system and method (ESTSM) that includes a plurality of hardware, software and firmware components that cooperate to allow tracking, disabling, and other interaction with the stolen electronic device. The ESTSM electronic device (hereinafter "electronic device") and the ESTSM server computer system communicate over a communication channel to determine if the user has registered for ESTSM services. The

user may be an individual consumer user or a corporate/government user. The corporate/government user's electronic device may be part of a corporation's or government organization's customized ESTSM system. If the electronic device is not registered for ESTSM services, then upon first time power-on and connection to the ESTSM server of the electronic device that includes ESTSM software and firmware, the user is prompted to register for different ESTSM services. Alternatively, ESTSM may remain disabled and the user may register using techniques that include but are not limited to selecting a menu option for registration or selecting an icon on the electronic device's desktop, or via World Wide Web pages from a remote system other than the ESTSM device itself. The electronic device may be a laptop computer, desktop computer, wearable computer, server computer system, personal digital assistant (PDA), cellular telephone, WLAN capable computer, Smart Phone, tablet personal computer, palm top device and so forth. Each of the services may consist of different monthly, yearly or multi-year service fees or a one time fee for the life of the electronic device. After registration is complete, the ESTSM server computer system communicates over the Internet or another communication protocol such as Short Messaging Service (SMS) with the user to determine if an electronic device has been reported stolen. In accordance with some embodiments of the invention, if the device is reported stolen, the ESTSM server may inform the ESTSM device via a secure communications channel to take the appropriate action based on the service options selected by the user (e.g. disabling the electronic device, destroying the storage device (e.g. hard disk drive (HDD)) data, recovering data, encrypting data and more). In some other embodiments of the invention, an automated voice prompting system at a call center or live call center operator after authentication of the user may communicate with the user to perform ESTSM activities. All ESTSM activities performed through the Internet may also be performed by the call center including registration, reporting a system stolen, reporting system has been recovered and so forth.

[0005] The ESTSM system may include an electronic device with three components and a server computer system. The three components may be an application component, a non-viewable component and a Basic Input/Output System (BIOS)

DELL EXHIBIT 1002
Page 5 of 659

component. In some embodiments of the invention, the application component includes ESTSM application software that executes under any Windows® operating system (OS). In other embodiments of the invention, the application component software may execute under the Disk Operating System (DOS), Linux operating system, Windows® CE (and its derivatives such as Windows® Mobile, SmartPhone, Pocket PC, and so on), Symbian and Palm operating system and others. In some embodiments of the invention, the application component is responsible for communicating over the Internet with the ESTSM server computer system to determine if the electronic device has been reported stolen. If the device has been reported stolen, the application component along with the ESTSM server computer system will determine what services the user has registered for and will take the appropriate action (e.g. disable the device, communicate identifying information to the server, erase the storage device, recover data, encrypt data, etc).

[0006] In some embodiments of the invention, the communication medium may be a messaging protocol such as Short Messaging Service (SMS) used in mobile devices such as cell phones and computers using Wireless Local Area Networks (WLAN) services from wireless service providers such as Verizon Wireless®. In such systems, the server computer system would inform the application component that the device had been reported stolen without the application component querying the server system to determine if the electronic device has been reported stolen.

[0007] In some embodiments of the invention, the non-viewable component may reside in a hidden partition on the hard disk drive HDD. Alternatively, in some other embodiments of the invention, the non-viewable component may reside in the Host Protected Area (HPA) of the HDD that is not accessible by the operating system of the electronic device. The non-viewable component may include a VALIDATOR program that inspects an ESTSM Communications Area (ECA) to determine if the ESTSM application components have run correctly during the last system boot. The non-viewable component may also contain a copy of the original application component software fileset if the files need to be re-installed to the HDD.

[0008] ESTSM also consists of a BIOS component that maintains the secured environment of the ESTSM application component. The BIOS component includes a

DELL EXHIBIT 1002
Page 6 of 659

secure nonvolatile area that stores critical information present after electronic device power-off and accessible during electronic device power-on and boot. If only the application component was provided, a simple low level format of the hard disk drive would remove the application and bypass all the security features. ESTSM implements an "application, BIOS and non-viewable component" based solution to electronic device security. The ESTSM BIOS components ensure that a thief cannot bypass or circumvent the ESTSM application from running.

[0009] On every boot, the BIOS component will check and ensure that the ESTSM application components have not been deleted or tampered with. If the BIOS component detects a problem with any of the application components, it will restore the components from a special hidden partition on the hard disk drive or from system recovery media. In some embodiments of the invention, the recovery media may be a floppy diskette but in other embodiments the recovery media may be a Compact Disc-Read Only Memory (CD-ROM), Universal Serial Bus (USB) key storage device, or other storage device accessible during device boot.

[0010] In other embodiments of the invention as mentioned above, the electronic device in the ESTSM may include a HDD that contains a HPA. The HPA is not accessible by the operating system of the electronic device or by the user of the electronic device. An ESTSM application component including ESTSM application software may be present on the HDD. The HPA may include an ESTSM non-viewable component. The ESTSM electronic device may also include an ESTSM BIOS component that is capable of communicating with the non-viewable component and application component. An ESTSM server computer system communicates with the other components through an ESTSM Communications Area (ECA) located on the HDD.

[0011] In some embodiments of the invention, the ESTSM system may include an electronic device with a BIOS component, an application component and a server computer system. On every boot, the BIOS component will check and ensure that the ESTSM application components have not been deleted or tampered with. If the BIOS component detects a problem with any of the application components, it will assume that the ESTSM application components will be installed by the user of the electronic device.

DELL EXHIBIT 1002
Page 7 of 659

If the application component is not installed after a number of unsuccessful attempts, the BIOS component will prevent the user from accessing the electronic device. The application component may be installed by downloading from the ESTSM website or from recovery media that came with the device.

[0012] In some other embodiments of the invention, the electronic device in the ESTSM includes a Flash memory and may be a PDA, mobile cellular telephone or WLAN capable computer. The Flash memory may contain a changeable area and a system area. The system area is not changeable by the user of the electronic device. The ESTSM application software may reside in the changeable area or the system area depending on the security requirements of the device implementation. An ESTSM server computer system communicates to the ESTSM application software on the electronic device through communication channels that may be the Internet, a wireless medium (such as SMS), a combination of the two, and so on. The PDA, mobile cellular telephone or WLAN capable computer may be continuously connected to the ESTSM server computer system through an always-on Internet connection or other mobile device communication protocols such as Short Messaging Service (SMS).

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] Figure 1 shows a screen shot of the registration reminder for the ESTSM;

Figures 2a-2b show screen shots of the service offerings and selection page for the ESTSM;

Figures 3a-3c shows screen shots of the user registration and information input pages for the ESTSM;

Figure 4 shows a screen shot of a new user registration email sent to a user after they have registered their electronic device with ESTSM;

Figure 5 shows a screen shot of the login page for connecting to ESTSM server computer system in accordance with one embodiment of the invention;

Figure 6 shows a screen shot of the device registry web page that resides in the ESTSM server computer system in accordance with one embodiment of the invention;

DELL EXHIBIT 1002
Page 8 of 659

Figure 7 shows a screen shot of the electronic device status web page that resides in the ESTSM server computer system in accordance with one embodiment of the invention;

Figures 8a-8b show screen shots of web pages that allow a user to report a stolen electronic device in accordance with one embodiment of the invention;

Figure 9 shows a screen shot of an email containing location identification information for a stolen electronic device in accordance with one embodiment of the invention;

Figure 10 shows a screen shot from another computer system that can display web pages of a registration web page for ESTSM on a PDA;

Figure 11 shows a screen shot of the service offerings for an ESTSM enabled PDA using another computer system capable of displaying web pages;

Figure 12 shows a screen shot for registration of a PDA with ESTSM in accordance with one embodiment of the invention that requests the user enter the registration key on their PDA;

Figure 13 shows for one embodiment of the invention a screen shot from a Pocket PC requesting the user enter the registration key shown in Figure 12;

Figure 14 shows a screen shot from a Pocket PC displaying a confirmation key generated after the user enters the registration key;

Figure 15 shows a screen shot from a computer system capable of displaying web pages of Pocket PC verification requesting the user enter the confirmation key from the Pocket PC display;

Figure 16 shows a screen shot from a computer system capable of displaying web pages of a successful registration message for a PDA;

Figure 17 shows a screen shot from a computer system capable of displaying web pages indicating that the PDA is currently secured;

Figure 18 shows a screen shot of the user authentication screen in accordance with one embodiment of the ESTSM invention that may be used by a call center operator to verify the identity of a user;

DELL EXHIBIT 1002
Page 9 of 659

Figure 19 shows a screen shot of the welcome page for corporate administration of ESTSM;

Figure 20 shows a screen shot of corporate information input and modification by the administrator;

Figure 21 shows a screen shot of a web page that allows a corporate administrator to register a user for ESTSM;

Figure 22 shows a screen shot of a web page that allows a corporate administrator to remove a user's access to ESTSM;

Figure 23 shows a screen shot of a web page that allows a corporate administrator to purchase licenses for services in ESTSM;

Figure 24 shows a screen shot of a web page that allows a corporate administrator to purchase licenses to upgrade or modify services in ESTSM;

Figure 25 shows a screen shot of a web page that allows a corporate administrator to give permission to users to report their computer stolen in accordance with one embodiment of the invention;

Figure 26 shows a screen shot of a web page showing menu options selectable by a corporate administrator for administration of ESTSM;

Figure 27 shows a screen shot of a web page that allows a corporate administrator to create a corporate ESTSM account and register a super-user;

Figures 28a-28b show screen shots of a web page requesting a corporate administrator to enter a purchase order quotation number for basic or upgraded ESTSM services;

Figure 29 shows a screen shot of a web page that allows a corporate administrator to send an email to a user indicating activation of ESTSM;

Figure 30 shows a screen shot of a web page that allows a corporate administrator to reset a login and password for a user;

Figure 31 shows a screen shot of a web page that allows a corporate administrator to override ESTSM on an electronic device using a generated password;

Figure 32 shows a screen shot of a web page that allows a corporate administrator to stop a machine or user from accessing ESTSM services;

DELL EXHIBIT 1002
Page 10 of 659

Figure 33 shows a screen shot of a web page that allows a corporate administrator to view the status of an electronic device using the machine id or a user login assigned to the device;

Figure 34 shows a screen shot of a web page that allows a corporate administrator to recover an electronic device that has been reported stolen using a generated password;

Figure 35 shows a screen shot of a web page that allows a corporate administrator to change the settings of the ESTSM server;

Figures 36a-36b show screen shots of web pages that allow a corporate administrator to change administrator login and master passwords;

Figure 37 shows the state transitions of an electronic device from a not registered state to registered and active state;

Figure 38 shows the state transitions of an electronic device from a not registered state to registered and active state with the device passing through a never remind state;

Figure 39 shows the state transitions of an electronic device from a registered and active state to deregistered state;

Figure 40 shows the state transitions of an electronic device with ESTSM that is reported stolen and then recovered;

Figure 41 shows the state transitions of an electronic device from a registered and active state to override state;

Figure 42 shows the states of an electronic device registered and active with ESTSM and including the data destroy service;

Figure 43 shows the states of an electronic device registered and active with corporate ESTSM in which the corporate user of the device is removed from ESTSM;

Figure 44 shows the architecture of ESTSM including an electronic device and server computer system in accordance with one embodiment of the invention;

DELL EXHIBIT 1002
Page 11 of 659

Figure 45 shows the architecture of ESTSM in accordance with some other embodiments of the invention for PDA or mobile phone connected to server computer system;

Figure 46 shows another embodiment of the ESTSM architecture including an electronic device and server computer system;

Figure 47 shows another embodiment of the ESTSM architecture including an electronic device with a WWW component and server computer system;

Figure 48 shows the architecture of ESTSM in accordance with another embodiment of the invention for an electronic device with Short Messaging Service (SMS) connected to server computer system;

Figure 49 shows a schematic of a computer system that includes a BIOS component, application component and non-viewable component in accordance with one embodiment of the invention;

Figure 50 shows a schematic of a cellular telephone that includes an application component in a system area in accordance with another embodiment of the invention;

Figure 51 shows a schematic of the ESTSM server computer system of Figures 44-47 in more detail in accordance with one embodiment of the invention;

Figure 52 shows the connections between the primary and secondary servers contained in the web server of Figure 51 in accordance with one embodiment of the invention;

Figure 53 is a flow diagram of the BIOS component of the ESTSM in accordance with some embodiments of the invention;

Figure 54 is a flow diagram of the VALIDATOR program in the non-viewable component of the ESTSM in accordance with some embodiments of the invention;

Figure 55 is a flow diagram of the application component of the ESTSM in accordance with some embodiments of the invention;

DELL EXHIBIT 1002
Page 12 of 659

Figure 56 shows encrypted and encoded communication between a client electronic device and the ESTSM server computer system in accordance with one embodiment of the invention;

Figure 57 shows encryption and encoding of information by the client electronic device and decoding and decryption of information by the server computer system;

Figure 58 is a flow diagram implemented in the client and server for encoding binary data into text format data in accordance with one embodiment of the invention;

Figure 59 is a flow diagram implemented in the client and server for decoding text format data into binary data in accordance with one embodiment;

Figure 60 is a flow diagram showing encryption and encoding of SMS messages from SMS server to SMS enabled ESTSM electronic device in accordance with one embodiment of the invention;

Figure 61 is a flow diagram showing decoding and decryption of SMS messages in accordance with some embodiments of the invention;

Figure 62a is a flow diagram showing integration of ESTSM BIOS image files into system BIOS of the electronic device in accordance with one embodiment of the invention;

Figure 62b is a flow diagram showing integration of the ESTSM option ROM into a BIOS binary image;

Figure 63 shows in accordance with another embodiment of the invention integration of ESTSM BIOS image files into electronic device system BIOS using BIOS editor;

Figure 64 shows in accordance with another embodiment of the invention integration of ESTSM BIOS image files into electronic device system BIOS using BIOS Configuration utility;

Figure 65 show screen shots of the service offerings for the ESTSM mobile device;

DELL EXHIBIT 1002
Page 13 of 659

Figure 66 shows screen shots of the user registration and information input pages for the ESTSM mobile device such as a Smart Phone;

Figure 67 shows a screen shot from a computer system capable of displaying web pages of a successful registration message for a mobile device;

Figure 68 shows a screen shot of the mobile device status web page that resides in the ESTSM server computer system in accordance with some embodiments of the invention;

Figure 69 shows a screen shot of the backup files web page for a mobile device that resides in the ESTSM server computer system in accordance with some embodiments of the invention;

Figure 70 shows a screen shot from a mobile device indicating that the device has been disabled;

Figure 71 is a flow diagram showing implementation of ESTSM on mobile devices; and

Figure 72 shows the state transitions of a mobile device with SMS messages for activation and operation of ESTSM services.

DETAILED DESCRIPTION

[0014] The ESTSM consumer user (i.e. non-corporate user) experience consists of two phases: (1) the registration phase and (2) administration phase via the ESTSM website. In the registration phase, the user creates an account with ESTSM, specifies what ESTSM services he wishes to purchase, and provides user and billing information to complete the registration.

[0015] Once registration is complete, the typical user will not interact with ESTSM until the electronic device is stolen. At that time, the user can log into the ESTSM website. Once logged in, the user can report the device as stolen, disable the device, or perform other device administration tasks. The user may also initiate all ESTSM device administration tasks through a call center that can validate the identity of the user and perform administrative tasks on the user's behalf.

DELL EXHIBIT 1002
Page 14 of 659

[0016] After registration is complete, the ESTSM server computer system communicates over the Internet with the user to determine if the electronic device has been reported stolen. In accordance with some embodiments of the invention, if the device is reported stolen, the ESTSM server will instruct the electronic device to take the appropriate action based on the service options selected by the user (e.g. disabling the electronic device, destroying the hard disk drive (HDD) data, recovering data, encrypting data and more).

[0017] When the user purchases the electronic device, the ESTSM components may be pre-installed by the manufacturer of the electronic device. In some embodiments of the invention, the ESTSM registration screen shown in Figure 1 will come up when the user starts using his electronic device and the ESTSM system determines that the electronic device is not registered. The ESTSM system determines if the electronic device is registered or not by communicating with the ESTSM server computer system.

[0018] In another embodiment of the invention, the user may request the manufacturer of the device to preregister the user for ESTSM services after the manufacturer builds the electronic device. In some alternative embodiments of the invention, the device may be preregistered for ESTSM services at the location (e.g. retail store) where the device is purchased. In one embodiment of the invention, the initial fees for the ESTSM services as described below may be included by the manufacturer in the price of the electronic device or may be discounted as a sales promotion for the device.

[0019] In some other embodiments of the invention, the ESTSM system may be provided to the manufacturer of the electronic device without charge or for a very small fee. The user of the device may select the ESTSM services they want and the revenue generated may be shared by the manufacturer and ESTSM administrator. Thus, the user may "opt-in" to purchase the ESTSM services. In some embodiments of the invention, the ESTSM services may be offered to the user of the electronic device on a trial basis for a limited time.

[0020] The user can proceed with the registration process at this point, or choose to register at a later time or never. If the user chooses to register at a later time, the ESTSM will remain disabled and the user may register using techniques that include but

are not limited to selecting a menu option for registration or selecting an icon on the electronic device's desktop. If the user proceeds with the registration process, the user will be asked to specify if they are a "new user" or an "existing user" that has other electronic devices running ESTSM. The next stage as shown in Figures 2a-2b is to choose the ESTSM services for the electronic device.

[0021] Figures 2a-2b shows the service selection screen that may include the cost of each service and the number of services offered. The services offered and the cost of each service may vary based on the manufacturer and model of the electronic device, the market segment of the electronic device (i.e. business device, home use device) and what the manufacturer has chosen to include for the device. Some manufacturers may want to change the pricing of the services, or offer bundled services to the user. For one embodiment of the invention, as shown below, is a list of the typical services available to the user and the associated costs.

1. Basic Service – with this service the user has the ability to have the electronic device disabled when it is stolen. However, the location of the stolen electronic device is not tracked and no other operation is performed.
2. Tracking Service – with this service, the location of the stolen electronic device will be tracked and the location report information is sent to the user of the electronic device via email (or the user can call a monitoring station to get the information). There are two sub-options under the tracking service: Track-and-Disable or Continuous Track. In the Track-and-Disable option, the location of the electronic device is captured one time and then the electronic device is disabled. In the Continuous Track option, the location of the electronic device is constantly tracked until the user manually disables the electronic device from the ESTSM website. Electronic devices such as cell phones because they are mobile and cannot be easily tracked may not offer this service.
3. Data Destroy Service – with this service, the hard disk of the stolen electronic device is erased when the thief connects the electronic device to the Internet. This service has two sub-options: (1) Automatically Erase when the electronic

DELL EXHIBIT 1002
Page 16 of 659

device is connected to the Internet, or (2) Manual Erase, the user must manually specify when to erase the hard disk drive via the ESTSM website.

4. Third Party Insurance Signup – with this service, ESTSM will re-direct the user to the website of third party companies that will assist the user in signing up for theft and damage replacement insurance for their electronic device.

[0022] In some embodiments of the invention, due to the extendible design of ESTSM, new services can be added into the ESTSM registration process as given below:

1. Data Encryption Service – with this service, a virtual file folder called "My Encrypted Documents" is created on the desktop of the electronic device. In some embodiments of the invention, all files saved in this folder are encrypted by encryption techniques built into the operating system. Access to the folder is denied unless the system is connected to the Internet and the electronic device has not been reported stolen. If the system is not connected to the Internet, the user can optionally enter the ESTSM username and password to get access. In another embodiment of the invention, the user may designate any virtual file folder in the electronic device as an "ESTSM Encrypted Folder."
2. Data Recovery Service – this service will allow a user to specify critical files and in the case of theft, the software will first recover these files to the ESTSM server computer system, before performing other service option actions. In one embodiment of the invention, a virtual file folder called "My Critical Files" is created on the desktop of the electronic device. The user may store the actual files, copies of files, or shortcut pointers to files in this folder that they want to recover if the electronic device is stolen. In another embodiment of the invention, right clicking a mouse button with the pointer pointing to a file displays a menu allowing the user to mark the file as a "Critical File." The file's icon is modified to indicate that it will be recovered if the electronic device is stolen. This embodiment of the invention allows the file to be present anywhere on the HDD of the electronic device rather than in a specific file folder. Another embodiment of the invention may use both the virtual file folder "My Critical Files" as well as

DELL EXHIBIT 1002
Page 17 of 659

files marked as "Critical Files" to indicate files that will be recovered if the electronic device is stolen.

[0023] In the preferred embodiment of the invention, most of ESTSM services are based on a yearly fee model. Some services such as data recovery may be billed on a per megabyte basis-that is, the user indicates the number of megabytes to be recovered during registration and is billed accordingly. However, if the electronic device is stolen and during data recovery more megabytes are recovered, then a one time fee is charged to the user. The user will automatically be billed at the end of the year to renew the service for one more year. The user will be sent an email before billing to give the user a chance to cancel the service if they wish.

[0024] The next stage in the registration phase is to create the username and password as shown in Figures 3a-3b that can be used to log onto the ESTSM website to report a stolen electronic device, etc. Once that is completed, the user must provide his user information (name, address, phone number, and so forth) as shown in Figure 3c so that the monitoring station can identify the user if the user calls the monitoring station to report a theft.

[0025] The final part of the registration phase is to provide the billing information for the ESTSM services. This requires the input of a credit card number, debit card number, or checking account number. The information is then validated, the credit card or other billing means is charged and a confirmation email as shown in Figure 4 is sent to the end user, corporation or insurance company that just completed the registration. The user will have to click a link at the end of the email to activate the ESTSM on that electronic device. In some embodiments of the invention, periodic ESTSM service charges may be billed by adding these charges to the existing electronic device bill. For example, ESTSM monthly service charges may be added to the users' existing mobile phone bill for ESTSM registered mobile phones.

[0026] As mentioned above, ESTSM provides a website from which the user may administer the ESTSM services on the electronic device. In some embodiments of the invention, corporate users may have limited administrative capabilities because of their access permissions (described in more detail below). As shown in Figure 5, the user

DELL EXHIBIT 1002
Page 18 of 659

must first log into the website using the username and password that was created during the registration phase. A user without access to the Internet (i.e. his electronic device was stolen), can call the ESTSM monitoring station to perform the administrative functions described below for the electronic device.

[0027] Once the user has logged into the ESTSM website, the main ESTSM menu in accordance with one embodiment of the invention is presented as shown in the left hand portion of Figure 6. In some embodiments of the invention, corporate and noncorporate users may have different ESTSM menus.

[0028] The "Device Registry" portion of the page in Figure 6 shows all the electronic devices the user currently has registered with ESTSM. By clicking on a device image from the "Device Registry" page of the ESTSM website, the user is taken to the "Device Status" page shown in Figure 7. On the "Device Status" web page for each device, the user can perform the following tasks: (1) View the status of the user's electronic devices running ESTSM; (2) Report an electronic device stolen; (3) Recover and re-enable a stolen system that has been found; (4) Upgrade or change the ESTSM service options; (5) Show the Billing and Electronic Device Location/Status Logs; (6) Perform User Management functions such as changing the user information, password and billing information; and (7) Perform Data Management functions such as viewing recovered data and transferring recovered data to another device.

[0029] As shown in Figure 7, the "Device Status" page shows for each electronic device, the Model Name, System Description, Current State, ESTSM Services Active on the Device, and Last Connection to ESTSM Server. Depending on the Current State and the services selected by the user, certain task buttons will appear below the electronic device information. These task buttons let you perform different operations on the device (e.g. report the electronic device stolen and so forth). As shown in Figure 7, the user may click on the button labeled "Report Stolen" to start the process of reporting an electronic device stolen. The user will be taken to the "Report a Stolen Device" web pages shown in Figures 8a-8b. The user fills out the information on the web page to generate a theft incident report and the ESTSM site will log this report so that it may be given later to the

DELL EXHIBIT 1002
Page 19 of 659

appropriate authorities as proof of filing the theft incident report. This documentation may be provided to the user upon request.

[0030] Once the report is completed, the electronic device will be put in the REPORTED STOLEN state (states of ESTSM are described in detail below). At this point, if the electronic device is connected to the Internet, the electronic device state will change to either BEING TRACKED or DISABLED state.

[0031] In some other embodiments of the invention, mobile devices such as cell phones, Smart Phones, and Wireless Local Area Network (WLAN) capable computers that may be always connected to the ESTSM server and contacted at anytime by the server can communicate through a message passing scheme. Message passing schemes may be SMS, WWW message passing protocol based on Transmission Control Protocol/Internet Protocol (TCP/IP), or Multimedia Messaging Service (MMS). The state diagram for mobile devices are shown in Figure 72.

[0032] If the electronic device is in the BEING TRACKED state, the user will receive an email, an example of which is shown in Figure 9, documenting the location of the stolen electronic device. This location information may contain the following information: (1) IP address of the stolen electronic device (2) domain name on the Internet of the stolen electronic device (3) owner of the domain name (4) contact information for the domain name owner (5) name and contact information of the Internet Service Provider (ISP) and (6) date and time of IP address connection.

[0033] With this information, the user may pursue recovery with the appropriate authorities. The information provided may be used to track the exact location of the electronic device. For example, ISPs may identify the network port, cable modem or phone number from which the electronic device was connected when provided with the IP address, date and time of the connection. A location tracking report email will be sent to the user each time the electronic device is connected to the Internet. If the "Track and Disable" service option is selected, by the user, then only one tracking location will be recorded since the electronic device will be automatically disabled once the location is recorded.

DELL EXHIBIT 1002
Page 20 of 659

[0034] In another embodiment of the invention, ESTSM registration as shown in Figure 10 for a PDA, mobile cellular telephone, or Smart Phone device may be performed using another computer system that can display ESTSM registration web pages. In some embodiments of the invention, a different set of ESTSM services as shown in Figure 11 may be offered for the PDA. Thus, the manufacturer may offer, but not limited to, a Basic service and a Data backup service for the device as shown in Figure 11.

[0035] After the user has selected the ESTSM services for their PDA, in some embodiments of the invention, the ESTSM system as shown in Figure 12 may request that the user interact with the ESTSM application on the PDA and enter the registration key into the device as shown in Figure 13. Entering the registration key into the device may be the first step to start a multi-step registration process that ensures that the correct electronic device is being registered. The PDA will then display a confirmation key as shown in Figure 14. The user through the computer system capable of displaying ESTSM web pages may then enter into the PDA verification screen shown in Figure 15 the confirmation key and a system description. The registration process for the PDA is successfully completed as shown in Figure 16 and the device is secured as shown in Figure 17. In some other embodiments of the invention, ESTSM registration may not require any user intervention with the ESTSM electronic device except an acknowledgement from the user at the end of the successful registration.

[0036] In another embodiment of the invention, an automated voice prompting system at a call center or live call center operator after authentication of the user as shown in Figure 18 may communicate with the user to perform ESTSM activities. All ESTSM activities performed through the Internet may also be performed by the call center including registration, reporting a system stolen, reporting system has been recovered and so forth.

[0037] In most business or government organizations, a central IT staff is responsible for configuring, maintaining and purchasing licenses for electronic devices. ESTSM is designed to work easily in controlled corporate or government environments. Electronic devices registered to corporations or government entities using

DELL EXHIBIT 1002
Page 21 of 659

corporate/government registration may contain a different set of administration pages and user pages as compared to non-corporate users. In one embodiment of the invention, the corporate web pages may be as shown in Figures 19-25. Web pages for government entities would be similar to the corporate web pages shown in Figures 19-25. Corporate ESTSM systems may be designed to be centrally maintained and administered as required by corporate customers. When a corporate account is created, a central administrator or manager is specified. The central manager can then create other managers and users and purchase and assign licenses to these managers and users as shown in Figures 21 and 23-24. As shown in Figure 21, the central manager can assign user permissions to other managers. Thus, the corporation can control which users are allowed to report stolen electronic devices as shown in Figure 25, remove users as shown in Figure 22, purchase more licenses, upgrade services, etc.

[0038] For electronic devices registered to corporations or government entities, the ESTSM may contain the user's position within the company and associate user permissions with that position as shown in Figure 21. Thus, if a user leaves the company, the electronic device may be assigned to another employee transparently and without any change in service fees. The ex-employees account information on ESTSM may be disabled and removed as shown in Figure 22, so that the ex-employee may not falsely report an electronic device stolen to disable access to the device.

[0039] Another embodiment of the registration and administration technique for electronic devices in ESTSM for corporations is shown in Figures 26-36b. A corporate administrator may access the ESTSM server computer system located in the monitoring station by calling the monitoring station or through the Internet. In another embodiment of the invention, the corporation or government entity may have the ESTSM server computer system located within their own premises for greater security and control. In this embodiment of the invention, the administrator can access the server system through a terminal connected to the server or from a computer system at a remote site connected to the server system through the Internet.

[0040] The corporate or government entity can setup a corporate account to use ESTSM. The corporation or government entity can purchase services licenses in "bulk"

DELL EXHIBIT 1002
Page 22 of 659

(i.e. 100 Data Destroy Services, 50 Tracking Services, etc). The licenses can be paid for via standard purchasing methods such as Purchase Orders as shown in Figures 28a-28b, net 30 day terms, etc. The corporation or government entity receives a license number for each purchase. This license number is given to the end users in the corporate or government entity who will consume the license. Alternatively, the corporation or government entity may pay a non-recurring one time fee for individual services.

[0041] The corporate or government end user will register in a similar fashion as described above. However, in one embodiment of the invention, when creating the username and password, the user can enter the license number for the "License Number" field as shown in Figure 3a. In this embodiment of the invention, the end user will not be required to select the services as they will be determined by the services paid for in the license number. Also, the end user will not have to provide a credit card or other form of payment.

[0042] The administrator of the corporate or governmental ESTSM account can manage and configure the electronic devices in the corporation or government entity that have the ESTSM application installed. Thus, for example, the administrator may re-send an activation email to a user of an ESTSM enabled electronic device as shown in Figure 29 or send a login and password reminder to the user as shown in Figure 30. The administrator may override an individual user's access to an electronic device as shown in Figure 31, deregister an electronic device from the ESTSM system, or remove user access to ESTSM enabled electronic devices as shown in Figure 32. The current state of the electronic device (ACTIVE, REPORTED STOLEN, BEING TRACKED, DISABLED, HALF-RECOVERED, and so on as described in detail below) registered with ESTSM may be viewed by the corporate or government administrator by entering the machine id, the login id of the user, mobile phone number, or any other ESTSM device specific identification as shown in Figure 33. The administrator can also perform other administrative tasks such as recover an ESTSM enabled system as shown in Figure 34, change server settings as shown in Figure 35, or change the administrator login password or administrator master password as shown in Figures 36a-36b.

DELL EXHIBIT 1002
Page 23 of 659

[0043] The administrator may add new users to the ESTSM system and designate the rights and permissions of users so that these users have administrator capabilities. Users on a corporate or governmental ESTSM account may heave permission to report their ESTSM device stolen, perform user management functions, and so forth.

[0044] As mentioned above and shown in Figure 7, the "Device Status" page displays task buttons below the electronic device information. The task buttons displayed depend on the current state of ESTSM and the services selected by the user. The task buttons let the user perform different operations on the device (e.g. report the electronic device stolen and so forth).

[0045] Each electronic device can have one of the following current states: ACTIVE, REPORTED STOLEN, BEING TRACKED, DISABLED and HALF-RECOVERED. The definition of each of the states is given below:

1. ACTIVE – This state indicates that ESTSM is actively running on the electronic device. The electronic device has not been reported stolen.
2. REPORTED STOLEN – This state indicates that the electronic device has been reported stolen by the user, but the electronic device in some embodiments of the invention has not communicated with the ESTSM server after being reported stolen.
3. BEING TRACKED – This state indicates that the electronic device has been reported stolen by the user and the electronic device has communicated with the ESTSM server. The ESTSM server has captured location information of the stolen device. Once the system is in the BEING TRACKED state, other actions can be performed such as disabling the electronic device (if the Continuous Track option has been selected) or erasing the hard disk drive (if Manual Data Destroy Service has been selected).
4. DISABLED – The stolen electronic device has been disabled by ESTSM. The system is now in the locked state and can not be used. If the system is recovered by the user, they will need to obtain the activation password to re-enable access to the electronic device.

DELL EXHIBIT 1002
Page 24 of 659

5. HALF-RECOVERED – This state indicates that the electronic device has not been totally recovered. The user of the electronic device has reported that the device has been recovered. The user must enter the activation password on the electronic device to re-enable access.

[0046] The ESTSM system may also be in one of these other states:

1. NOT REGISTERED – The electronic device is not registered with the ESTM system. The device will be in this state if the user chooses not to register with ESTSM when prompted to do so upon first time power-on of the electronic device.
2. DE-REGISTERED – ESTSM is no longer active on this electronic device. The user may want to put the electronic device in this state in the event that the transfer of electronic device from one user to another is to take place. Once the electronic device is placed in the DE-REGISTERED state, the user must re-register the electronic device (which may involve re-paying service fees) to re-activate the electronic device.
3. USER REMOVED – For users of a corporate ESTSM system, the ESTSM corporate administrator may remove a user's access rights to the ESTSM system. This situation may occur when the user leaves the company.
4. NEVER REMIND – This state indicates that the user of the electronic device does not want to be reminded to register with the ESTSM system. This state may be entered if the user activates the "Never Remind" option in the registration process. After activating "Never Remind", the user may register with ESTSM by manually selecting "Register Now" option on the ESTSM application icon and successfully completing the registration process.
5. REGISTERED NOT ACTIVATED – In this state the user has successfully registered the electronic device through the registration process but has not clicked on the link sent with the activation email to complete the registration process.

DELL EXHIBIT 1002
Page 25 of 659

6. GOING TO DISABLE – This state indicates that the user has selected the "Disable" option after the electronic device has been reported stolen and is being tracked.
7. OVERRIDE – This state indicates that ESTSM has been disabled temporarily by the user. This may be because the application component is not able to communicate with the ESTSM server computer system. To use the electronic device while in this state, the user enters an activation password when prompted with a warning.
8. ERASE HARDDISK – This state indicates that the user selected "Data Destroy Services" option when registering with the ESTSM system. This state is entered after the user reports the electronic device as stolen and the device is connected to the Internet and tracked.
9. ACTIVATION PENDING – A message has been sent to the electronic device and the ESTSM server is waiting for an acknowledgment.
10. DISABLED DATA BACKUP – This state indicates that the electronic device is disabled after the data on the electronic device has been backed up.
11. ACTIVE DATA BACKUP – This state indicates that the device has been re-enabled after it was in the DISABLED DATA BACKUP state and a successful acknowledgment is received from the electronic device. In this state, the user may restore the data back on the electronic device from the backup on the ESTSM server.
12. BACKUP IN PROGRESS – In this state the electronic device has been disabled and the ESTSM server is in the process of getting the data from the device.
13. RESTORE IN PROGRESS – The user has requested that the data backed up on the ESTSM server be restored into the electronic device and the restore is in progress.
14. ENABLE PENDING – This state indicates that the stolen electronic device has been re-enabled and the ESTSM server has sent the message to the electronic device and is awaiting acknowledgment.

DELL EXHIBIT 1002
Page 26 of 659

15. ENABLE AFTER RECOVERY – This state indicates that the electronic device was enabled from either the BACKUP IN PROGRESS state or the DISABLED DATA BACKUP state. The electronic device is sent a message and the state is changed after receiving a confirmation.

[0047] Turning now to Figures 37-44 and Figure 72, state diagrams including the states described above and the conditions to enter and exit the states are shown. Figure 37 shows the states and transitions of an electronic device in ESTSM from a not registered state to registered and active state. After the user goes through the registration process 3720, an electronic device in the not registered state 3710 transitions into the registered and not activated state 3730. Once the user clicks on an activation email 3740 on the electronic device or calls an activation telephone number, the device becomes registered and active 3750.

[0048] Referring to Figure 38, the states and transitions of an electronic device in ESTSM from a not registered state to registered and active state with the device passing through a never remind state are shown. If the user clicks the never remind option shown in Figure 1, the electronic device transitions 3820 to the never remind state 3830. Next, if the user at a later time decides to manually register (i.e. in some embodiments of the invention by clicking on an ESTSM application icon on the graphical interface of the device and going through registration process 3840), the electronic device is placed into a registered and not activated state 3850. Once the user clicks on an activation email 3860 on the electronic device or calls an activation telephone number, the device becomes registered and active 3870.

[0049] Referring to Figure 39, the states and transitions of an electronic device in ESTSM from a registered and active state to deregistered state are shown. The user may decide they no longer want ESTSM services and select the "Stop ESTSM" option 3920 shown in Figure 7. The electronic device that was previously in the registered and active state 3910 will transition to the deregistered state 3930 after selection of "Stop ESTSM."

[0050] Referring to Figure 40, the states and transitions of an electronic device in ESTSM that is reported stolen and then tracked, disabled, and recovered are shown. During registration and activation with ESTSM, the user must select the Track and

DELL EXHIBIT 1002
Page 27 of 659

Disable service option to activate the states and transitions shown in Figure 40. Once the electronic device is registered and active with ESTSM 4010 and the user reports the system stolen 4015, ESTSM will place the device into the reported stolen state 4020. When the electronic device is next connected to the Internet, ESTSM will begin tracking the device in the being tracked state 4030. The user is sent a location identification email shown in Figure 9 and because the user had selected the track and disable service is again given the option to disable 4035. If the user selects disable 4035 then the electronic device is placed into the going to disable state 4040. The Application component on the electronic device disables the device 4045 and informs the ESTSM server computer system that the electronic device is in a disabled state 4050. If the user recovers the device and performs the recovery procedure 4055, the electronic device is placed into the half recovered state 4060. Next, the Application component on the electronic device informs the ESTSM server computer system that it is operating normally 4065 and the electronic device transitions back into the registered and active state 4010.

[0051] Referring to Figure 41, the states and transitions of an electronic device in ESTSM from a registered and active state to override state are shown. As described above, to continue using the electronic device if the Application component on the electronic device is unable to communicate with the ESTSM server computer system, the user must enter an activation password 4120. ESTSM on the electronic device is then bypassed in the override state 4130. If the electronic device is not reported stolen and the ESTSM Application component re-establishes communication with the ESTSM server computer system 4140, the electronic device returns back to the registered and active state 4110.

[0052] Referring to Figure 42, the states and transitions of an electronic device in ESTSM for the "Data Destroy Service" is shown. As shown in Figure 2b, the user may select the "Data Destroy Service" that erases the electronic device hard disk drive. If the "Data Destroy Service" is selected, the electronic device registered and active 4210 with ESTSM may be reported stolen 4220 by the user. A stolen electronic device is placed into the reported stolen state 4230 and once the stolen device connects to the Internet 4240, it is placed into the being tracked state 4250. The user is sent a location

DELL EXHIBIT 1002
Page 28 of 659

identification email shown in Figure 9 and because the user had selected the data destroy service is again given the option to select or bypass data destroy. If the user selects data destroy 4260, then the Application component on the electronic device erases the hard disk drive and the electronic device is in the erase hard disk state 4270.

[0053] Referring to Figure 43, the states and transitions of an electronic device in which the corporate user of the device is removed from ESTSM is shown. As described above, a corporate user may have an electronic device which is registered and active 4310 with ESTSM. If ESTSM were not installed on the electronic device but rather the device was protected by a password known only to the user, the electronic device would be rendered unusable if the user left the organization. With ESTSM, if the corporate user leaves the organization 4320, the corporate administrator may remove the user's access rights to the ESTSM system. The electronic device used by the user is placed into the user removed state 4330.

[0054] If an electronic device is in the REPORTED STOLEN, BEING TRACKED or DISABLED state, the user can use a "System Recovered" interface that may be a button to bring the electronic device back to the ACTIVE state. The procedure after the electronic device is recovered may be different depending on the ESTSM services selected for the recovered electronic device and the current state of the electronic device. In some embodiments of the invention, the user may be required to fill out a recovery incident report, which documents the circumstances under which the electronic device was recovered.

[0055] The electronic device may be in the HALF-RECOVERED state when recovered, indicating that the electronic device is currently locked from boot access. The electronic device screen will show system information such as the manufacturer, model number and serial number of the electronic device and an unlock key. The electronic device screen will prompt the user to enter an activation password to re-enable boot access to the device. On the ESTSM website, after completing the recovery incident report, the user will be asked to enter the system information and unlock key indicated on the screen of the electronic device. The ESTSM server computer system will generate

DELL EXHIBIT 1002
Page 29 of 659

the activation password that the user can enter on the recovered electronic device to re-enable boot access.

[0056] From the ESTSM website, a user may also view the ESTSM services that are currently active on any of their electronic devices. The user may also add other ESTSM services and be billed accordingly. The user may also switch the options of certain services. For example, as shown in Figure 2a, the user may switch from "Track and Disable" option to "Continuous Track" option under the "Tracking Service."

[0057] A user may be informed by the Application component of new services that are available for ESTSM. In some embodiments, the Application component may display a pop-up information message box that explains the new services along with pricing information. The Application component may optionally allow the user to purchase the new service using an interface in the message box.

[0058] The user may also view billing information about their account. The billing information will show all charges to the user's credit card and the services which were purchased along with the date of purchase.

[0059] The ESTSM server computer system includes electronic device status logs that show all the ESTSM activity for an electronic device. The user may view the electronic device status logs. These logs may be used to see when an electronic device was reported stolen, a summary of the tracking location information collected for an electronic device, date and times of recovery or device disabling events, and any other device status information.

[0060] The ESTSM website may also be used to update user information, such as address, telephone number, email address, and so forth. Also, the user's billing information such as the credit card number and expiration date may also be updated.

[0061] The user may want to upgrade the operating system or hardware (specifically the hard disk drive) on the electronic device. As described above, the ESTSM BIOS ensures that the ESTSM application components may not be removed from the hard disk drive. Thus, if the user upgrades to a new hard disk drive, the user will be asked to insert the electronic device's recovery media. In some embodiments of the invention, the recovery media may be a floppy diskette but in other embodiments the

DELL EXHIBIT 1002
Page 30 of 659

recovery media may be a Compact Disc-Read Only Memory (CD-ROM) or Universal Serial Bus (USB) key storage device. The ESTSM BIOS will prevent the system from booting until it detects the presence of the recovery media. The ESTSM BIOS component will automatically run a special program from the recovery media and this program will re-install all the ESTSM application components and special hidden partition on the hard disk drive (described in greater detail below). In some other embodiments of the invention where a special hidden partition is not present, the user may load the ESTSM application components into the hard disk drive directly.

[0062] The user has to take no special action to upgrade the operating system on an electronic device that already has the ESTSM components properly installed and running. When the user upgrades the OS, the ESTSM application components will also be maintained as part of the OS upgrade. If the ESTSM components are removed inadvertently, the ESTSM BIOS component will automatically re-install the ESTSM application components from a special hidden partition that exists on the hard disk. This operation will be transparent to the user.

[0063] Turning now to Figure 44, in some embodiments of the invention, the ESTSM architecture consists of application components 4405, non-viewable component 4415 and a BIOS component 4410 that work together to provide a secure environment for electronic device operation. The application components may be files stored on a hard disk drive (HDD) 4400 of the electronic device and may include startup files 4420, ESTSM application 4425, and ESTSM Dynamic Link Libraries (DLL) 4430. A web browser application 4435 connected to and capable of communicating with the ESTSM DLL 4430 may be present on the HDD. The application component runs within the operating system environment and is responsible for communicating with the ESTSM server computer system 4465 through the Internet 4475. Server computer system 4465 includes a number of servers 4470a, 4470b, ... 4470n that may be web servers containing the web pages and data for ESTSM described above. The application component 4405 determines from the ESTSM server computer system 4465 if the electronic device has been reported stolen, and if so, the application component takes the appropriate action

DELL EXHIBIT 1002
Page 31 of 659

based on the services the user registered for (i.e. disable electronic device, track location, erase hard disk drive, etc).

[0064] The BIOS component 4410 ensures that the application component 4405 cannot be removed from the system or bypassed in any way. The BIOS component 4410 consists of a small piece of code that resides in the system BIOS ROM image located in a secure non-volatile area 4465. In some embodiments of the invention, a non-viewable component 4415 program VALIDATOR 4450 resides on a special hidden partition 4455 of the hard disk drive and is executed during Power-On-Self-Test (POST) of the electronic device. Every time the electronic device boots up, the BIOS component 4410 will check the integrity of the ESTSM non-viewable component 4415 and application component 4405 programs and files, and restore the original programs and files, if they have been tampered with. Furthermore, the BIOS component 4410 will ensure that the application component 4405 has run properly on the previous device boot and will take action if it is determined that an attempt to bypass the application component 4405 has occurred.

[0065] In some embodiments of the invention, the BIOS component 4410 consists of a BIOS ROM image that is integrated into the system BIOS. The non-viewable component 4415 consists of a VALIDATOR program 4450 which resides in a special hidden partition 4455 created by ESTSM. Together, the ROM image and VALIDATOR cooperate to make sure that someone cannot bypass or circumvent the ESTSM application component 4405 from running. This is done by the ESTSM BIOS in the three ways shown below. In this document, reference made to "ESTSM BIOS" may refer to the code in the BIOS ROM image or VALIDATOR or combination of both.

1. Validating the integrity of the ESTSM special hidden partition 4455 and VALIDATOR program 4450. The ESTSM hidden partition 4455 contains the VALIDATOR program 4450 and also contains a copy of the original application component fileset 4445. If the ESTSM hidden partition 4455 has been deleted from the electronic device's hard disk drive 4400 or in some other way altered, the ESTSM BIOS ROM image component will detect this and effectively force re-installation of the partition 4455 and original fileset 4445 from the recovery media

DELL EXHIBIT 1002
Page 32 of 659

4460. This prevents someone from simply low level formatting the hard disk drive, or just replacing the hard disk drive with a new blank disk to bypass ESTSM. The ESTSM VALIDATOR program 4450 can then "re-install" the ESTSM application component 4405 from the ESTSM Backup (Original) fileset 4445 on the special hidden ESTSM partition 4455 of the hard disk drive 4400.

2. Verifying that the application has been run on each boot. The ESTSM BIOS implements a messaging protocol with the ESTSM application components 4405 to ensure that the ESTSM application components 4405 are run on every boot. This messaging protocol utilizes the ESTSM Communications Area (ECA) 4440. In order to bypass ESTSM, someone may delete key ESTSM application files in an attempt to prevent the ESTSM application from running. Furthermore, the thief may develop applications that will prevent ESTSM from running on every boot even though it is correctly installed on the electronic device's hard disk drive. The ESTSM application and BIOS components work together to make sure that the ESTSM application runs on every boot. If the ESTSM application component does not run after the electronic device has booted, the ESTSM system will allow the electronic device to boot a limited number of times and attempt to run the ESTSM application component. If the ESTSM application component does not run during any of these retries, the electronic device will be prevented from booting after system POST. For devices like PDA or SmartPhones this procedure is not required since the application component is not removable or replaceable.

3. Disabling a stolen electronic device reported as stolen so it may not boot the operating system. If the ESTSM application component 4405 detects that the electronic device has been reported stolen, it will inform the BIOS of the theft and freeze the system. If the thief powers off the electronic device and attempts to boot the system again, the ESTSM BIOS will prevent the system from booting the operating system. If the electronic device is recovered and returned to the original user, the user can "unlock" the device as described above so it can boot.

[0066] In another embodiment of the invention as shown in Figure 45, the architecture for an ESTSM enabled PDA, WLAN capable computer, mobile phone that in

DELL EXHIBIT 1002
Page 33 of 659

some embodiments may be a cell phone, or SmartPhone may include a Flash memory 4500 containing a changeable area 4510 and a system area 4520. The system area 4520 may include application components 4530 containing ESTSM application programs and a secure non-volatile area 4540 coupled to the application components 4530. In one embodiment of the invention, the system area 4520 may be non-viewable and implemented in non-volatile memory. The ESTSM enabled PDA, WLAN capable computer, mobile phone, or SmartPhone may continuously communicate to an ESTSM Server Computer System 4560 through an always-on Internet connection 4550 or other mobile device communication protocols such as Short Messaging Service (SMS). Server computer system 4560 includes a number of servers 4570a, 4570b, ... 4570n that may be web servers containing the web pages and data for ESTSM described above.

[0067] In another embodiment of the invention as shown in Figure 46, an ESTSM enabled electronic device may contain a HDD 4600 including an application component 4610 and an ECA 4620. Through an Internet connection 4690, the ECA 4620 allows the electronic device to communicate with the ESTSM Server Computer System 4685. Server computer system 4685 includes a number of servers 4685a, 4685b, ... 4685n that may be web servers containing the web pages and data for ESTSM described above. The HDD may include a Host Protected Area (HPA) 4630 containing ESTSM non-viewable components 4640. The non-viewable components 4640 may include a VALIDATOR program 4650 that inspects an ESTSM Communications Area (ECA) 4620 to determine if the ESTSM application components 4610 have run correctly during the last system boot. The non-viewable component may also contain a copy of the original application component software fileset 4660 if the files need to be re-installed to the HDD. As described above, every time the electronic device boots up, the BIOS component 4675 will check the integrity of the ESTSM non-viewable components 4640 and application component 4610 programs and files, and restore the original programs and files from the backup fileset 4660 or from recovery media 4670, if they have been tampered with. Furthermore, the BIOS component 4675 will ensure that the application component 4610 has run properly on the previous device boot and will take action if it is determined that an attempt to bypass the application component 4610 has occurred.

DELL EXHIBIT 1002
Page 34 of 659

[0068] In another embodiment of the invention as shown in Figure 47, the ESTSM enabled electronic device may include a HDD 4700 containing an application component 4710 that receives and transmits information to a remote component that may be an ESTSM WWW component 4725 through the Internet 4723. In some embodiments of the invention, the application component may reside in the ESTSM WWW component on the ESTSM website and may be installed by the user from the ESTSM website. The application component 4710 may be coupled to an ECA 4720. The ECA may couple to a BIOS component 4730 that is connected to a secure non-volatile area 4740 as described above. The ESTSM application component 4710 may communicate through the ECA 4720 to the BIOS component 4730. The ECA also allows the application and BIOS components to communicate with an ESTSM server computer system 4750 through an Internet connection 4770. Server computer system 4750 includes a number of servers 4760a, 4760b, ... 4760n that may be web servers containing the web pages and data for ESTSM described above.

[0069] Turning now to Figure 48, in accordance with some other embodiments of the invention, the architecture for an ESTSM enabled electronic device with Short Messaging Service (SMS) capability is shown. The ESTSM enabled electronic device with SMS capability may be a PDA, WLAN capable computer, mobile phone that in some embodiments may be a cell phone, or Smart Phone. The electronic device may include a Flash memory 4800 containing a changeable area 4810 that functions like non-volatile storage and may include a file system. A system area 4820 in the Flash memory 4800 that is non-changeable to a user of the electronic device may include an ESTSM SMS component 4830, ESTSM application component 4840 and a secure non-volatile area 4850 coupled to the application component 4840. The application component 4840 communicates with web servers 4870a, 4870b, ... 4870n in the ESTSM server computer system through an Internet connection 4845. The ESTSM server computer system also includes a SMS server 4860 coupled to the SMS component 4830 through a wireless communication connection 4855 such as Code Division Multiple Access (CDMA) or Global Mobile System (GSM). In some embodiments, the SMS component 4830

DELL EXHIBIT 1002
Page 35 of 659

communicates with the ESTSM server using SMS services on the electronic device when an Internet connection is not available.

[0070] Turning now to Figure 49, a computer system that includes a BIOS component, application component and non-viewable component in accordance with one embodiment of the invention is shown. Computer system 4900 may be configured in any number of ways, including as a laptop unit, a desktop unit, a network server, or any other configuration. Computer system 4900 generally includes a central processing unit (CPU) 4902 coupled to a main memory array 4906 and to a variety of other peripheral computer system components through an integrated bridge logic device 4904. The bridge logic device 4904 is sometimes referred to as a "North bridge" for no other reason than it often is depicted at the upper end of a computer system drawing. The CPU 4902 couples to North bridge logic 4904 via a CPU bus 4908, or the bridge logic 4904 may be integrated into the CPU 4902. The CPU 4902 may comprise, for example, a Pentium™ IV microprocessor. It should be understood, however, that computer system 4900 could include other alternative types of microprocessors. Further, an embodiment of computer system 4900 may include a multiple-CPU architecture, with each processor coupled to the bridge logic unit 4904. An external cache memory unit 4909 further may couple to the CPU bus 4908 or directly to the CPU 4902.

[0071] The main memory array 4906 couples to the bridge logic unit 4904 through a memory bus 4910. The main memory 4906 functions as the working memory for the CPU 4902 and generally includes a conventional memory device or array of memory devices in which program instructions and data are stored. The main memory array may comprise any suitable type of memory such as dynamic random access memory (DRAM) or any of the various types of DRAM devices such as synchronous DRAM (SDRAM), extended data output DRAM (EDO DRAM), or Rambus™ DRAM (RDRAM).

[0072] The North bridge 4904 couples the CPU 4902 and memory 4906 to the peripheral devices in the system through a Peripheral Component Interconnect (PCI) bus 112 or other expansion bus, such as an Extended Industry Standard Architecture (EISA) bus. The present invention, however, is not limited to any particular type of expansion

DELL EXHIBIT 1002
Page 36 of 659

bus, and thus various buses may be used, including a high speed (66 MHz or faster) PCI bus. Various peripheral devices that implement the PCI protocol may reside on the PCI bus 4912, as well.

[0073] The computer system 4900 includes a graphics controller 4916 that couples to the bridge logic 4904 via an expansion bus 4914. As shown in FIG. 49, the expansion bus 4914 comprises an Advanced Graphics Port (AGP) bus. Alternatively, the graphics controller 4916 may couple to bridge logic 4904 through the PCI bus 4912. The graphics controller 4916 may embody a typical graphics accelerator generally known in the art to render three-dimensional data structures on display 4918.

[0074] Bridge logic 4904 includes a PCI interface to permit master cycles to be transmitted and received by bridge logic 4904. The bridge logic 4904 also includes an interface for initiating and receiving cycles to and from components on the AGP bus 4914. The display 4918 comprises any suitable electronic display device upon which an image or text can be represented. A suitable display device may include, for example, a cathode ray tube (CRT), a liquid crystal display (LCD), a thin film transistor (TFT), a virtual retinal display (VRD), or any other type of suitable display device for a computer system.

[0075] The computer system 4900 optionally may include a Personal Computer Memory Card International Association (PCMCIA) drive 4932 coupled to the PCI bus 4912. The PCMCIA drive 4932 is accessible from the outside of the computer and accepts one or more expansion cards that are housed in special PCMCIA cards, enclosures which are approximately the size of credit cards but slightly thicker. Accordingly, PCMCIA ports are particularly useful in laptop computer systems, in which space is at a premium. A PCMCIA card typically includes one connector that attaches to the PCMCIA port 4932, and additional connectors may be included for attaching cables or other devices to the card outside of the computer 4900. Accordingly, various types of PCMCIA cards are available, including modem cards, network interface cards, bus controller cards, and memory expansion cards.

[0076] If other secondary expansion buses are provided in the computer system, another bridge logic device typically couples the PCI bus 4912 to that expansion bus.

DELL EXHIBIT 1002
Page 37 of 659

This bridge logic is sometimes referred to as a "South bridge," reflecting its location vis-à-vis the North bridge in a typical computer system drawing. In FIG. 49, the South bridge 4922 couples the PCI bus 4912 to an Industry Standard Architecture (ISA) bus 4926 and to an Integrated Drive Electronics (IDE) bus 4964. The IDE bus 4964 typically interfaces input and output devices such as a CD ROM drive, a Digital Video Disc (DVD) drive, a hard disk drive, and one or more floppy disk drives. In accordance with the embodiment of the invention shown in Figure 44, the IDE bus 4964 shown in Figure 49 couples to HDD 4400. ESTSM application component 4405 and ECA 4440 may be executable software files stored in a file system of HDD 4400. Hidden partition 4455 in HDD 4400 may include ESTSM non-viewable components 4415 as described in detail above with reference to Figure 44.

[0077] Various ISA-compatible devices are shown coupled to the ISA bus 4926, including a BIOS ROM 4944. The BIOS ROM 4944 is a memory device that stores commands which instruct the computer how to perform basic functions such as sending video data to the display or accessing data on hard floppy disk drives. In addition, the BIOS ROM 4944 may be used to store power management instructions for hardware-based (or "legacy") power management systems or to store register definitions for software-based power management systems. The BIOS instructions also enable the computer to load the operating system software program into main memory during system initialization and transfer control to the operating system so the operating system can start executing, also known as the INT19 "boot" sequence. BIOS ROM 4944 in Figure 49 includes the ESTSM BIOS component 4410 in accordance with the embodiment of the invention shown in Figure 44. The ESTSM BIOS component 4410 in BIOS ROM 4944 couples through a bus that may be a serial bus 4464 (a serial bus generally is a bus with only one data signal) to secure non-volatile area 4465 containing firmware code. The BIOS ROM 4944 typically is a "nonvolatile" memory device, which means that the memory contents remain intact even when the computer 4900 powers down. By contrast, the contents of the main memory 4906 typically are "volatile" and thus are lost when the computer shuts down.

DELL EXHIBIT 1002
Page 38 of 659

[0078] The South bridge 4922 supports an input/output (I/O) controller 4960 that operatively couples to basic input/output devices such as a keyboard 4968, a mouse 4970, a floppy disk drive 4966, general purpose parallel and serial ports 4972, and various input switches such as a power switch and a sleep switch (not shown). The I/O controller 4960 typically couples to the South bridge via a standard bus, shown as the ISA bus 4926 in FIG. 49. A serial bus 4962 may provide an additional connection between the I/O controller 4960 and South bridge 4922. The I/O controller 4960 typically includes an ISA bus interface (not specifically shown) and transmit and receive registers (not specifically shown) for exchanging data with the South bridge 122 over the serial bus 4962.

[0079] Turning now to Figure 50, a wireless communication device that may be a PDA, WLAN capable computer, mobile phone that in some embodiments is a cell phone, or SmartPhone includes a changeable area and an application component in a system area in accordance with the embodiment of the invention of Figure 45. The wireless communication device 5000 may transmit and receive information with a plurality of base transceiver stations (BTS) not shown in Figure 50. Each BTS may transmit in a forward or downlink direction both physical and logical channels to the mobile station 5000 in accordance with a predetermined air interface standard. A reverse or uplink communication path also exists from the mobile station 5000 to the BTS, which conveys mobile originated access requests and traffic.

[0080] The air interface standard can conform to any suitable standard or protocol, and may enable both voice and data traffic, such as data traffic enabling Internet access and web page downloads. One suitable type of air interface is based on Time Division Multiple Access (TDMA) and may support a GSM or an advanced GSM protocol, although these teachings are not intended to be limited to TDMA or to GSM or GSM-related wireless systems. Another wireless system and air interface, such as a Wideband Code Division Multiple Access (WCDMA) system, may serve at least a part of the geographical area served by the wireless communication system shown in FIG. 50, and the mobile station 5000 maybe a multi-band terminal that is capable of operating with either the GSM or the WCDMA network.

DELL EXHIBIT 1002
Page 39 of 659

[0081] The mobile station 5000 typically includes a microcontrol unit (MCU) 5020 having an output coupled to an input of a display 5040 and an input coupled to an output of a keyboard or keypad 5060. The mobile station 5000 may be contained within a card or module that is connected during use to another device. For example, the mobile station 5000 could be contained within a PCMCIA or similar type of card or module that is installed during use within a portable data processor, such as a laptop or notebook computer, or even a computer that is wearable by the user.

[0082] The MCU 5020 includes or is coupled to a memory 5030, including a system area 4520 for storing ESTSM application components 4530, as well as a changeable area for temporarily storing required data, scratchpad memory, received packet data, packet data to be transmitted, and the like. A separate, removable Subscriber Identity Module (SIM) that is not shown can be provided as well, the SIM storing, for example, a preferred Public Land Mobile Network (PLMN) list and other subscriber-related information. The system area 4520 may also store a program enabling the MCU 5020 to execute the software routines, layers and protocols required to operate in the wireless communications system, as well as to provide a suitable user interface (UI), via display 5040 and keypad 5060, with a user. Although not shown, a microphone and speaker are typically provided for enabling the user to conduct voice calls in a conventional manner.

[0083] The mobile station 5000 also contains a wireless section that includes a digital signal processor DSP 5080, or equivalent high speed processor or logic or control unit, as well as a wireless transceiver that includes a transmitter (Tx) 5010 and a receiver (Rx) 5020, both of which are coupled to an antenna 5040 for communication with the BTS 50. At least one local oscillator (LO) 5060, such as a frequency synthesizer, is provided for tuning the transceiver. Data, such as digitized voice and packet data, is transmitted and received through the antenna 5040.

[0084] As mentioned above with reference to Figure 45, the ESTSM enabled PDA, mobile phone, WLAN capable computer, or SmartPhone may continuously communicate to the ESTSM Server Computer System through an always-on Internet connection. Information such as telephone numbers, email addresses, calendar

DELL EXHIBIT 1002
Page 40 of 659

appointments, sales meetings and other daily reminders on a PDA, mobile phone, WLAN capable computer, or SmartPhone with ESTSM can be retrieved from a stolen device in one embodiment of the invention by the user calling an ESTSM service center to report the device as stolen. Because the PDA, mobile phone, WLAN capable computer, or SmartPhone has an always-on Internet connection, data on the device can be recovered and stored on the ESTSM server computer system as soon as the device is reported stolen. After recovery, the data may be erased off the stolen PDA, mobile phone, WLAN capable computer, or SmartPhone and the device disabled, making it worthless for the thief. Upon the ESTSM user purchasing a replacement PDA, mobile phone, WLAN capable computer, or SmartPhone, the data recovered and stored on the ESTSM server computer system from the user's stolen device can be placed on the user's new replacement device.

[0085] Turning now to Figure 51, one embodiment of the ESTSM server computer system 5100 of Figures 44-47 is shown in more detail. Clients 5110 are ESTSM enabled electronic devices that transmit and receive information through firewall 5120 to web servers 5130. The firewall 5120 may be software executing on each of the web servers 5130 or a stand alone firewall device with dedicated hardware and software that may be a computer system. Web servers 5130 as described above include web pages for administration and use of ESTSM as well as software to transmit the web pages and receive responses from clients 5110. Web servers 5130 connect through firewall 5140 to one or more database servers 5150. Firewall 5140 may be software executing on each of the database servers 5150 or a stand alone firewall device with dedicated hardware and software that may be a computer system. Database servers 5150 may contain among other information, user configuration information and access rights for clients 5110. Configuration information may include the ESTSM services selected by a user, the electronic devices associated with a particular user, electronic device identification information, billing information such as credit card number and expiration date, electronic device location and status logs, and so forth. Web servers 5130 may also couple to File Transfer Protocol (FTP) server 5160 that allows clients 5110 to download large files directly without having to go through web servers 5130. Web servers 5130

DELL EXHIBIT 1002
Page 41 of 659

also have access to files on FTP server 5160 allowing clients to access and view the contents of these files through the web servers.

[0086] Turning now to Figure 52, web servers 5130 of Figure 51 are depicted in greater detail and show connections between the primary and secondary servers in accordance with some embodiments of the invention. Clients 5110 may each connect to primary server 5210 and each of secondary server 5220a, 5220b, ... and 5220n. The primary server 5210 and secondary servers 5220a, 5220b, ... 5220n are coupled to each other and can communicate and transfer information. In some embodiments of the invention as described in greater detail below, each of clients 5110 includes an application component that works with web browser software such as Microsoft® Internet® Explorer® to ensure that if Explorer® can access the ESTSM website, the ESTSM application components will also be able to access the website. If Explorer® on the client cannot get to the ESTSM website on the primary server 5210, it will then try to access the ESTSM secondary servers 5220a, 5220b, ... 5220n for status of the primary. If the secondary servers are also unavailable, but ESTSM application component on the client can access other popular websites, then it is assumed that some firewall or other software has been loaded to attempt to block ESTSM operation.

[0087] The web pages for registration on the ESTSM server can be customized for each type of electronic device and manufacturer. This way, manufacturers can offer different services to the user, during the registration phase, based on the model and target customers for that model. Thus, for example, a manufacturer may want to set a higher price for "Data Destroy Services" on corporate laptop models, then on consumer laptop models.

[0088] If the ESTSM server computer system receives a message from an electronic device that has been reported stolen, and the "Tracking Service" is registered for that electronic device, the ESTSM server will log the IP address of the stolen electronic device. The ESTSM server computer system will get the IP address from the header of the message packet (part of Internet Protocol (IP)) and will not have to execute a tracing program such as TraceRoute on the electronic device that may be a client personal computer. The ESTSM server will use the Internet to lookup the information

DELL EXHIBIT 1002
Page 42 of 659

for that IP address and will send the tracking location email as described above to the user.

[0089] The ESTSM server computer system hosts all the web pages that provide the user experience once logged into the ESTSM website. The ESTSM server environment can be duplicated at a corporate customer facility and the specific serial numbers of the electronic devices at that corporation can be re-directed to work directly with the ESTSM server located at that corporation. Thus, corporate customers, for security purposes, can control the flow of messages to servers located at their own facility.

[0090] If the ESTSM server needs repairs to hardware, new software, functional changes to web pages, etc. electronic device clients may be requested by the server to stop making new queries to the server for a random amount of time. Thus, needed updates and repairs to the ESTSM sever may be performed during this time.

[0091] Turning now to Figure 53, a flow diagram in accordance with some embodiments of the invention of the BIOS component of ESTSM of Figure 44 is shown. The Power on Self Test (POST) firmware may call the ESTSM BIOS component 5310 towards end of POST. The BIOS component will first check to see if the electronic device has already been disabled by ESTSM 5335 (i.e. the electronic device was reported stolen, or some other ESTSM failure occurred). If the electronic device is already disabled, the BIOS component will display the system information and a boot specific unlock key and will prompt the user to enter the activation password to re-enable system boot 5320. This activation password can be obtained by the original user through the ESTSM website or by calling the monitoring station.

[0092] If the system was not already disabled, the BIOS component checks to see if the special ESTSM hidden partition exists 5340. If it does exist, the BIOS component will transfer control to ESTSM non-viewable component VALIDATOR program 5345. If the hidden partition does not exist the BIOS component will create the ESTSM hidden partition 5350. If there is a bootable operating system partition on the hard disk 5355, the BIOS component will force the user to insert the recovery media into the appropriate device 5365. The BIOS component will re-build the ESTSM hidden partition using the

DELL EXHIBIT 1002
Page 43 of 659

files from the recovery media 5370. As mentioned above, if the hidden partition does not exist, a check is also made to see if a bootable operating system partition is present before forcing the recovery media to be inserted. If a bootable operating system partition is not present, then the electronic device will proceed with the boot process 5360 until it stops because no bootable OS is present. This may occur if the thief deletes the OS in which case he must install the OS and the recovery media to allow the system to reboot. Alternatively, a bootable OS partition may not be present as during initial HDD installation at the factory, and a master hard disk image may be used for seamless factory installation during boot process 5360 without requiring the recovery media to be inserted in each electronic device during manufacture.

[0093] Turning now to Figure 54, a flow diagram of the VALIDATOR program in the non-viewable component of the ESTSM in accordance with some embodiments of the invention is shown. If the hidden partition on the hard disk is valid, the BIOS component will load and transfer control to the VALIDATOR program 5345 on the hidden partition as shown in Figure 53 and described above. The VALIDATOR program inspects the ESTSM Communications Area (ECA) to determine if the ESTSM application components have run correctly during the last system boot 5410. If the ECA information is correct (i.e. ESTSM application was run correctly), then the VALIDATOR program will return control to POST to proceed with INT19 OS boot process 5430. If the VALIDATOR program determines that the application components failed to run correctly 5420, the user is warned to correct the problem otherwise the electronic device will be disabled within a number of system boots 5440 that in one embodiment of the invention is 5 system boots. The VALIDATOR program will then restore the ESTSM application components from ESTSM backup fileset to try to correct the problem 5450. If the number of system boots has been reached and ECA information is still not correct 5460, then ESTSM will disable the system 5470. The procedure described above may then be used to re-enable the system. An application component failure will be generated if the thief deletes or tampers with ESTSM files, loads an application or service to try to bypass ESTSM operation, or in any other way tries to prevent ESTSM from running. After the VALIDATOR program has completed operation, it returns control back to the

DELL EXHIBIT 1002
Page 44 of 659

electronic device BIOS 5430 so that system POST may be completed and the normal OS boot can occur via the INT19 interface.

[0094] In some other embodiments of the invention, the check of the ECA to determine if the ESTSM application components have run correctly is performed by the BIOS component-thus the VALIDATOR program may be located in the BIOS component. If the VALIDATOR program determines that the application components failed to run correctly, the user is asked to install the application components onto the electronic device.

[0095] As shown in Figure 44, the ESTSM application component consists of two sets of programs: (1) ESTSM application program and (2) startup program files. The application component programs work together to provide the ESTSM environment described above and periodically check with the ESTSM server computer system to see if the electronic device is reported stolen and take the appropriate action.

[0096] A flow diagram of the application component of the ESTSM is shown in Figure 55 in accordance with one embodiment of the invention. The startup program 5500 creates the appropriate system processes and loads and executes the ESTSM application program 5505 on the electronic device that performs most of the ESTSM operations. The ESTSM application program works with the operating system driver files to communicate with the ECA. The ESTSM application program will check the integrity of all the ESTSM application components 5510 and will ensure ESTSM is working correctly. The ESTSM application program will communicate this information to the BIOS component through the ECA. Checking the integrity of ESTSM application components may include interfacing with specialized security hardware on the electronic device that in one embodiment of the invention may be Trusted Platform Module (TPM) integrated circuitry. If there is a problem with the ESTSM application components, no information will be communicated to the ECA and on the next electronic device boot, the BIOS component will not allow the electronic device to boot. Otherwise, the ESTSM application program will then try to detect an Internet connection on the electronic device. Once an Internet connection is established by the user, the ESTSM application program will attempt to contact the primary ESTSM server 5515. If the ESTSM

DELL EXHIBIT 1002
Page 45 of 659

application program is successful in contacting the primary ESTSM server, the application program will then send an encrypted query to the primary ESTSM server 5520. Encryption of the query may involve interfacing with specialized security hardware on the electronic device such as TPM integrated circuitry described in more detail below. This query will identify the electronic device by the device system information such as serial number and model number (no other user data is sent to the server) 5520. The ESTSM application program receives the electronic device status from the server to determine if the device is registered with ESTSM 5525. If the electronic device is not registered with the ESTSM server, the user is given the option to complete the registration phase as described above and shown in Figure 55 5535, 5540, and 5545 .

[0097] If the system is registered with ESTSM server, the electronic device executing the ESTSM application program will receive a response from the ESTSM server computer system indicating whether or not the electronic device is reported stolen. If the electronic device is in an active state (i.e. not stolen), the application program will wait an interval and again contact the ESTSM server 5515. If the electronic device is reported stolen 5550, the ESTSM application program will cooperate with the other application components to take the appropriate action (i.e. disable the system, erase the hard disk drive, etc) 5555 and 5560. If the user has selected the disable electronic device service, then the ESTSM application program will inform the ECA of electronic device disabled state 5580 and freeze the electronic device 5585. The electronic device executing the ESTSM application program will send an encrypted message to the ESTSM server periodically while the system is connected to the Internet.

[0098] The application component of ESTSM is designed so that firewall software cannot block the ESTSM application components from accessing the ESTSM website. If firewall software could block the ESTSM application components, a thief could merely install the firewall software to bypass ESTSM. The ESTSM application program works with web browser software such as Microsoft® Internet® Explorer® to ensure that if Explorer® can access the ESTSM website, the ESTSM application components will also be able to access the website. If Explorer® cannot get to the ESTSM website on the primary server, it will then try to access the ESTSM secondary

DELL EXHIBIT 1002
Page 46 of 659

servers for status of the primary as shown in Figure 55 in 5565. If the secondary servers are also unavailable, but ESTSM can access other popular websites 5587, then it is assumed that some firewall or other software has been loaded to attempt to block ESTSM operation. In this case, in one embodiment of the invention, the user is warned that they must correct the problem 5570 within five boots 5575 or enter an "override" code to continue operation with ESTSM temporarily disabled. The "override" code can be obtained from the ESTSM website, call center, or an automated response system. If the override code is not entered, the system will be disabled after five boots 5580 and 5585, and the user must get the activation password as described above.

[0099] The ESTSM server is located at a particular address on the WWW accessible to the user. The application components of ESTSM communicate with this web server during the registration phase and periodically once the system is registered to determine if the electronic device has been reported stolen.

[0100] Turning now to Figure 56, encryption and encoding of information by the client electronic device and decoding and decryption of information by the server computer system in accordance with one embodiment of the invention is shown. A client 5610 that is an ESTSM enabled electronic device includes an ESTSM application component 5615 as described above. The ESTSM application component 5615 may be coupled to an encryption/decryption module 5620 that transmits and receives encrypted and encoded data. The encrypted and encoded data may be transmit and received from an ESTSM server computer system 5630 through a communication medium 5625 such as HyperText Transfer Protocol (HTTP). The server computer system 5630 includes an ESTSM server application 5640 that may include web pages and information displayable on ESTSM enabled devices as described above and ESTSM server application software. The ESTSM server application 5640 may be coupled to an encryption/decryption module 5635 that transmits and receives encrypted and encoded data to and from client 5610.

[0101] Turning now to Figure 57, encryption and encoding of information by the client electronic device and decoding and decryption of information by the server computer system of Figure 56 is shown. Client electronic device 5610 may frequently and at randomly selected times send a query to server computer system 5630 asking if the

DELL EXHIBIT 1002
Page 47 of 659

electronic device has been reported stolen. The query is encrypted 5715 by encryption/decryption module 5620 using an encryption technique as described below into a binary format sequence 5720 of ones and zeroes. The sequence of ones and zeros is encoded 5725 by encryption/decryption module 5620 using an encoding technique as described below into an American Standard Code of Information Interchange (ASCII) text format 5730. ASCII text format is a standard 7-bit ASCII character code embedded in an 8 bit byte whose high order bit is always zero as described in ANSI standard X3.64, herein incorporated by reference.

[0102] Simultaneously with the encryption and encoding performed by encryption/decryption module 5620, the server computer system receives ASCII text formatted data 5755 via communication medium 5625. The ASCII text formatted data is decoded 5750 by encryption/decryption module 5635 using a decoding technique as described below into a binary format sequence 5745 of ones and zeroes. The sequence of ones and zeroes is decrypted 5740 by encryption/decryption module 5635 into query information 5735 that may be as mentioned above asking if the electronic device has been reported stolen.

[0103] Referring now to Figure 58, a flow diagram implemented in the client and server for encoding binary format sequence data into ASCII text format data in accordance with some embodiments of the invention is shown. If the end of the binary format sequence data source 5810 has been reached as determined by the value of the source_length variable then encoding ends 5815. If the end has not been reached, then the next byte to encode is stored 5820 in a variable. Thus, 'n' bits from the variable are extracted 5820 into another variable that in one embodiment may be C1. ASCII text format may have n=6 bits with the highest order 7th and 8th bit being zero. Variable C1 is passed to ENC( ) function that performs binary mapping operations on the binary sequence data to generate an encoded byte 5830. In some embodiments of the invention, the binary mapping operations on C1 includes mapping C1 to a base 64 number. The encoded byte is placed into a Destination data structure 5840 that may be an array of bytes for transmission over communication medium 5625. The encoded byte is re-

DELL EXHIBIT 1002
Page 48 of 659

initialized to a zero value in one embodiment of the invention and the source_length variable is decremented.

[0104] Referring now to Figure 59, a flow diagram implemented in the client and server for decoding ASCII text format data into binary data in accordance with some embodiments of the invention is shown. Encryption/decryption modules located in the client electronic device or server computer system receive encoded bytes of ASCII text format data that are placed into a source byte stream data structure that may be an array of bytes. The source byte stream data structure is described by a source_length variable that indicates the number of ASCII text format data bytes present in the array. Every time a new byte of data is received by the encryption/decryption module and placed in the array, the source_length variable is incremented and when a byte of data is removed and decoded the source_length variable is decremented. If the end of source 5910 has been reached, the array will become empty and decoding will end 5930. If the end of the source has not been reached, then, a current ASCII text format byte of data is placed into variable E. The ASCII text format byte of data in variable E is passed to DECODE( ) function that performs mapping operations on the data to generate a decoded byte ED 5950. The lower six bits of the decoded byte ED are placed into a final byte stream data structure 5960 and the upper two bits are discarded. Finally, the source_length variable is decremented as described above. If the end of the source byte stream is reached, every eight bits in the final byte stream 5920 corresponds to the original unencoded data.

[0105] Turning now to Figure 60, a flow diagram showing encryption and encoding of SMS messages from SMS server to SMS enabled ESTSM electronic device for the system of Figure 48 is depicted. Each SMS capable device that in some embodiments of the invention may be a Smart Phone includes unique device information that is used in the encoding and encryption process. The encryption/decryption module in the Smart Phone stores the device information into a variable DI as shown in block 6010. The encryption/decryption module passes the device information in variable DI to a function Jumble as shown in block 6020 and stores the result into a variable JDI. In some embodiments of the invention, the function Jumble rearranges and reorders the individual bytes in variable DI. Next, the encryption/decryption module as shown in

DELL EXHIBIT 1002
Page 49 of 659

block 6030 generates an encrypted command by passing the jumbled device information in variable JDI and an ESTSM Secret Cmd to function FN. The ESTSM Secret Cmd is a command sent from the ESTSM server to the electronic device for a function supported by the electronic device. The function FN returns an encrypted command that is stored in variable ECMD and may be an array of bytes. Next, in block 6040, the encryption/decryption module calls the Encode function that may be the flowchart shown in Figure 58. The Encode function is passed the variable ECMD containing the encrypted command and encodes the array of bytes as shown in Figure 58. The encoded array of bytes is stored in a variable EncECMD that is transmitted as a message to the ESTSM server computer system over the communication medium 5625.

[0106] Turning now to Figure 61, a flow diagram showing decoding and decryption of SMS messages is depicted. A MESSAGE variable that in some embodiments of the invention is variable EncECMD containing the encoded array of bytes is decoded by a Decode function 6110 that may be the flow chart shown in Figure 59. The decoded array of bytes is stored in a variable DecFCMD that is then passed to a Decrypt function 6120. The Decrypt function returns a decrypted command that is stored in variable FCMD and may be an array of bytes. The jumbled device information is extracted from FCMD and stored in variable JDI 6130. Similarly, the ESTSM Secret Cmd/Data message is extracted from FCMD 6130. The encryption/decryption module passes the jumbled device information in variable JDI to a function UnJumble as shown in block 6140. The device information after being unjumbled is stored in a variable DEVICE INFO that is verified with the unique device information of the electronic device.

[0107] Implementing ESTSM on an electronic device may necessitate the manufacturer integrating the ESTSM BIOS components including the BIOS ROM images into the system BIOS of the electronic device. In some embodiments, this is the only task that may have to be performed during the system's development phase. The integration of the ESTSM BIOS component needs very little effort. The ESTSM BIOS component is designed to minimize the effort needed to integrate with the existing electronic device BIOS. Factors, such as size of code, complexity of integration, and so

DELL EXHIBIT 1002
Page 50 of 659

forth, have been addressed in the design of the ESTSM BIOS component. In one embodiment of the invention as shown in Figure 62a, the ESTSM BIOS component is integrated with the existing electronic device BIOS using the technique described below.

1. Place the ESTSM BIOS component image files into a system BIOS build file 6200. In some embodiments, the electronic device BIOS has 16 Kilobytes of free space to integrate the BIOS component image files.

2. Build a data structure including the electronic device's system information, programs to save and restore ESTSM critical information in the Secure Non-volatile Area, and an optional recovery media read function pointer and pass the address of this data structure to an ESTSM BIOS image entry point in the BIOS build file as shown in block 6210. Also ensure that the Random Access Memory (RAM) areas that ESTSM uses are not used by other BIOS functions. After the ESTSM BIOS image files are integrated into the system BIOS build, the system BIOS code builds the data structure as described above. The ESTSM BIOS image may need a pointer to the function in the system BIOS that reads from the recovery media. Since modern day BIOSes support reading from almost all types of recovery media (i.e. floppy diskettes, CD-ROM, USB key, and so forth), no extra code development is required and the address of the read function needs to be placed in the data structure passed to the ESTSM BIOS image. In some alternative embodiments of the invention that do not use recovery media, a pointer to the recovery media read function in system BIOS is not needed. The electronic device system BIOS developer should make sure that the RAM address locations used by ESTSM are not used by the system BIOS.

3. As shown in block 6220, system BIOS needs to call the ESTSM BIOS image entry point just before the INT19 bootstrap call. The system BIOS calls the ESTSM BIOS image entry point before making the INT19 boot strap call. At this point, the ESTSM BIOS image will be invoked and will perform all the checks that enable the secure system environment of ESTSM.

[0108] Figure 62b is a flow diagram showing integration of the ESTSM option ROM into a BIOS binary image in accordance with some embodiments of the invention.

DELL EXHIBIT 1002
Page 51 of 659

A BIOS editor application 6300 shown in Figure 63 is started in block 6230 and the "File" menu option 6315 is selected within the BIOS editor application in block 6235. The target .ROM or .WPH BIOS binary is opened in block 6235. The ESTSM ROM will be placed into the target BIOS binary. An "OPTION ROM" node 6320 in a "PROJECT" panel 6330 may be expanded in block 6240. In block 6245, if option ROMS are present under the "OPTION ROM" node than determine if space is present in the target BIOS binary for the ESTSM ROM in block 6250. If the target BIOS binary does not contain the space for the ESTSM ROM, an error message is generated in block 6260. If the target BIOS binary contains the space needed for the ESTSM ROM or no option ROMS are present in block 6245, then the ESTSM ROM is added to the target BIOS binary in block 6255. In some embodiments of the invention, the ESTSM ROM is added to the target BIOS binary by pressing the "Add" button 6340 shown in Figure 63. In block 6245, from the "File" menu 6315 "BUILD BIOS" is selected as shown in block 6265. Finally, in block 6270 after the "BUILD BIOS" has been completed, the ESTSM option ROM is present in the target BIOS binary.

[0109] As discussed above, the ESTSM BIOS component is provided to the manufacturer of the electronic device in an encapsulated Option ROM image format that may be ESTSM.ROM as shown in Figures 63 and 64. In some embodiments of the invention as shown in Figure 63, the manufacturer may utilize tools provided by BIOS vendors such as BIOS editors 6300 to merge the encapsulated ROM ESTSM image into the manufacturer's base BIOS image using the Option ROM format 6310. In some other embodiments of the invention as shown in Figure 64, the manufacturer may use a BIOS Configuration Utility 6400 to insert the encapsulated ROM ESTSM image 6410 into the manufacturer's base BIOS ROM image 6420. In this embodiment, the BIOS calls the ESTSM Option ROM in the same way as it would any other Option ROM image. The ESTSM ROM proceeds in the same manner as it would if it had been integrated into the BIOS using known BIOS integration techniques by checking the system security during INT 19 boot strap call.

[0110] Returning now to Figure 62a, maintaining and updating of the electronic device system BIOS is minimized because of the design of the ESTSM BIOS component.

DELL EXHIBIT 1002
Page 52 of 659

When the manufacturer needs to do a system BIOS update for the electronic device, no changes need to be made to the ESTSM BIOS component in the system BIOS. The manufacturer can simply fix the bugs in the BIOS and do a new system BIOS build as shown in Figure 62a (which will include the ESTSM BIOS components) and the new system BIOS will work correctly. The new system BIOS can then be Flash upgraded by the user without any impact to ESTSM operation.

[0111] If an update is released for the ESTSM components, the updated versions of the BIOS component image files may be copied into the BIOS build file and a new build performed. Once the new build is complete, the updated system BIOS can be released to the user. No additional coding or maintenance tasks need to be performed to update the ESTSM BIOS components in the system BIOS.

[0112] Integration of the ESTSM application component requires no action by the manufacturer of the electronic device. This is because the ESTSM BIOS component restores the application components onto the hard disk drive of the electronic device once the OS is installed on the electronic device. In some other embodiments of the invention, the application component may be installed by the user of the electronic device as described above.

[0113] For some embodiments of the invention, creation of the ESTSM hidden partition may be performed immediately after installation of the electronic device's hard disk drive. Various utilities can be used to create the hidden partition. In one embodiment, a scripted installation program including the utility to create the hidden partition may be run at the beginning of the manufacturing process. Typically, this utility should be run just before the FDISK.EXE or some other utility is used to create the OS partition on the hard disk drive.

[0114] If the manufacturing process copies a prepared hard disk image directly to a blank hard disk, then the prepared image should be created with the ESTSM hidden partition installed. Thus, when the prepared image is copied to the blank hard disk drive during manufacture, the ESTSM hidden partition will also be copied automatically from the prepared image.

DELL EXHIBIT 1002
Page 53 of 659

[0115] Engineering and electronic device quality assurance test processes may be performed by the manufacturer providing the ESTSM monitoring station with a block of electronic device serial numbers to be used as part of the testing process. The monitoring station will mark these serial numbers as "test" in the ESTSM server computer system and the user will not be billed on the credit card for these systems. This will facilitate the test process at the manufacturer's facilities.

[0116] Figures 65-70 show screen shots, in accordance with some embodiments of the invention, for registering and using ESTSM in the PDA or mobile phone shown in Figures 45 and 50. ESTSM registration as shown in Figure 65 for a mobile device may be performed using a computer system that can display ESTSM registration web pages. In some other embodiments of the invention, the ESTSM registration pages may be displayed on the mobile device capable of displaying web pages. Figure 65 shows a service selection screen that may include the cost of each service and the services offered. The services offered and the cost of each service may vary based on the manufacturer and model of the mobile device, the market segment of the mobile device (i.e. business device, home use device) and what the manufacturer has chosen to include for the device. Some manufacturers may want to change the pricing of the services, or offer bundled services to the user. For one embodiment of the invention, as shown below, is a list of the services available to the user.

1. Basic Service – with this service the user has the ability to have the mobile device disabled if it is stolen or lost. The information on the mobile device is made secure so that it cannot be accessed by someone who steals the mobile device or finds the device.
2. Data Recovery Service – this service will recover Contacts, Calendar, and other data such as pictures form the mobile device if the device is stolen or lost. ESTSM may recover this information to the ESTSM server computer system, before performing other service option actions. The user may then restore the data into a new cell phone, SmartPhone or PDA device that they purchase.

DELL EXHIBIT 1002
Page 54 of 659

[0117] In some embodiments of the invention, due to the extendible design of ESTSM, new services can be added for a mobile device such as third party insurance, data destroy service, tracking service, and data encryption service.

[0118] In some embodiments of the invention, most of ESTSM services are based on a yearly fee model. Some services such as data recovery may be billed on a per kilobyte basis-that is, the user indicates the number of kilobytes to be recovered during registration and is billed accordingly. However, if the mobile device is stolen and during data recovery more kilobytes are recovered, then a one time fee is charged to the user. The user may be billed at the end of the year to renew the service for one more year. The user may be sent an email before billing to give the user a chance to cancel the service if they wish.

[0119] After the user has selected the ESTSM services for their mobile device, in some embodiments of the invention, the ESTSM system as shown in Figure 66 may request that the user turn on the cell phone or open the flip cover. In accordance with some embodiments, the user through the computer system capable of displaying ESTSM web pages may then enter the mobile phone number, service provider, International Mobile Equipment Identifier (IMEI) number, and a phone description. The registration process for the mobile device is successfully completed as shown in Figure 67. In some other embodiments of the invention, ESTSM registration may not require any user intervention with the mobile device except an acknowledgement from the user at the end of the successful registration.

[0120] In another embodiment of the invention, an automated voice prompting system at a call center or live call center operator after authentication of the user may communicate with the user to perform ESTSM activities. All ESTSM activities performed through the Internet may also be performed by the call center including registration, reporting a system stolen, reporting system has been recovered and so forth.

[0121] Figure 68 shows a screen shot of the mobile device status web page that resides in the ESTSM server computer system in accordance with some embodiments of the invention. The user can perform the following tasks for the mobile device on the device status web page: (1) View the status of the mobile device running ESTSM; (2)

DELL EXHIBIT 1002
Page 55 of 659

Report a mobile device stolen; (3) Show the Billing and Electronic Device Location/Status Logs; (4) Perform User Management functions such as changing the user information, password and billing information; and (5) Perform Data Management functions such as viewing recovered data and transferring recovered data to another device.

[0122] As shown in Figure 68, the "Device Status" page shows for each mobile device, the Model Name, System Description, Phone Number, Current State, and ESTSM Services Active on the device. Depending on the Current State and the services selected by the user, certain task buttons will appear below the mobile device information. These task buttons let you perform different operations on the device (e.g. report the mobile device stolen and so forth). As shown in Figure 68, the user may click on the button labeled "Report Stolen" to start the process of reporting a mobile device stolen. The user will be taken to the "Report a Stolen Device" web pages. The user fills out the information on the web page to generate a theft incident report and the ESTSM site will log this report so that it may be given later to the appropriate authorities as proof of filing the theft incident report. This documentation may be provided to the user upon request.

[0123] In some embodiments of the invention, once the report is completed, the electronic device will be placed into the REPORTED STOLEN state. At this point, because of the always on connection of the mobile device to the Internet, in some embodiments the mobile device files are backed up and the device state will change to RECOVERED state as shown in Figure 69. The user may then manage these files to move them into a new cell phone, SmartPhone or PDA device that they purchase. After the data has been recovered, the ESTSM system informs the user that the mobile device is disabled as shown in Figure 70.

[0124] Turning now to Figure 71, a flow diagram showing implementation of ESTSM on mobile devices such as cellular telephones, Smart Phones, or WLAN capable computers as in Figure 45 and Figure 48 that have a messaging capability that may be Short Messaging Service (SMS) is depicted. In some embodiments of the invention, as described above, the ESTSM server computer system may inform the mobile device that it has been reported stolen and backup the data on the device. In some other

DELL EXHIBIT 1002
Page 56 of 659

embodiments of the invention, the ESTSM server may periodically backup the data on the device even if the mobile device has not been reported stolen. The ESTSM server may disable the mobile device (i.e. lock the user out but device can still communicate with ESTSM server) if the Subscriber Identity Module (SIM) card has been changed and the mobile device is reported stolen. The ESTSM server may also disable the mobile device if the IMEI number has been changed and the device is reported stolen.

[0125] As shown in Figure 71, the ESTSM application component located in the system area of the mobile device (Figure 45) gets the device identifier of the mobile device in block 7105. In some embodiments of the invention, the device identifier is a concatenated string of numbers that may include the IMEI number, manufacturer's model number of the mobile device, and the phone number associated with the mobile device. If the application component is not able to get the device identifier in block 7110, then the application component disables the mobile device 7115. If the application component is able to successfully get the device identifier, then the application component determines if the user information module has been changed in block 7120. In some embodiments of the invention, the user information module may be a SIM card located in the mobile device. In some other embodiments of the invention, the user information module may be stored on a Read-Only-Memory (ROM) that is a FLASH ROM or Electronically-Erasable-Programmable ROM (EEPROM) of the mobile device. The user information module identifies user information with the mobile device. The user information may be the phone number associated with the mobile device, user details, security information, and memory for a personal directory of numbers. If the user information module has been changed in the mobile device, the ESTSM application component gets the new phone number from the mobile device 7125. The application component in block 7135 notifies the ESTSM server of the new phone number. Next, in block 7130, the ESTSM application component determines the current state of the mobile device and begins the status loop 7140, waiting for a message from the ESTSM server. An encrypted and encoded message as described above may be communicated from the ESTSM server to the application component of the mobile device as shown in block 7150.

DELL EXHIBIT 1002
Page 57 of 659

[0126] In Figure 71, if the application component detects that a new message has arrived, message data is processed in block 7145. A command is extracted from the message data in block 7160 as described above and is stored into the variable Cmd. If the Cmd is "REGISTER" as shown in block 7165, then the user has registered the mobile device for ESTSM services. The ESTSM server is notified to change the mobile device state to "ACTIVE" in block 7187 and the application component sets the current state to "ACTIVE" in block 7185. If the Cmd is "DISABLE" as shown in block 7170, the mobile device is disabled 7192 and the application component sets the current state to "DISABLE" in block 7190. The ESTSM server may send a "DISABLE" command 7170 if the mobile device is reported stolen or the user information module that may be a SIM card has been changed and the device identifier has not changed in the mobile device. If the Cmd is "BACKUP" as shown in block 7175, the ESTSM server requests that the data on the mobile device be copied to the ESTSM server. As shown in block 7194, the ESTSM server begins to backup the data stored on the mobile device. The ESTSM server will recover the data requested by the user during registration for the mobile device. Thus, if during ESTSM registration the user had selected recovery of contacts and calendar data, these items will be backed-up. In some embodiments of the invention, the user may specify other data for recovery such as Mobile Commerce (M-commerce) monetary information stored on the mobile device. The ESTSM server in some embodiments of the invention may request that the mobile device be placed into a disabled state and, thus, the application component in the mobile device sets the current state to "DISABLE" in block 7190. If the Cmd is "RESTORE" as shown in block 7180, the ESTSM server starts to restore the data 7199 backed up from the mobile device back to the original mobile device that may have been recovered or a new mobile device. After restoring the data to the mobile device, the ESTSM server places the mobile device into an active state. The application component in the mobile device sets the current state to "ACTIVE" in block 7196 and waits for some time 7155 before starting the status loop 7140.

[0127] Turning now to Figure 72, the states and transitions of a mobile device with SMS messages for activation and operation of ESTSM services is shown. A mobile

DELL EXHIBIT 1002
Page 58 of 659

device as shown in Figure 45 including the ESTSM application component is initially in an "UNREGISTERED" state 7205. After completion of the registration process, the ESTSM server sends a SMS message to the mobile device indicating that the device is registered with ESTSM and placing the mobile device into an "ACTIVATION PENDING" state 7210. The mobile device sends a SMS confirmation message to the ESTSM server and transitions into an "ACTIVE" state 7215. In some embodiments of the invention as shown in Figure 72, the ESTSM server performs periodic backups of the data on the mobile device while in the "ACTIVE" state 7215. While in the active state, the ESTSM server computer system communicates over the Internet with the user to determine if the mobile device has been reported stolen. If the device is reported stolen using the ESTSM website, the mobile device is placed into a "REPORTED STOLEN" state 7225. The ESTSM server informs the mobile device via a secure communications channel to take the appropriate action based on the service options selected by the user (e.g. disabling the electronic device, destroying the storage device (e.g. hard disk drive (HDD)) data, recovering data, encrypting data and more). In some embodiments of the invention as shown in Figure 72, if the user during registration had selected the basic service, the mobile device is disabled and placed into a "DISABLE" state 7230. If the mobile device has been recovered or the user has purchased a new mobile device and the user re-enables the device using the ESTSM website, an SMS message is sent from the server to the mobile device placing the device into an "ENABLE PENDING" state 7220. The mobile device sends an SMS confirmation message to the ESTSM server indicating that it has received the re-enablement SMS message from the ESTSM server. The mobile device is placed into the "ACTIVE" state 7215.

[0128] If the user during registration had selected the data recovery service, the mobile device is placed into "BACKUP IN PROGRESS" state 7235 and data on the mobile device is backed-up to the ESTSM server. If the data is backed up successfully, the mobile device is placed into "DISABLED DATA BACKUP" state 7240, data on the device is deleted, and the mobile device is disabled. The mobile device may be transitioned to "ENABLE AFTER RECOVERY" state 7245 from either the "BACKUP IN PROGRESS" state 7235 or "DISABLED DATA BACKUP" state 7240 if the user re-

DELL EXHIBIT 1002
Page 59 of 659

enables the mobile device while the data backup is in progress. Once the mobile device has been recovered or the user has purchased a new mobile device and the user re-enables the device using the ESTSM website, an SMS message is sent from the server to the mobile device placing the device into an "ENABLE AFTER RECOVERY" state 7245. The mobile device sends an SMS confirmation message to the ESTSM server indicating that it has received the re-enablement SMS message from the ESTSM server. The mobile device is activated and placed into the "ACTIVE DATA BACKUP" state 7250. The data that has been backed-up into the ESTSM server is restored into the new or re-enabled mobile device in the "RESTORE IN PROGRESS" state 7260. After data has been restored into the mobile device, the device is placed into the "ACTIVE" state 7215.

[0129] While the invention has been disclosed with respect to a limited number of embodiments, those skilled in the art will appreciate numerous modifications and variations therefrom. It is intended that the appended claims cover all such modifications and variations as fall within the true spirit and scope of the invention.

DELL EXHIBIT 1002
Page 60 of 659

What is claimed is:

1. An electronic device security and tracking system, comprising:

a nonvolatile storage device;

a changeable area in the nonvolatile storage device, wherein the changeable area further comprises an application component and a secure area coupled to the application component; and,

a server system capable of communicating through a secure medium with the application component.

2. The electronic device security and tracking system of claim 1, wherein the server system is capable of communicating through the secure medium with the secure area.

3. The electronic device security and tracking system of claim 1, wherein the electronic device is a personal digital assistant.

4. The electronic device security and tracking system of claim 1, wherein the nonvolatile storage device is a Flash memory.

5. The electronic device security and tracking system of claim 1, wherein the application component comprises an application file.

6. An electronic device security and tracking system, comprising:

a nonvolatile storage device;

a changeable area in the nonvolatile storage device, wherein the changeable area further comprises a system area in the nonvolatile storage device, said system area comprising an application component and a secure area coupled to the application component; and

a server system capable of communicating through a secure medium with the application component.

DELL EXHIBIT 1002
Page 61 of 659

7. The electronic device security and tracking system of claim 6, wherein the server system is capable of communicating through the secure medium with the secure area.

8. The electronic device security and tracking system of claim 7, wherein the system area is not modifiable by a user of the electronic device.

9. The electronic device security and tracking system of claim 6, wherein the electronic device is a personal digital assistant.

10. The electronic device security and tracking system of claim 6, wherein the nonvolatile storage device is a Flash memory.

11. The electronic device security and tracking system of claim 6, wherein the application component comprises an application file.

12. An electronic device security and tracking system, comprising:

a nonvolatile storage device;

a changeable area in the nonvolatile storage device, wherein the changeable area further comprises an application component and a communication protocol component coupled to the application component; and,

one or more servers capable of communicating through a secure medium with the application component.

13. The electronic device security and tracking system of claim 12, wherein the communication protocol component is a smart messaging service component for mobile devices.

14. The electronic device security and tracking system of claim 13, further comprising:

DELL EXHIBIT 1002
Page 62 of 659

one or more smart messaging service servers capable of communicating through a communications medium with the smart messaging service component; and,

wherein the one or more servers that communicate with the application component are web servers.

15. The electronic device security and tracking system of claim 14, wherein the communications medium is from the group consisting essentially of smart messaging service wireless link, Code Division Multiple Access, and Global Mobile System.

16. The electronic device security and tracking system of claim 13, wherein the electronic device is from the group consisting essentially of Smart phone, smart messaging service capable device, and mobile phone device.

17. The electronic device security and tracking system of claim 12, wherein the nonvolatile storage device is a Flash memory.

18. The electronic device security and tracking system of claim 12, wherein the application component comprises an application file.

19. An electronic device security and tracking system, comprising:

a nonvolatile storage device;

a changeable area in the nonvolatile storage device, wherein the changeable area further comprises a system area in the nonvolatile storage device, said system area comprising an application component and a communication protocol component coupled to the application component; and,

one or more servers capable of communicating through a secure medium with the application component.

DELL EXHIBIT 1002
Page 63 of 659

20. The electronic device security and tracking system of claim 19, wherein the communication protocol component is a smart messaging service component for mobile devices.

21. The electronic device security and tracking system of claim 20, further comprising:

one or more smart messaging service servers capable of communicating through a communications medium with the smart messaging service component; and,

wherein the one or more servers that communicate with the application component are web servers.

22. The electronic device security and tracking system of claim 21, wherein the communications medium is from the group consisting essentially of smart messaging service wireless link, Code Division Multiple Access, and Global Mobile System.

23. The electronic device security and tracking system of claim 20, wherein the electronic device is from the group consisting essentially of Smart phone, smart messaging service capable device, and mobile phone device.

24. The electronic device security and tracking system of claim 19, wherein the nonvolatile storage device is a Flash memory.

25. The electronic device security and tracking system of claim 19, wherein the system area is not modifiable by a user of the electronic device.

26. The electronic device security and tracking system of claim 19, wherein the application component comprises an application file.

27. A communication system, comprising:

a communication device, comprising:

DELL EXHIBIT 1002
Page 64 of 659

a controller unit;

a digital signal processor coupled to the controller unit;

a nonvolatile storage device coupled to the controller unit, comprising:

a changeable area, wherein the changeable area further comprises an application component and a secure area coupled to the application component; and

a server system capable of communicating through a secure medium with the application component.

28. The communication system of claim 27, wherein the server system is capable of communicating through the secure medium with the secure area.

29. The communication system of claim 27, wherein the communication device is a personal digital assistant.

30. The communication system of claim 27, wherein the nonvolatile storage device is a Flash memory.

31. The communication system of claim 27, wherein the application component comprises an application file.

32. A communication system, comprising:

a communication device, comprising:

a controller unit;

a digital signal processor coupled to the controller unit;

a nonvolatile storage device coupled to the controller unit, comprising:

a changeable area, wherein the changeable area further comprises a system area, said system area comprising an application component and a secure area coupled to the application component; and

a server system capable of communicating through a secure medium with the application component.

DELL EXHIBIT 1002
Page 65 of 659

33. The communication system of claim 32, wherein the server system is capable of communicating through the secure medium with the secure area.

34. The communication system of claim 33, wherein the system area is not modifiable by a user of the communication device.

35. The communication system of claim 32, wherein the communication device is a personal digital assistant.

36. The communication system of claim 32, wherein the nonvolatile storage device is a Flash memory.

37. The communication system of claim 32, wherein the application component comprises an application file.

38. A communication system, comprising:

a communication device, comprising:

a controller unit;

a digital signal processor coupled to the controller unit;

a nonvolatile storage device coupled to the controller unit, comprising:

a changeable area, wherein the changeable area further comprises

an application component and a communication protocol component coupled to the application component; and,

one or more servers capable of communicating through a secure medium with the application component.

39. The communication system of claim 38, wherein the communication protocol component is a smart messaging service component for mobile devices.

DELL EXHIBIT 1002
Page 66 of 659

40. The communication system of claim 39, further comprising:

one or more smart messaging service servers capable of communicating through a communications medium with the smart messaging service component; and,

wherein the one or more servers that communicate with the application component are web servers.

41. The communication system of claim 40, wherein the communications medium is from the group consisting essentially of smart messaging service wireless link, Code Division Multiple Access, and Global Mobile System.

42. The communication system of claim 39, wherein the communication device is from the group consisting essentially of Smart phone, smart messaging service capable device, and mobile phone device.

43. The communication system of claim 38, wherein the nonvolatile storage device is a Flash memory.

44. The communication system of claim 38, wherein the application component comprises an application file.

45. A communication system, comprising:

a communication device, comprising:

a controller unit;

a digital signal processor coupled to the controller unit;

a nonvolatile storage device coupled to the controller unit, comprising:

a changeable area, wherein the changeable area further comprises a system area in the nonvolatile storage device, said system area comprising an application component and a communication protocol component coupled to the application component; and,

DELL EXHIBIT 1002
Page 67 of 659

one or more servers capable of communicating through a secure medium with the application component.

46. The communication system of claim 45, wherein the communication protocol component is a smart messaging service component for mobile devices.

47. The communication system of claim 46, further comprising:

one or more smart messaging service servers capable of communicating through a communications medium with the smart messaging service component; and,

wherein the one or more servers that communicate with the application component are web servers.

48. The communication system of claim 47, wherein the communications medium is from the group consisting essentially of smart messaging service wireless link, Code Division Multiple Access, and Global Mobile System.

49. The communication system of claim 46, wherein the communication device is from the group consisting essentially of Smart phone, smart messaging service capable device, and mobile phone device.

50. The communication system of claim 45, wherein the nonvolatile storage device is a Flash memory.

51. The communication system of claim 45, wherein the application component comprises an application file.

52. The communication system of claim 45, wherein the system area is not modifiable by a user of the communication device.

DELL EXHIBIT 1002
Page 68 of 659

ELECTRONIC DEVICE SECURITY AND TRACKING SYSTEM AND METHOD

ABSTRACT OF THE DISCLOSURE

A system and method for securing and tracking an electronic device. The system includes hardware, software and firmware components that cooperate to allow tracking, disabling, and other interaction with the stolen electronic device. The system includes an application component, non-viewable component and Basic Input/Output Subsystem (BIOS) component that are present on the electronic device. The BIOS component maintains the secured environment of the application and non-viewable components. If only the application component was provided, a simple low level format of the hard disk drive would remove the application and bypass the security features. The system implements an "application and BIOS" based solution to electronic device security.

DELL EXHIBIT 1002
Page 69 of 659

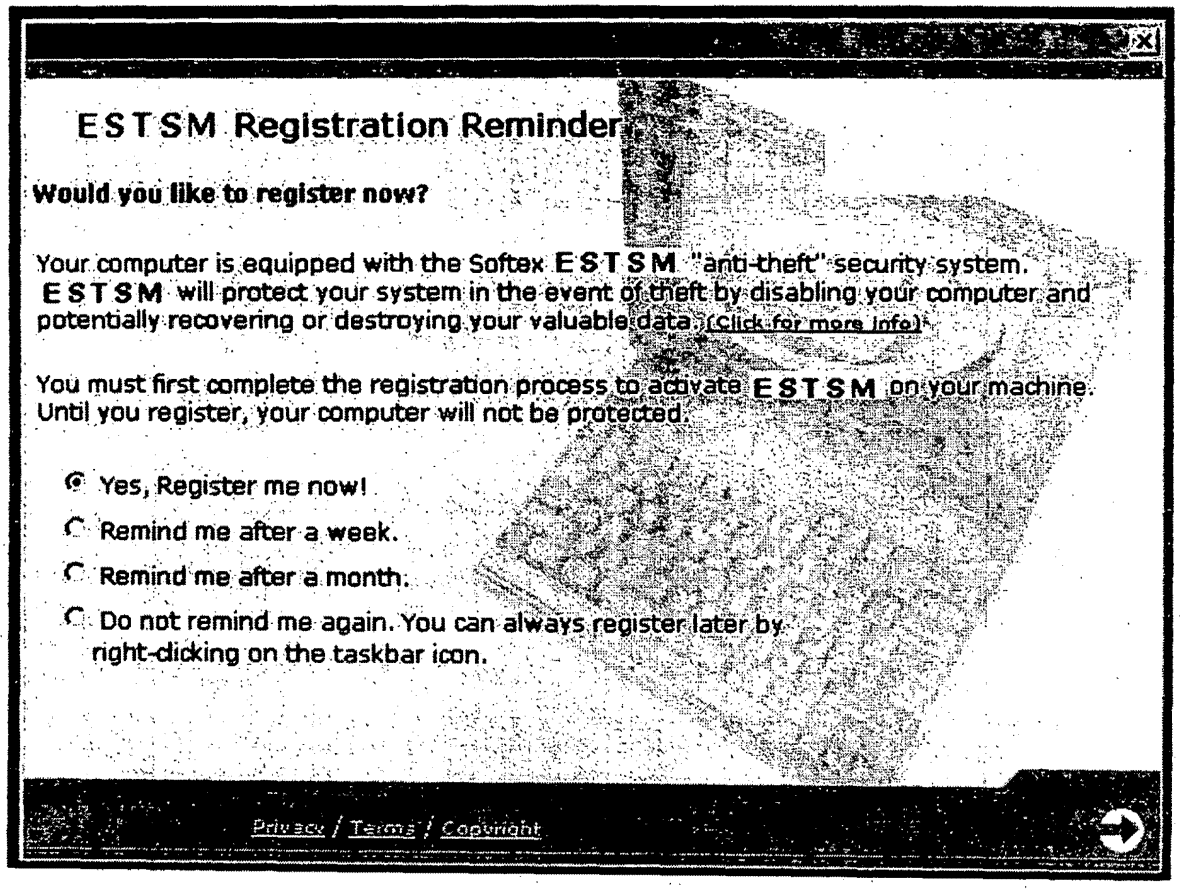

ESTSM Registration Reminder
Would you like to register now?
Your computer is equipped with the Softex ESTSM "anti-theft" security system. ESTSM will protect your system in the event of theft by disabling your computer and potentially recovering or destroying your valuable data. (Click for more info)
You must first complete the registration process to activate ESTSM on your machine. Until you register, your computer will not be protected.
Yes, Register me now!
Remind me after a week.
Remind me after a month.
Do not remind me again. You can always register later by right-clicking on the taskbar icon.
Privacy / Terms / Copyright

FIGURE 1

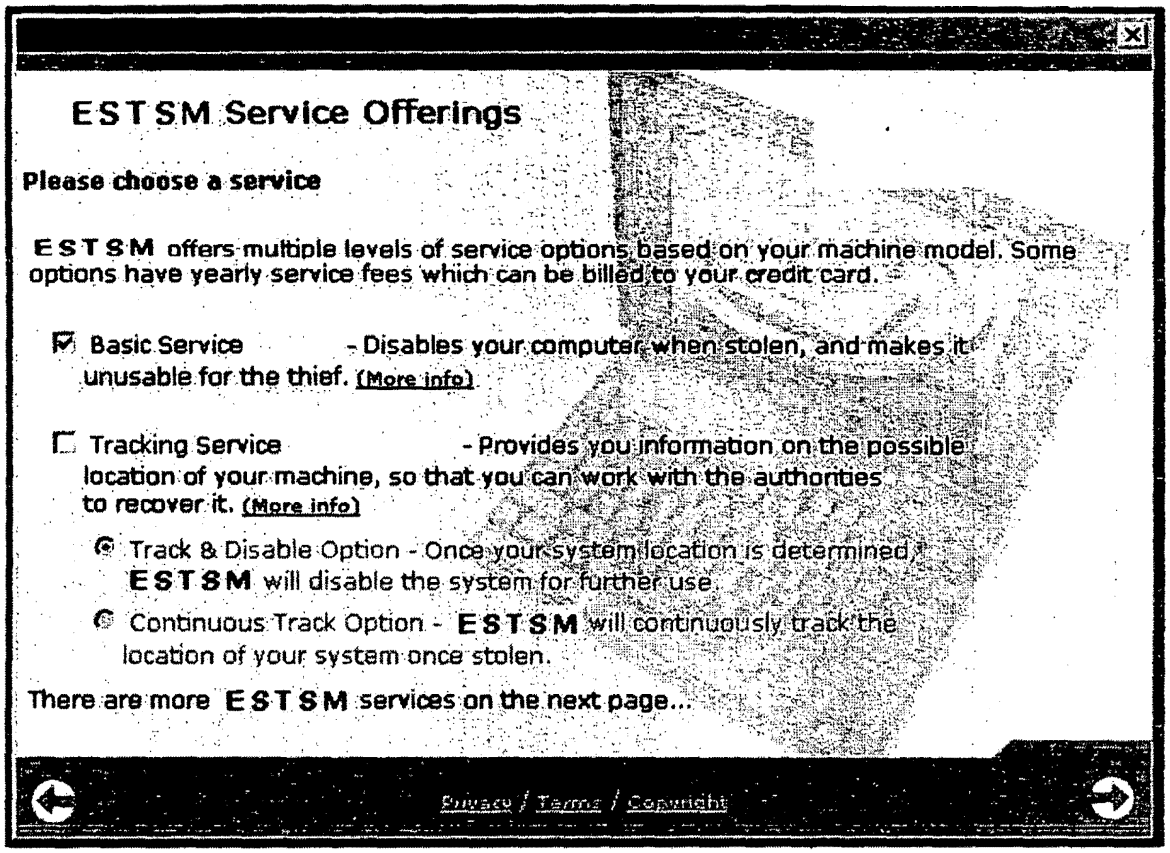

ESTSM Service Offerings
Please choose a service
ESTSM offers multiple levels of service options based on your machine model. Some options have yearly service fees which can be billed to your credit card.
Basic Service - Disables your computer when stolen, and makes it unusable for the thief. (More info)
Tracking Service - Provides you information on the possible location of your machine, so that you can work with the authorities to recover it. (More info)
Track & Disable Option - Once your system location is determined, ESTSM will disable the system for further use.
Continuous Track Option - ESTSM will continuously track the location of your system once stolen.
There are more ESTSM services on the next page...
Privacy / Terms / Copyright

FIGURE 2a

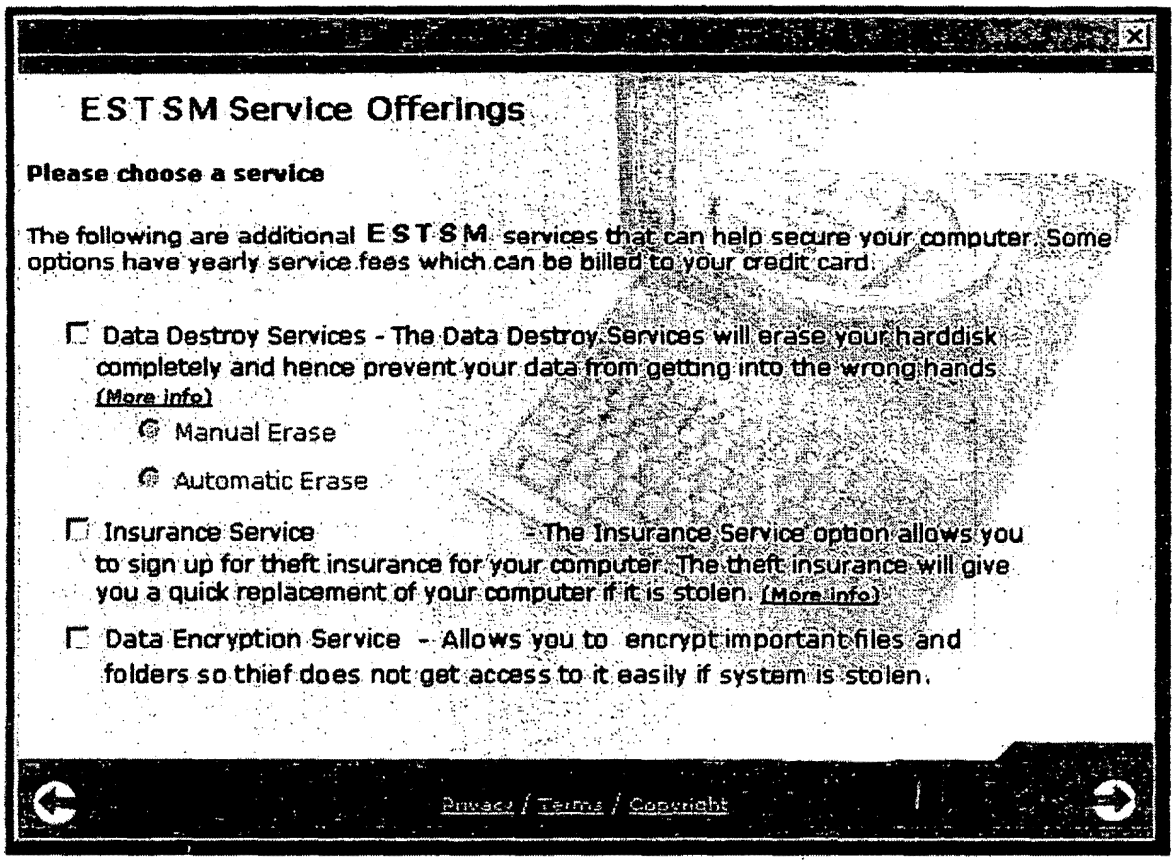

ESTSM Service Offerings
Please choose a service
The following are additional ESTSM services that can help secure your computer. Some options have yearly service fees which can be billed to your credit card.
Data Destroy Services - The Data Destroy Services will erase your harddisk completely and hence prevent your data from getting into the wrong hands (More info)
Manual Erase
Automatic Erase
Insurance Service - The Insurance Service option allows you to sign up for theft insurance for your computer. The theft insurance will give you a quick replacement of your computer if it is stolen. (More info)
Data Encryption Service - Allows you to encrypt important files and folders so thief does not get access to it easily if system is stolen.
Privacy / Terms / Copyright

FIGURE 2b

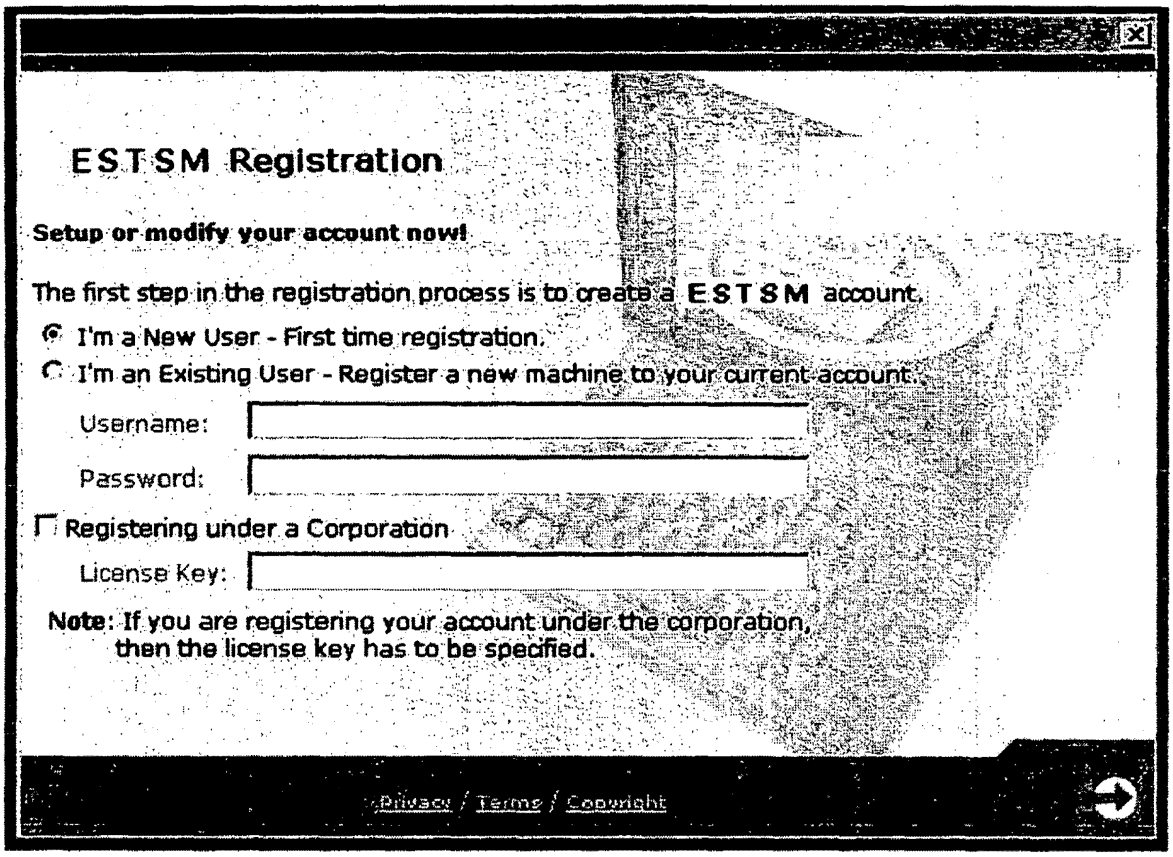

ESTSM Registration
Setup or modify your account now!
The first step in the registration process is to create a ESTSM account.
I'm a New User - First time registration.
I'm an Existing User - Register a new machine to your current account.
Username:
Password:
Registering under a Corporation
License Key:
Note: If you are registering your account under the corporation, then the license key has to be specified.
Privacy / Terms / Copyright

FIGURE 3a

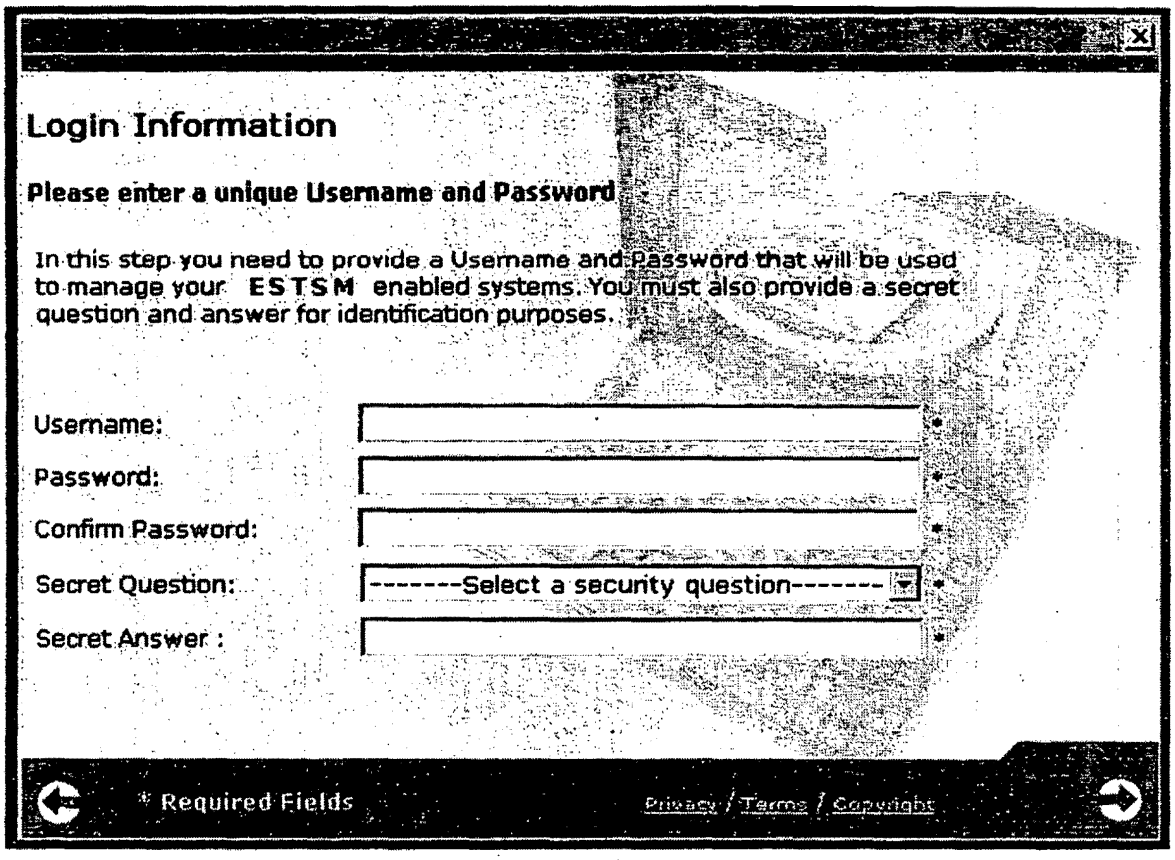

Login Information
Please enter a unique Username and Password
In this step you need to provide a Username and Password that will be used to manage your ESTSM enabled systems. You must also provide a secret question and answer for identification purposes.
Username:
Password:
Confirm Password:
Secret Question:
-------Select a security question-------
Secret Answer :
* Required Fields
Privacy / Terms / Copyright

FIGURE 3b

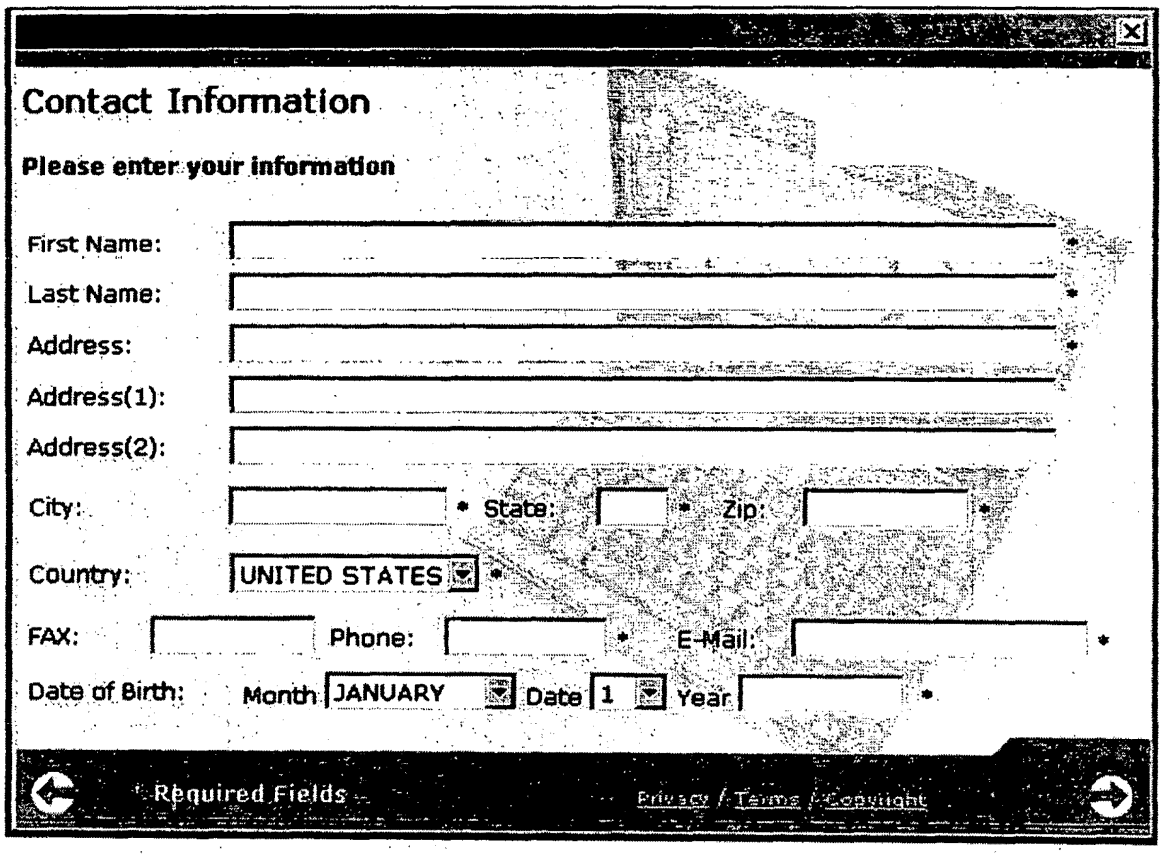

Contact Information
Please enter your information
First Name:
Last Name:
Address:
Address(1):
Address(2):
City:
State:
Zip:
Country:
UNITED STATES
FAX:
Phone:
E-Mail:
Date of Birth:
Month
JANUARY
Date
1
Year
Required Fields
Privacy / Terms / Copyright

FIGURE 3c

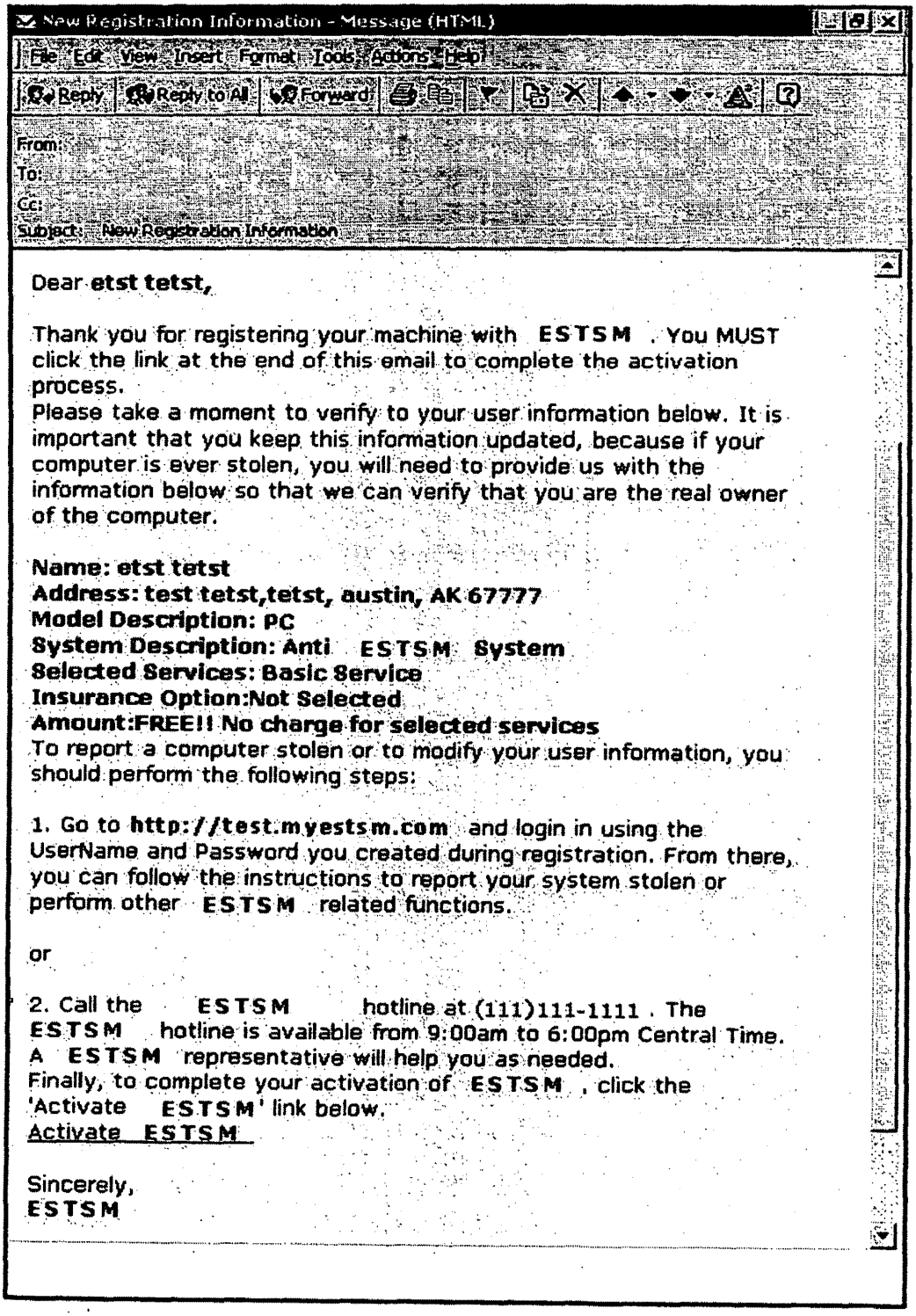

New Registration Information - Message (HTML)
File Edit View Insert Format Tools Actions Help
Reply Reply to All Forward
From:
To:
Cc:
Subject: New Registration Information
Dear etst tetst,
Thank you for registering your machine with ESTSM . You MUST click the link at the end of this email to complete the activation process.
Please take a moment to verify to your user information below. It is important that you keep this information updated, because if your computer is ever stolen, you will need to provide us with the information below so that we can verify that you are the real owner of the computer.
Name: etst tetst
Address: test tetst,tetst, austin, AK 67777
Model Description: PC
System Description: Anti ESTSM System
Selected Services: Basic Service
Insurance Option:Not Selected
Amount:FREE!! No charge for selected services
To report a computer stolen or to modify your user information, you should perform the following steps:
1. Go to http://test.myestsm.com and login in using the UserName and Password you created during registration. From there, you can follow the instructions to report your system stolen or perform other ESTSM related functions.
or
2. Call the ESTSM hotline at (111)111-1111 . The ESTSM hotline is available from 9:00am to 6:00pm Central Time. A ESTSM representative will help you as needed.
Finally, to complete your activation of ESTSM , click the 'Activate ESTSM' link below.
Activate ESTSM
Sincerely,
ESTSM

FIGURE 4

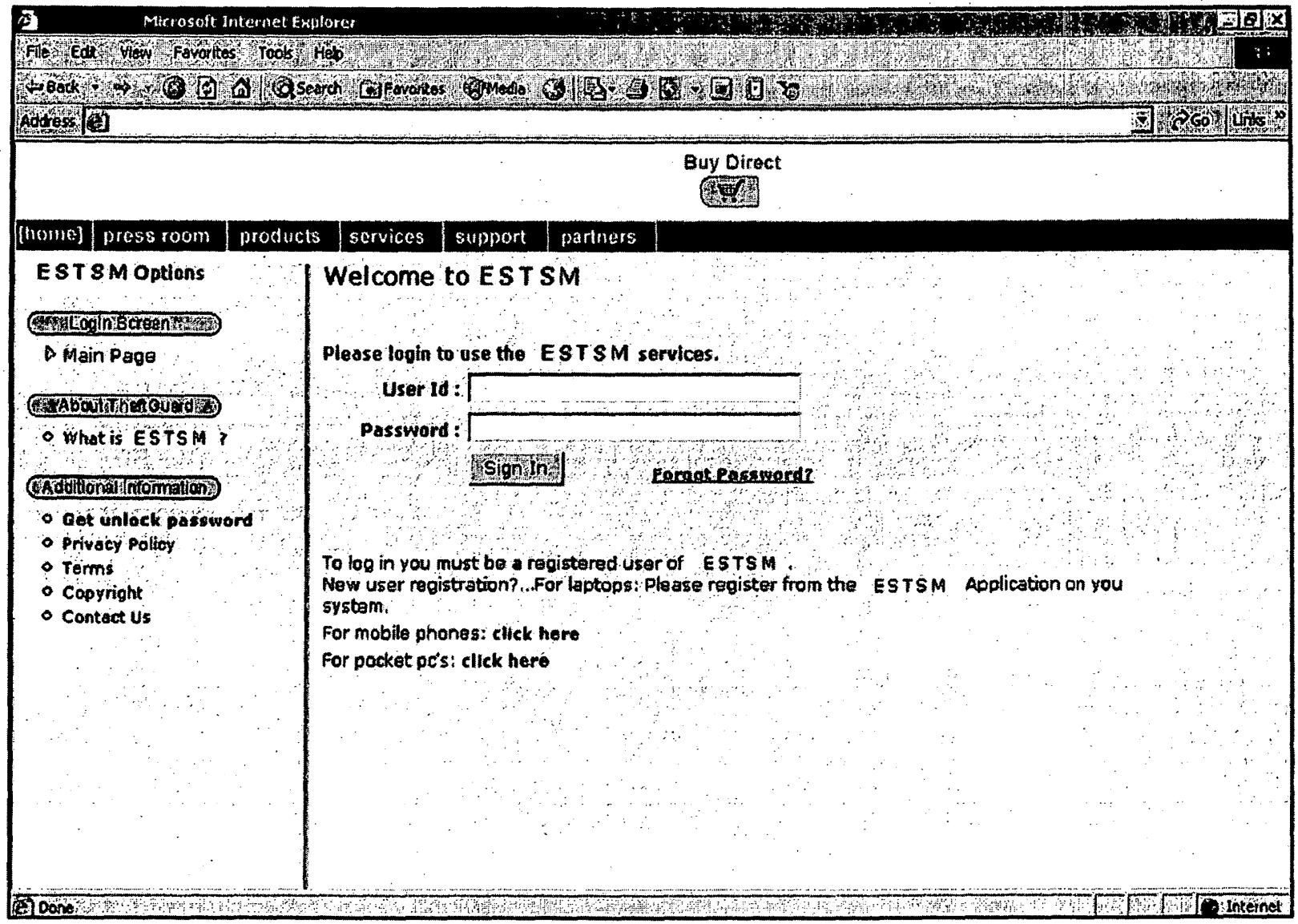

Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
Buy Direct
[home] press room products services support partners
ESTSM Options
Log In Screen
Main Page
About TheftGuard
What is ESTSM ?
Additional Information
Get unlock password
Privacy Policy
Terms
Copyright
Contact Us
Welcome to ESTSM
Please login to use the ESTSM services.
User Id :
Password :
Sign In
Forgot Password?
To log in you must be a registered user of ESTSM .
New user registration?...For laptops: Please register from the ESTSM Application on you system.
For mobile phones: click here
For pocket pc's: click here
Done
Internet

FIGURE 5

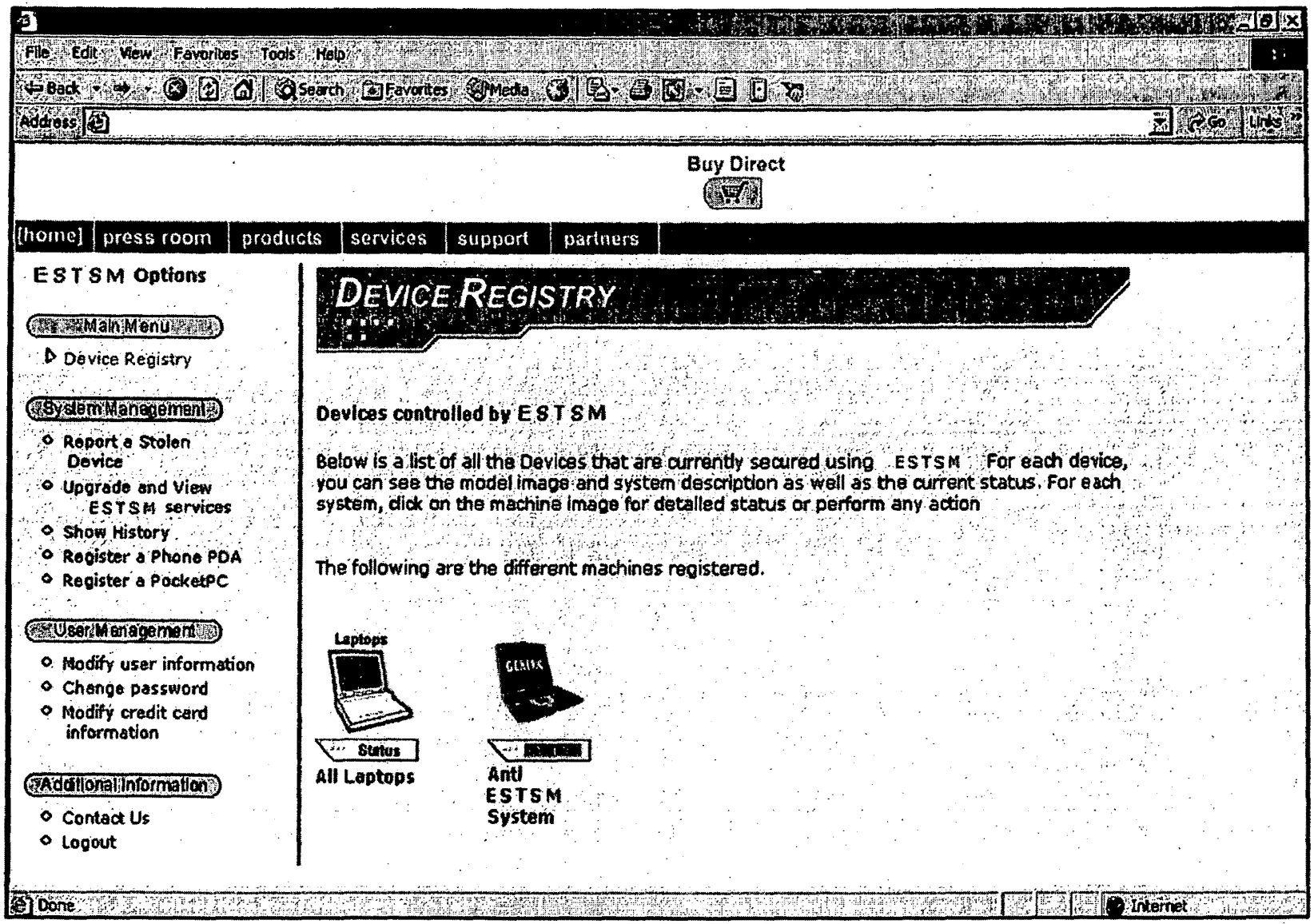


FIGURE 6

DELL EXHIBIT 1002
Page 78 of 659

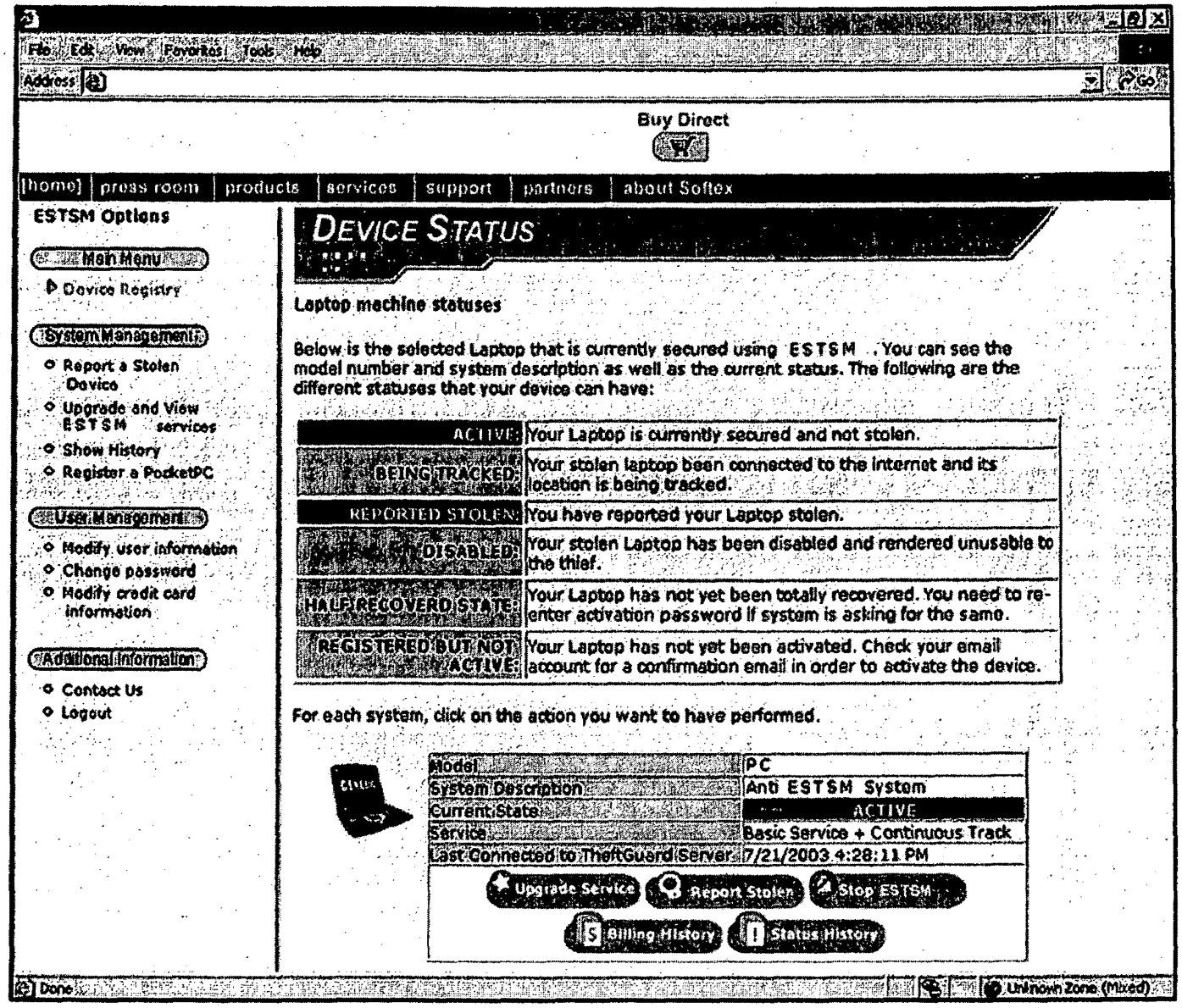


FIGURE 7

DELL EXHIBIT 1002
Page 79 of 659

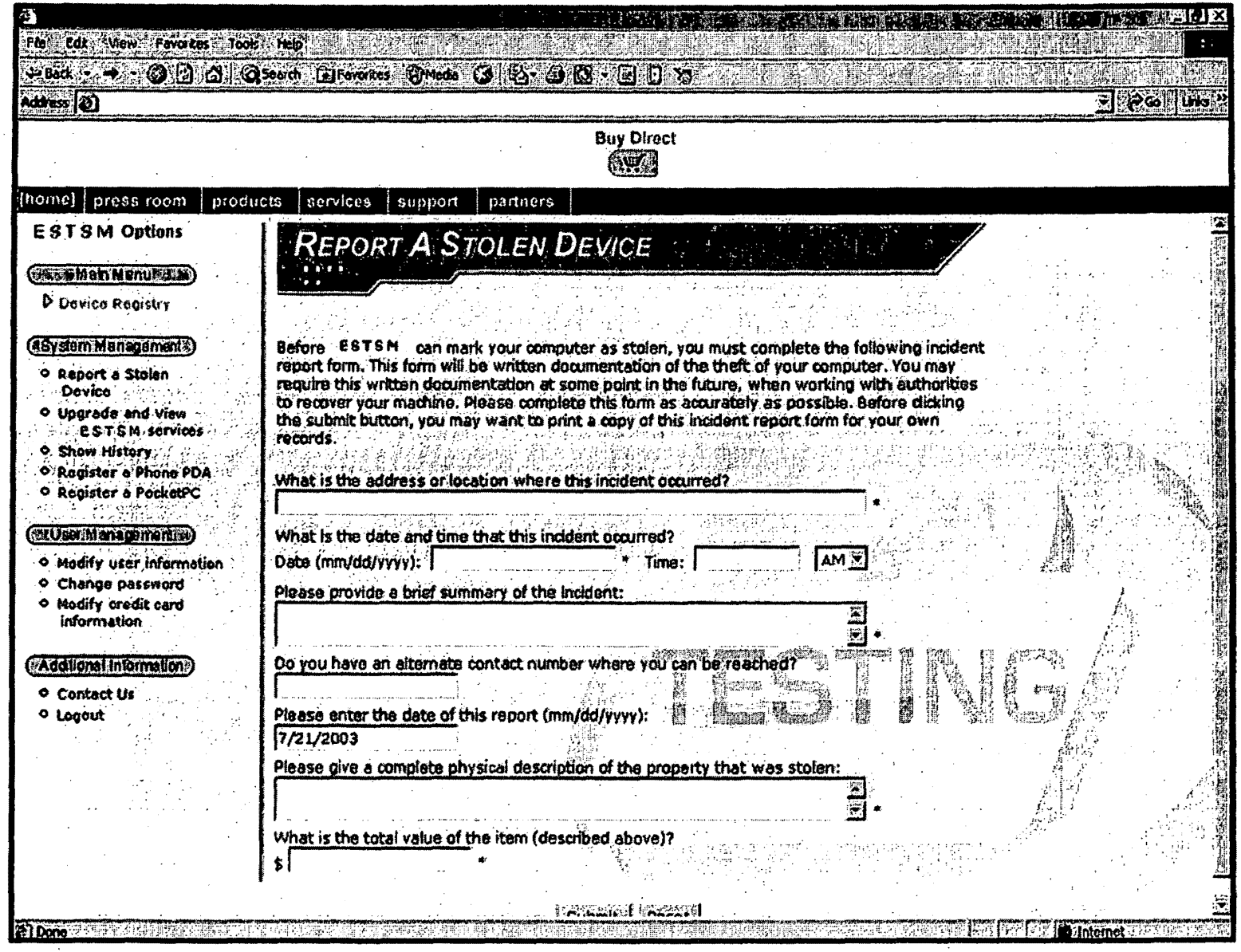

File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Buy Direct
[home] press room products services support partners
ESTSM Options
Main Menu
Device Registry
System Management
Report a Stolen Device
Upgrade and View ESTSM services
Show History
Register a Phone PDA
Register a PocketPC
User Management
Modify user information
Change password
Modify credit card information
Additional Information
Contact Us
Logout
REPORT A STOLEN DEVICE
Before ESTSM can mark your computer as stolen, you must complete the following incident report form. This form will be written documentation of the theft of your computer. You may require this written documentation at some point in the future, when working with authorities to recover your machine. Please complete this form as accurately as possible. Before clicking the submit button, you may want to print a copy of this incident report form for your own records.
What is the address or location where this incident occurred?
What is the date and time that this incident occurred?
Date (mm/dd/yyyy):
Time:
AM
Please provide a brief summary of the incident:
Do you have an alternate contact number where you can be reached?
Please enter the date of this report (mm/dd/yyyy):
7/21/2003
Please give a complete physical description of the property that was stolen:
What is the total value of the item (described above)?
$
TESTING
Done
Internet

FIGURE 8a

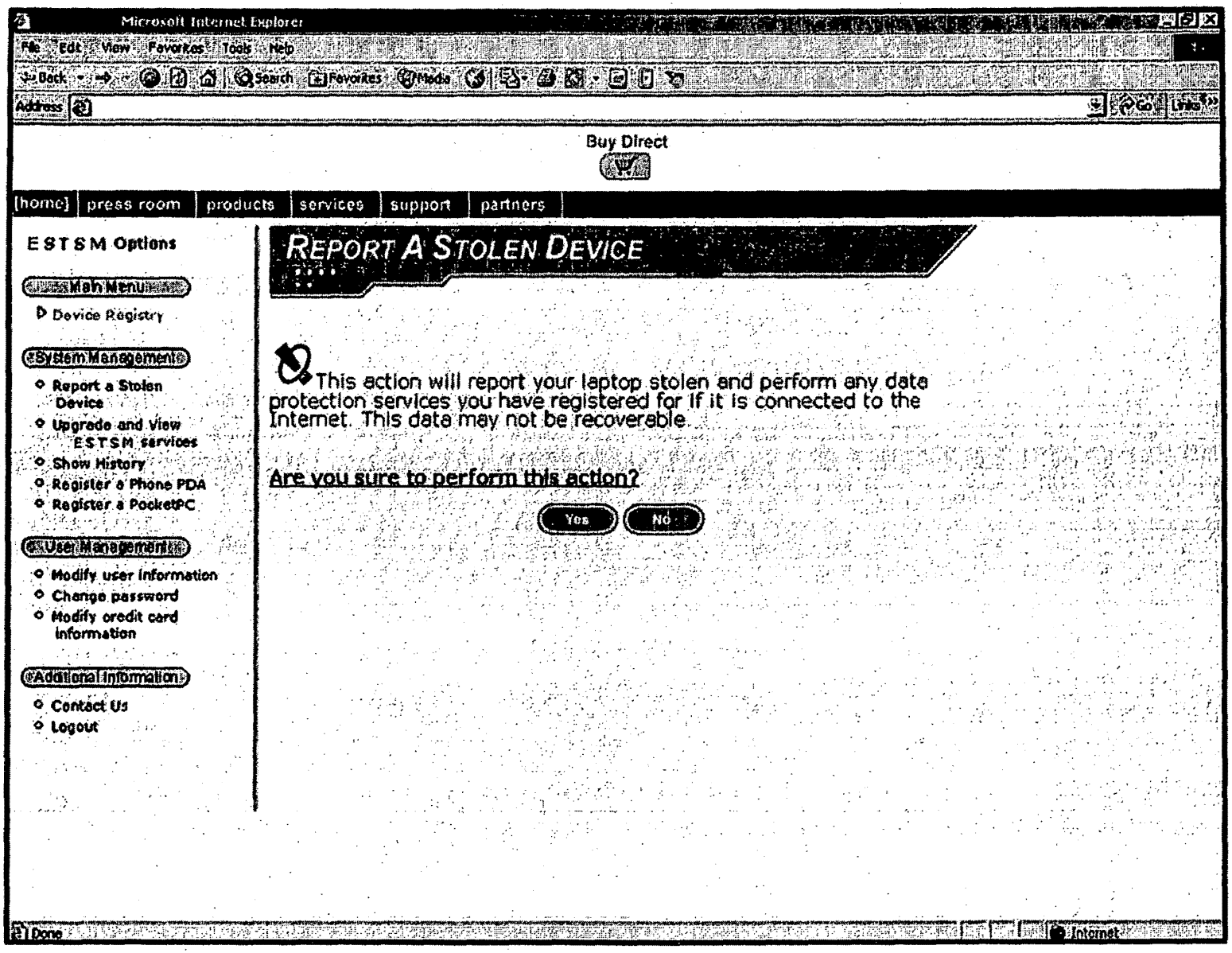


FIGURE 8b

DELL EXHIBIT 1002
Page 81 of 659

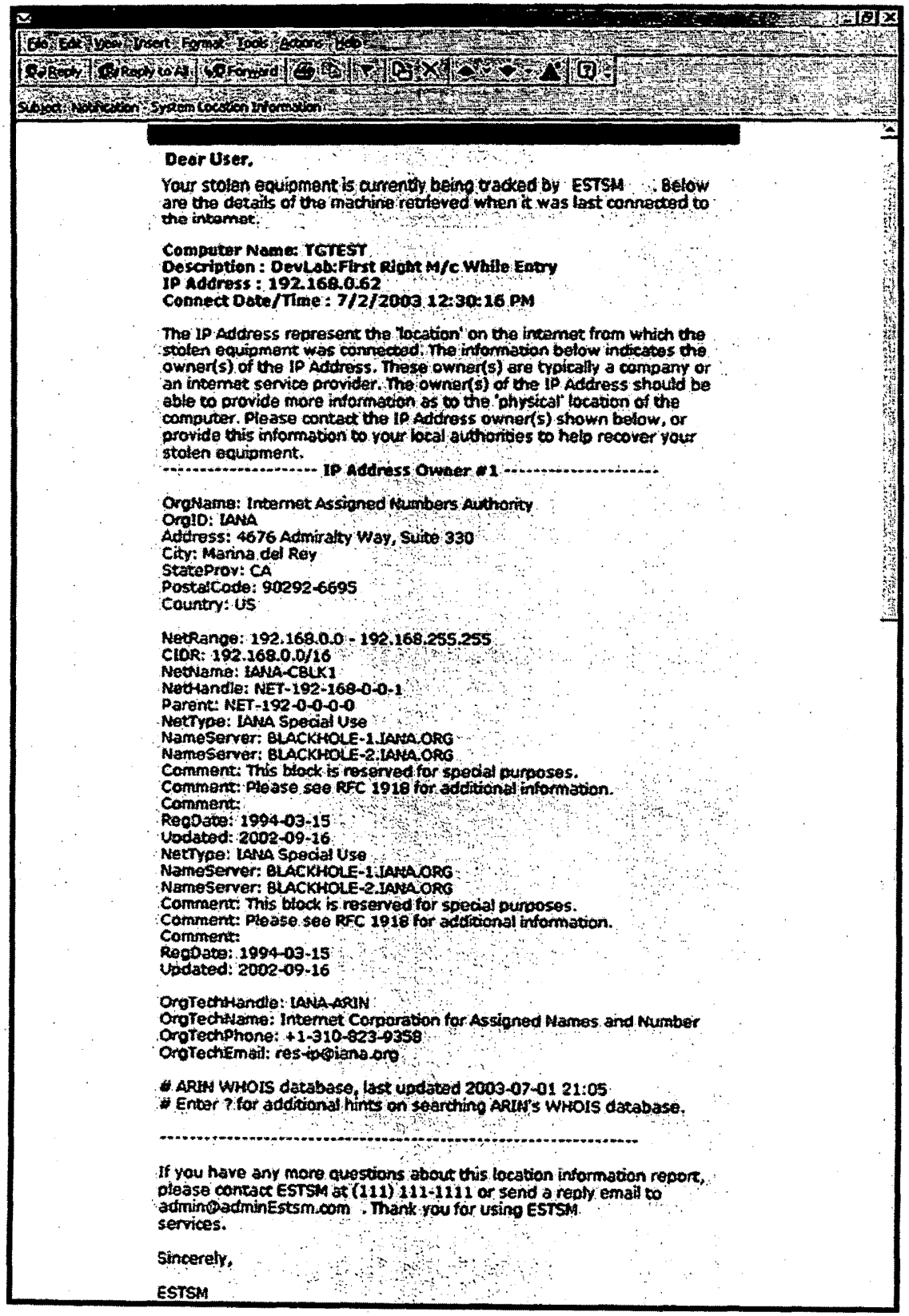

File Edit View Insert Format Tools Actions Help
Reply Reply to All Forward
Subject: Notification - System Location Information
Dear User,
Your stolen equipment is currently being tracked by ESTSM . Below are the details of the machine retrieved when it was last connected to the internet.
Computer Name: TGTEST
Description : DevLab:First Right M/c While Entry
IP Address : 192.168.0.62
Connect Date/Time : 7/2/2003 12:30:16 PM
The IP Address represent the 'location' on the internet from which the stolen equipment was connected. The information below indicates the owner(s) of the IP Address. These owner(s) are typically a company or an internet service provider. The owner(s) of the IP Address should be able to provide more information as to the 'physical' location of the computer. Please contact the IP Address owner(s) shown below, or provide this information to your local authorities to help recover your stolen equipment.
---------- IP Address Owner #1 ----------
OrgName: Internet Assigned Numbers Authority
OrgID: IANA
Address: 4676 Admiralty Way, Suite 330
City: Marina del Rey
StateProv: CA
PostalCode: 90292-6695
Country: US
NetRange: 192.168.0.0 - 192.168.255.255
CIDR: 192.168.0.0/16
NetName: IANA-CBLK1
NetHandle: NET-192-168-0-0-1
Parent: NET-192-0-0-0-0
NetType: IANA Special Use
NameServer: BLACKHOLE-1.IANA.ORG
NameServer: BLACKHOLE-2.IANA.ORG
Comment: This block is reserved for special purposes.
Comment: Please see RFC 1918 for additional information.
Comment:
RegDate: 1994-03-15
Updated: 2002-09-16
NetType: IANA Special Use
NameServer: BLACKHOLE-1.IANA.ORG
NameServer: BLACKHOLE-2.IANA.ORG
Comment: This block is reserved for special purposes.
Comment: Please see RFC 1918 for additional information.
Comment:
RegDate: 1994-03-15
Updated: 2002-09-16
OrgTechHandle: IANA-ARIN
OrgTechName: Internet Corporation for Assigned Names and Number
OrgTechPhone: +1-310-823-9358
OrgTechEmail: res-ip@iana.org
ARIN WHOIS database, last updated 2003-07-01 21:05
Enter ? for additional hints on searching ARIN's WHOIS database.
If you have any more questions about this location information report, please contact ESTSM at (111) 111-1111 or send a reply email to admin@adminEstsm.com . Thank you for using ESTSM services.
Sincerely,
ESTSM

FIGURE 9

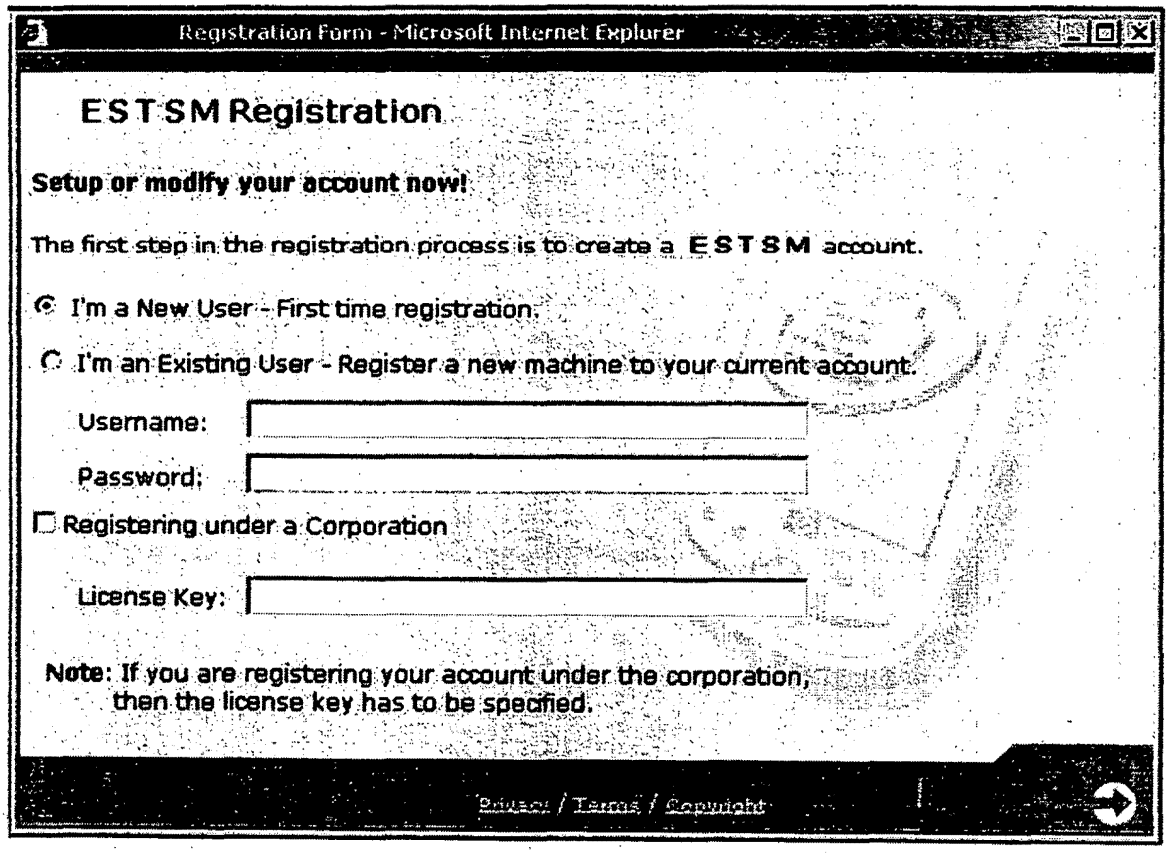

Registration Form - Microsoft Internet Explorer
ESTSM Registration
Setup or modify your account now!
The first step in the registration process is to create a ESTSM account.
I'm a New User - First time registration.
I'm an Existing User - Register a new machine to your current account.
Username:
Password:
Registering under a Corporation
License Key:
Note: If you are registering your account under the corporation, then the license key has to be specified.
Privacy / Terms / Copyright

FIGURE 10

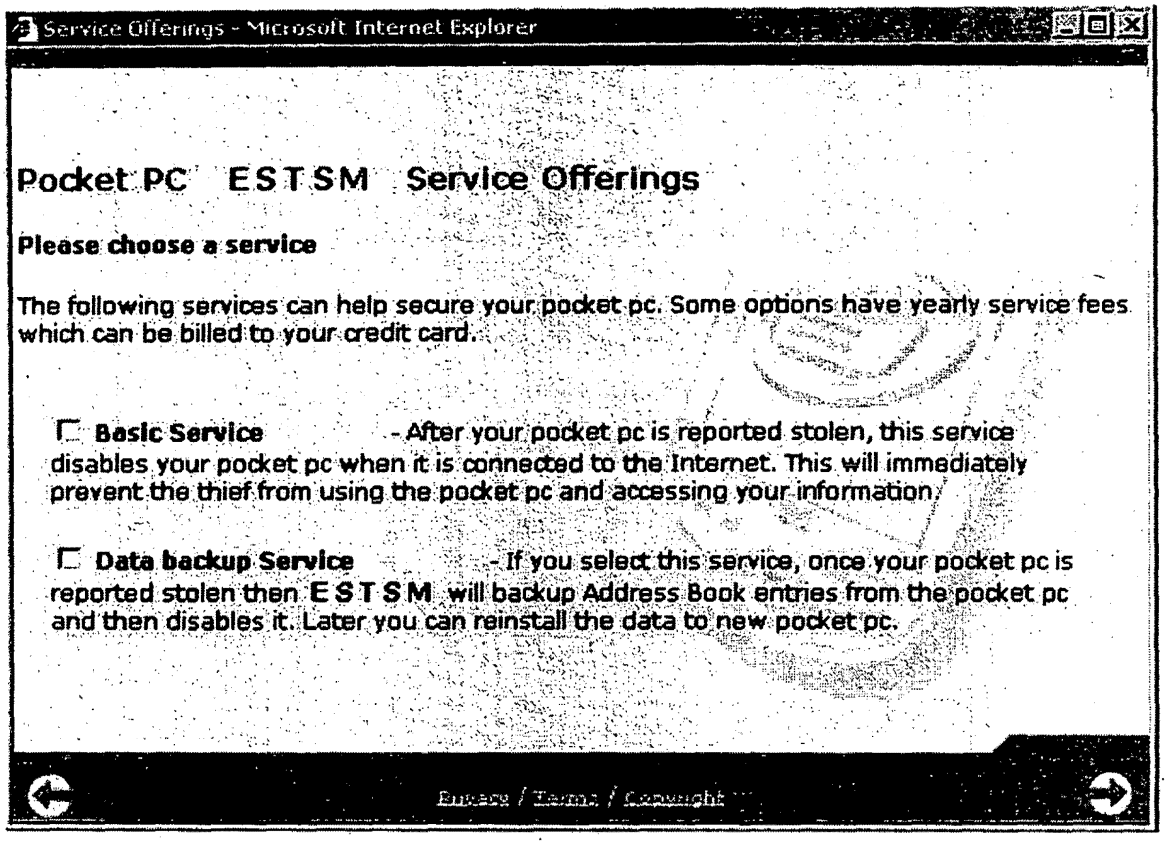

Service Offerings - Microsoft Internet Explorer
Pocket PC ESTSM Service Offerings
Please choose a service
The following services can help secure your pocket pc. Some options have yearly service fees which can be billed to your credit card.
Basic Service - After your pocket pc is reported stolen, this service disables your pocket pc when it is connected to the Internet. This will immediately prevent the thief from using the pocket pc and accessing your information.
Data backup Service - If you select this service, once your pocket pc is reported stolen then ESTSM will backup Address Book entries from the pocket pc and then disables it. Later you can reinstall the data to new pocket pc.
Privacy / Terms / Copyright

FIGURE 11

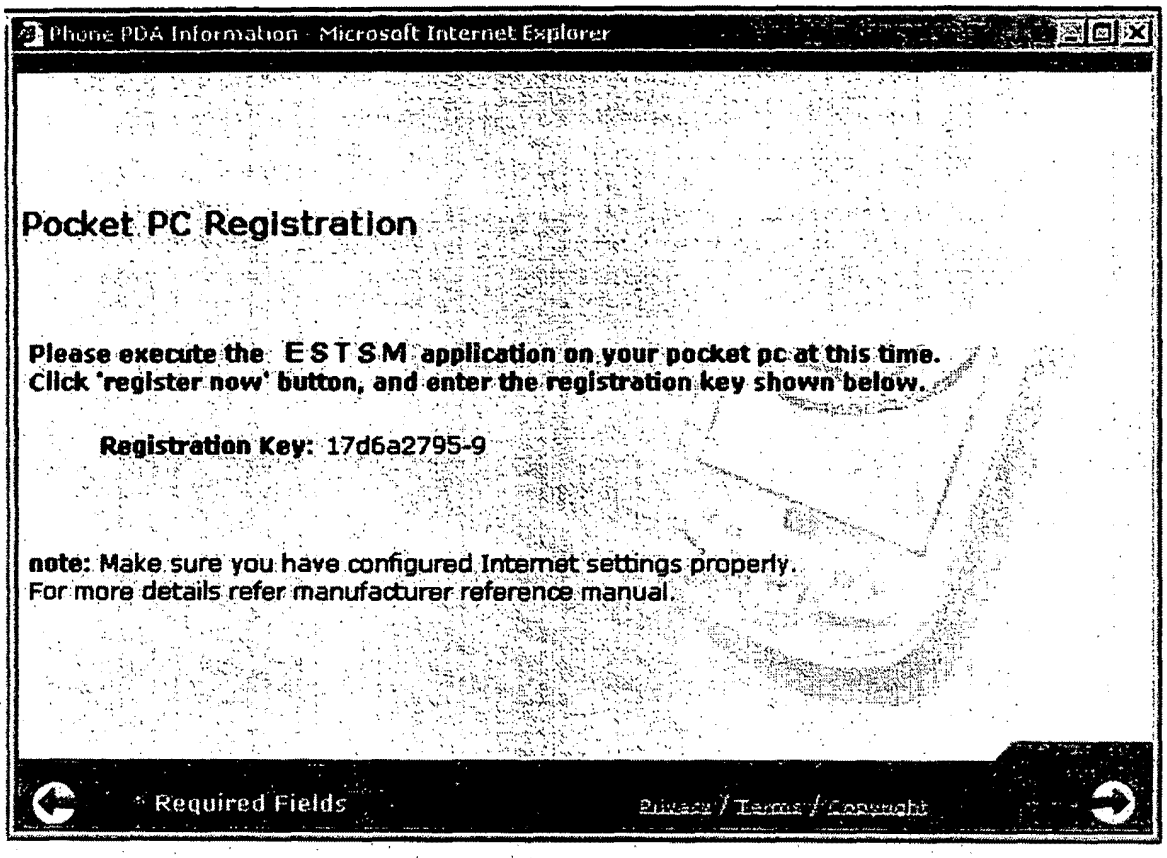

Phone PDA Information - Microsoft Internet Explorer
Pocket PC Registration
Please execute the ESTSM application on your pocket pc at this time.
Click 'register now' button, and enter the registration key shown below.
Registration Key: 17d6a2795-9
note: Make sure you have configured Internet settings properly.
For more details refer manufacturer reference manual.
* Required Fields
Privacy / Terms / Copyright

FIGURE 12

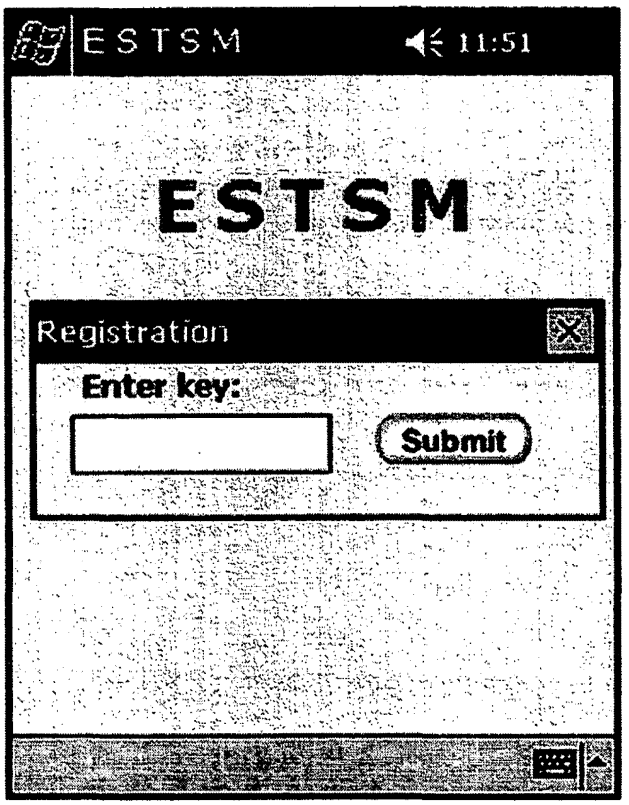


FIGURE 13

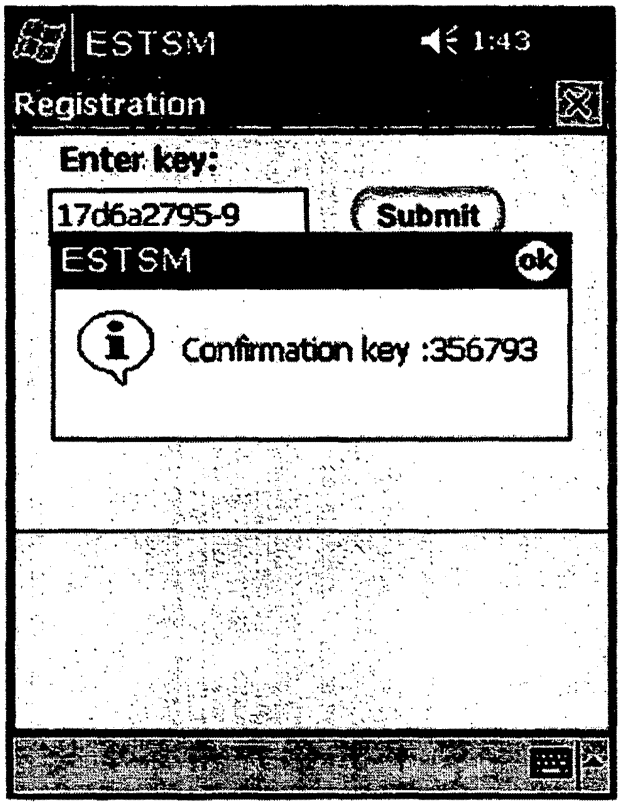

ESTSM
1:43
Registration
Enter key:
17d6a2795-9
Submit
ESTSM
ok
Confirmation key :356793

FIGURE 14

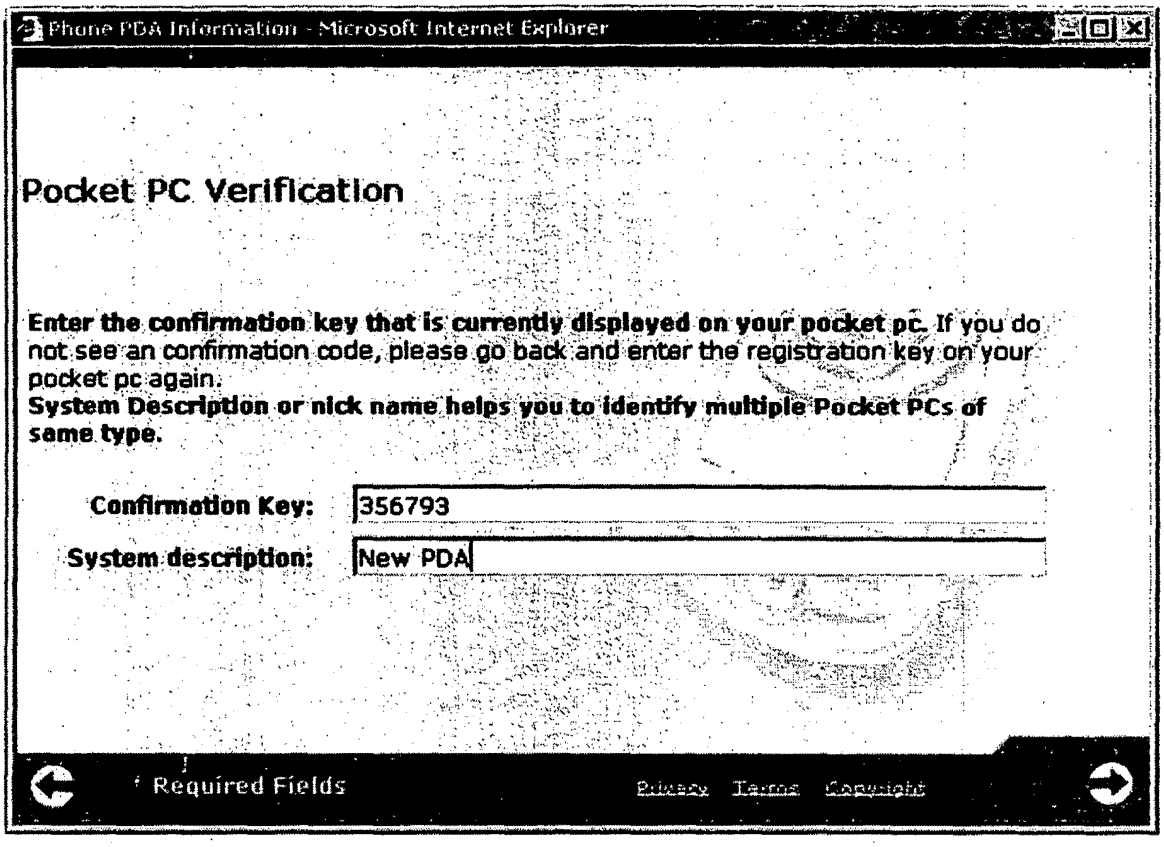

Phone PDA Information - Microsoft Internet Explorer
Pocket PC Verification
Enter the confirmation key that is currently displayed on your pocket pc. If you do not see an confirmation code, please go back and enter the registration key on your pocket pc again.
System Description or nick name helps you to identify multiple Pocket PCs of same type.
Confirmation Key:
356793
System description:
New PDA
* Required Fields
Privacy Terms Copyright

FIGURE 15

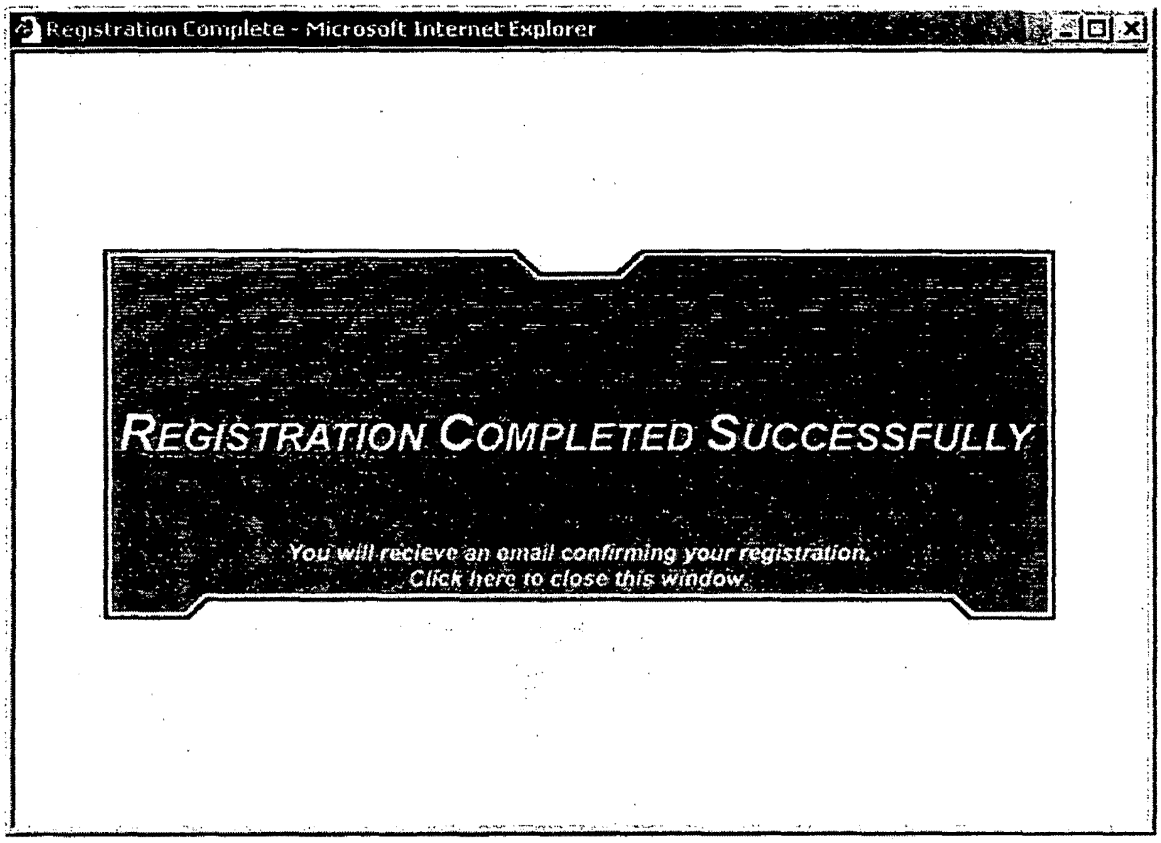

Registration Complete - Microsoft Internet Explorer
REGISTRATION COMPLETED SUCCESSFULLY
You will recieve an email confirming your registration.
Click here to close this window.

FIGURE 16

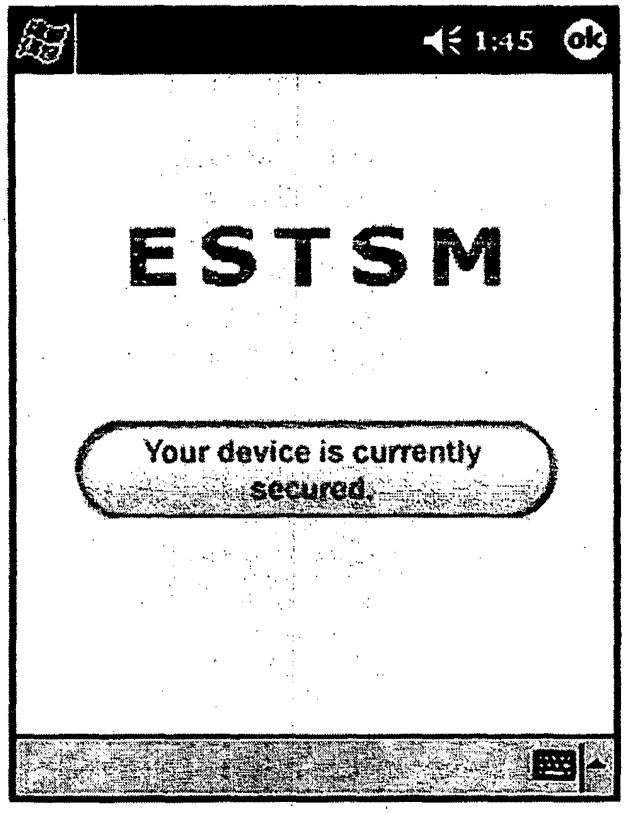


FIGURE 17

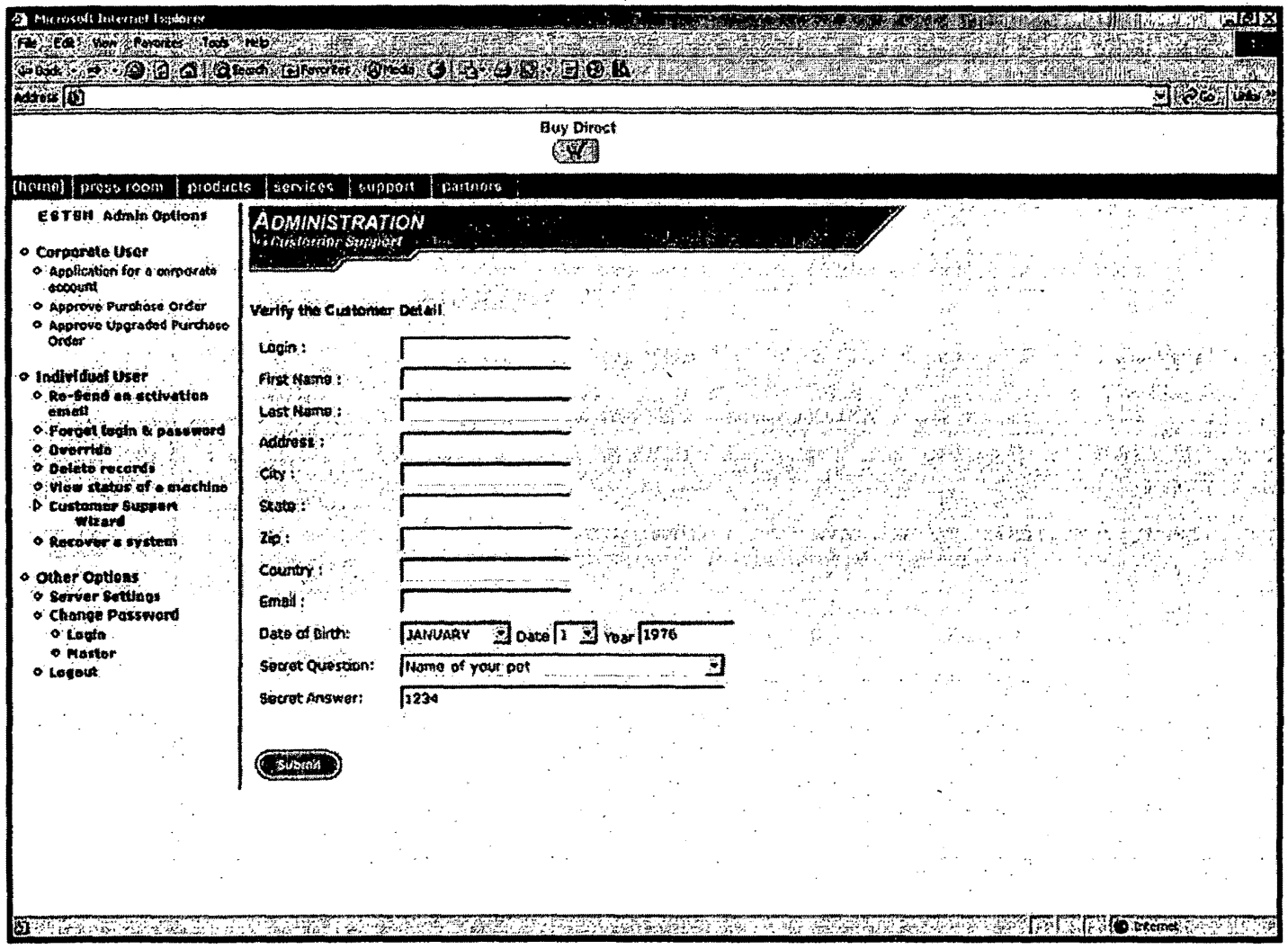


FIGURE 18

DELL EXHIBIT 1002
Page 91 of 659

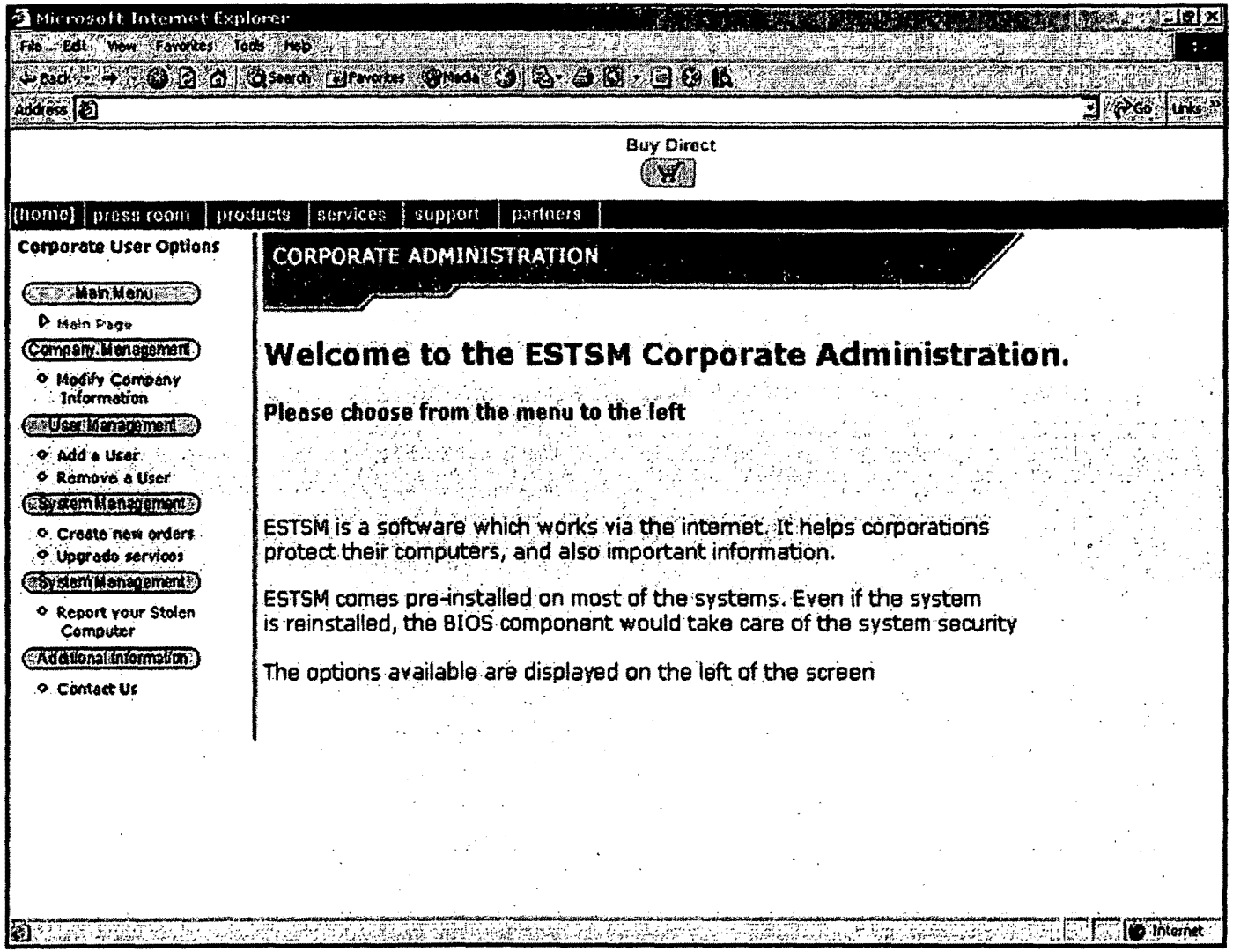


FIGURE 19

DELL EXHIBIT 1002
Page 92 of 659

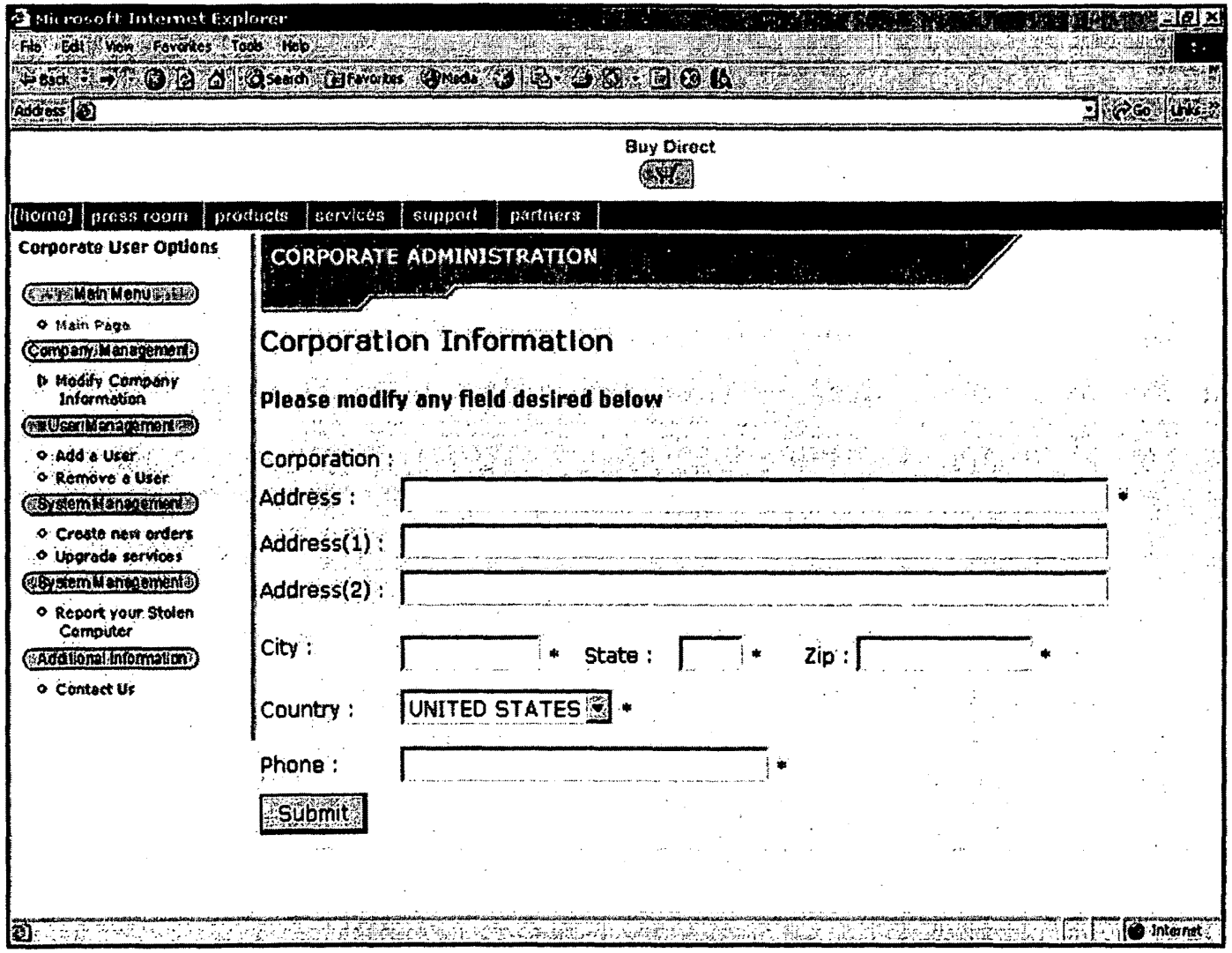


FIGURE 20

DELL EXHIBIT 1002
Page 93 of 659

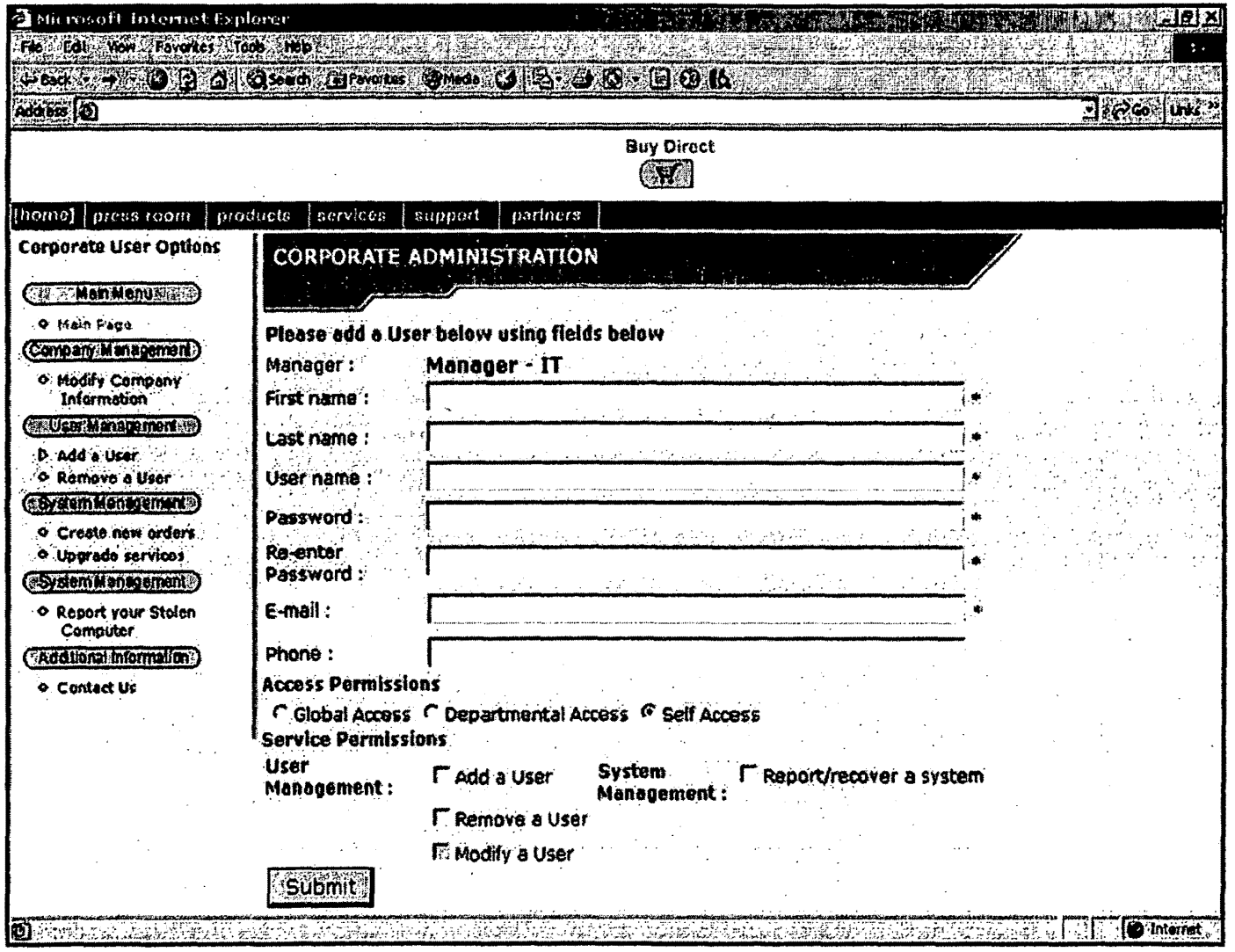

Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
Buy Direct
home | press room | products | services | support | partners
Corporate User Options
Main Menu
Main Page
Company Management
Modify Company Information
User Management
Add a User
Remove a User
System Management
Create new orders
Upgrade services
System Management
Report your Stolen Computer
Additional Information
Contact Us
CORPORATE ADMINISTRATION
Please add a User below using fields below
Manager :
Manager - IT
First name :
Last name :
User name :
Password :
Re-enter Password :
E-mail :
Phone :
Access Permissions
Global Access
Departmental Access
Self Access
Service Permissions
User Management :
Add a User
Remove a User
Modify a User
System Management :
Report/recover a system
Submit
Internet

FIGURE 21

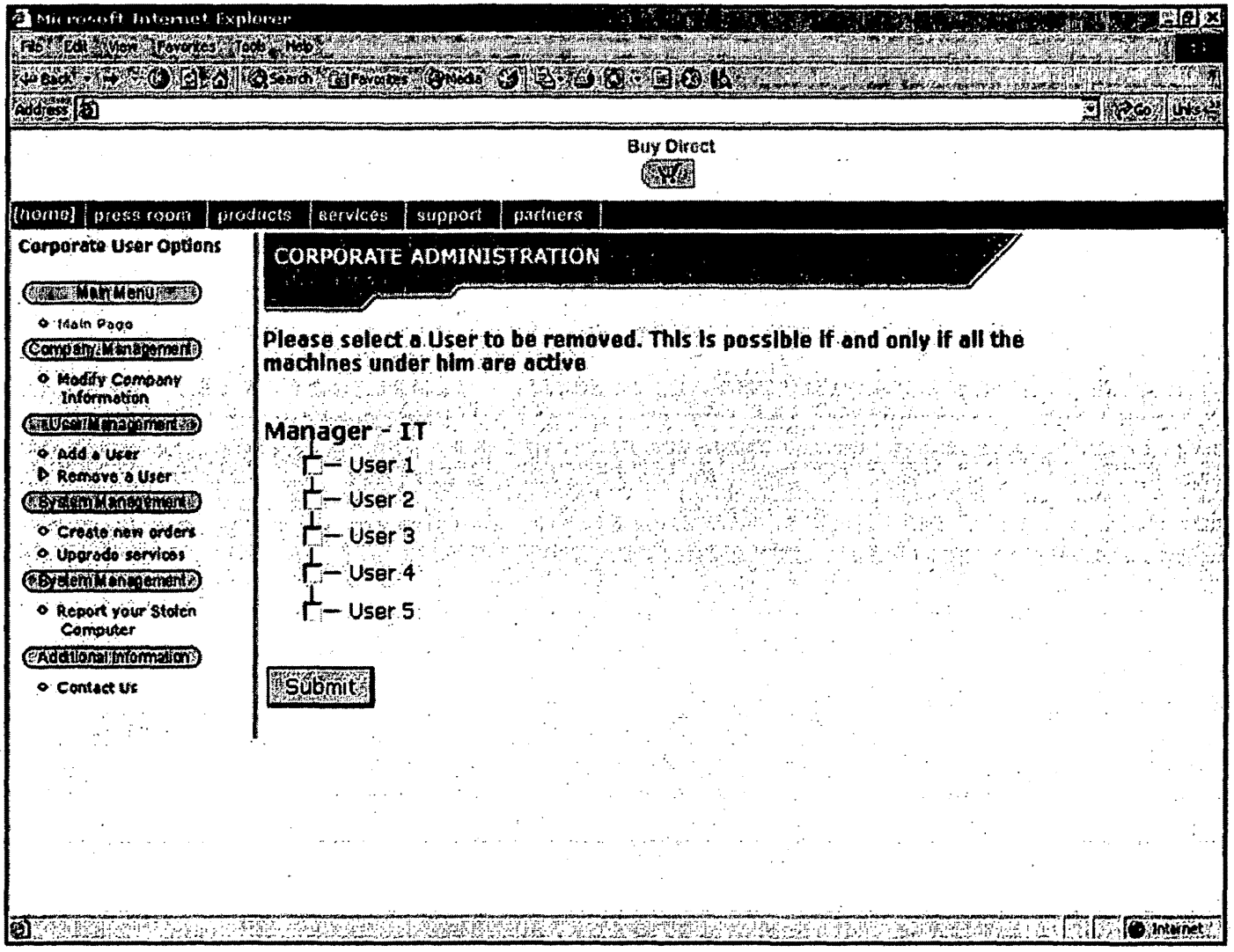


FIGURE 22

DELL EXHIBIT 1002
Page 95 of 659

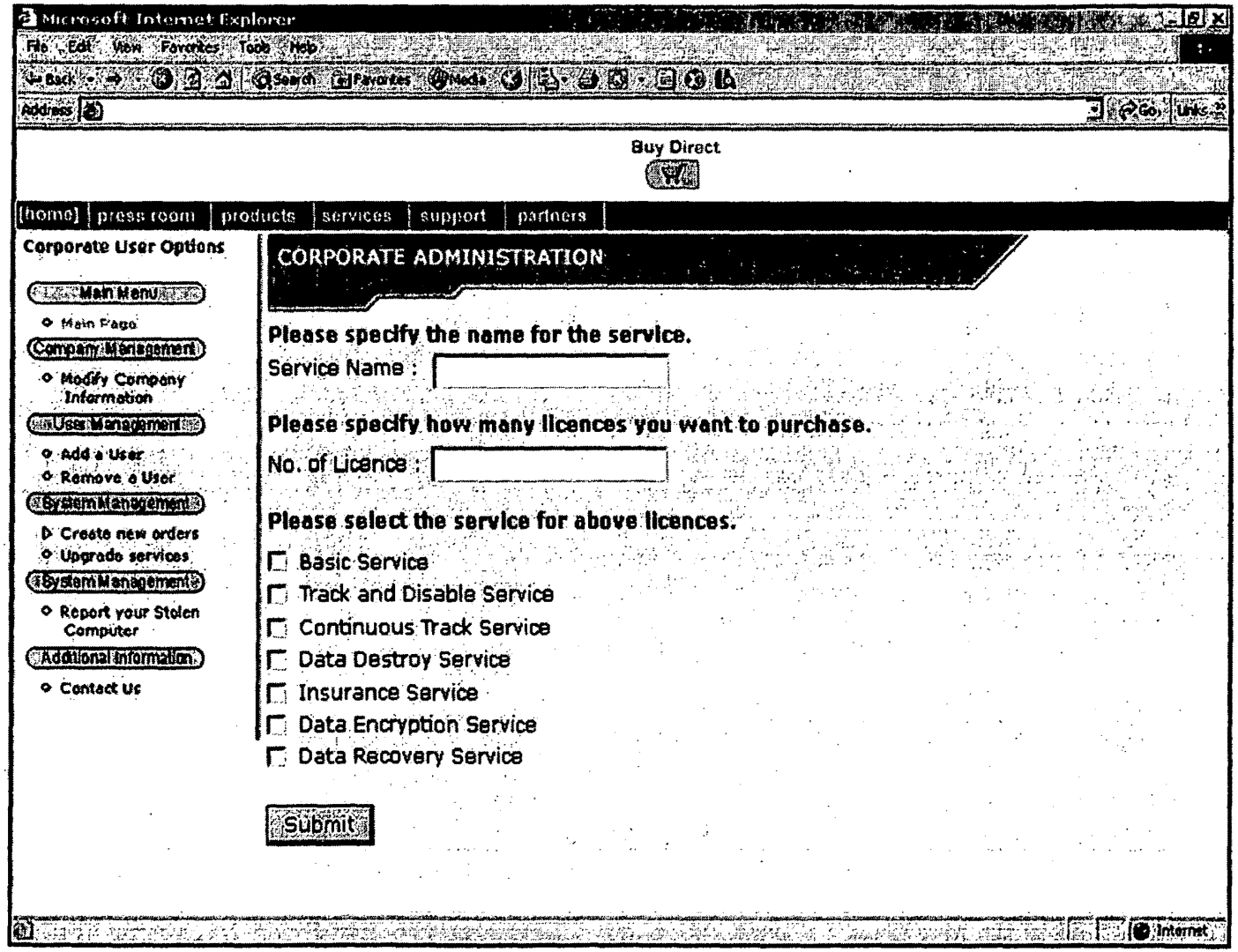


FIGURE 23

DELL EXHIBIT 1002
Page 96 of 659

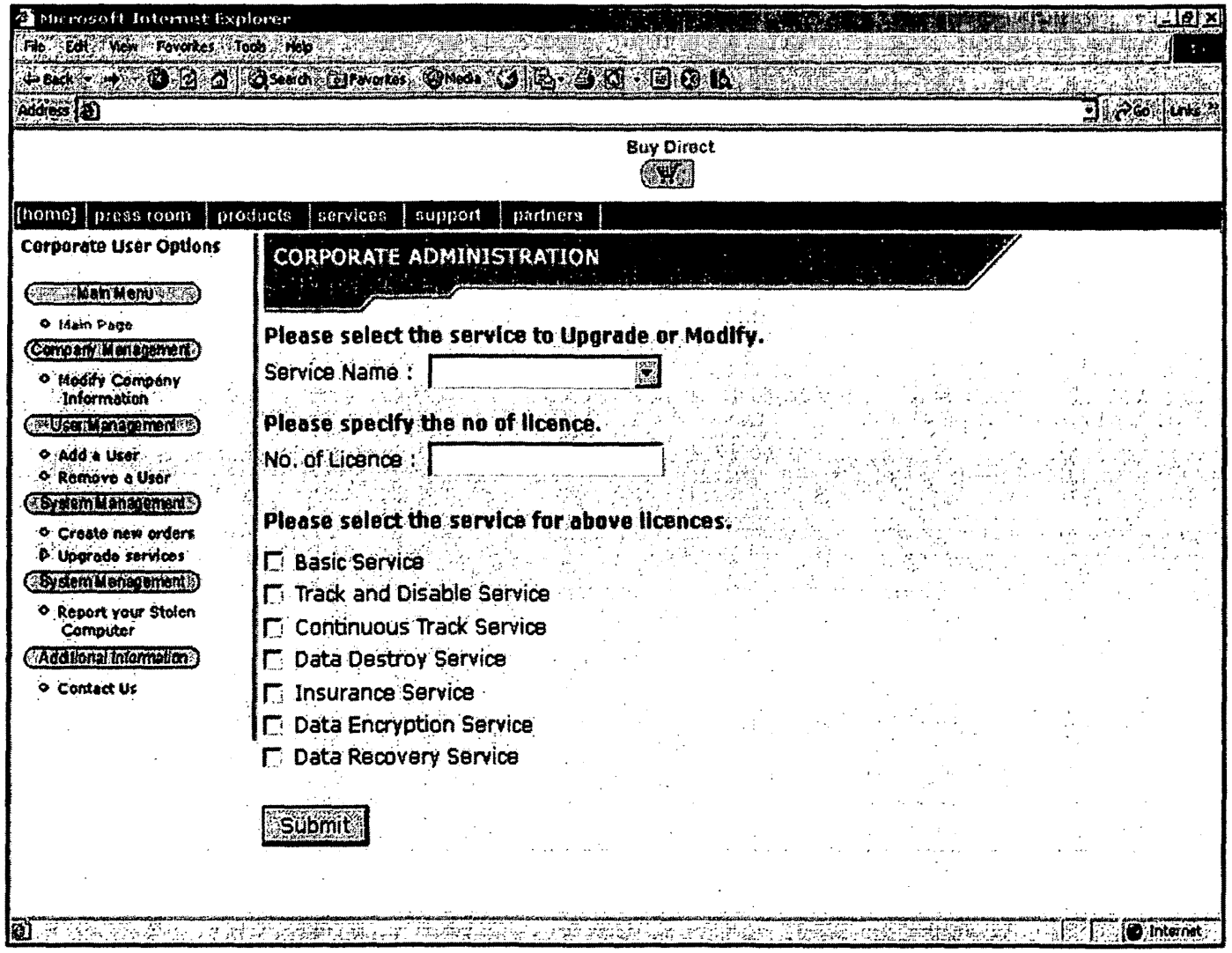


FIGURE 24

DELL EXHIBIT 1002
Page 97 of 659

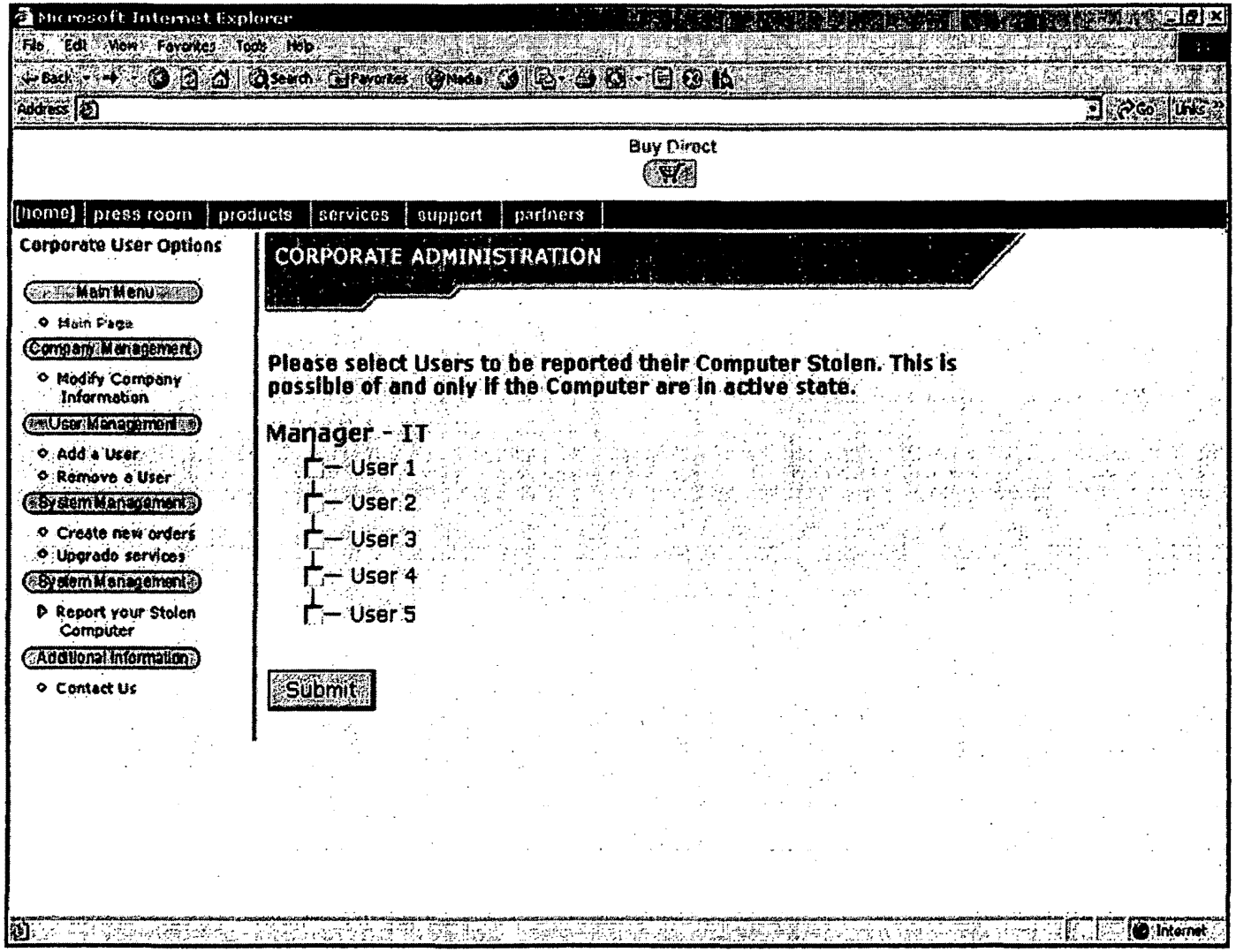

Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
Buy Direct
[home] press room products services support partners
Corporate User Options
Main Menu
Main Page
Company Management
Modify Company Information
User Management
Add a User
Remove a User
System Management
Create new orders
Upgrade services
System Management
Report your Stolen Computer
Additional Information
Contact Us
CORPORATE ADMINISTRATION
Please select Users to be reported their Computer Stolen. This is possible of and only if the Computer are in active state.
Manager - IT
User 1
User 2
User 3
User 4
User 5
Submit
Internet

FIGURE 25

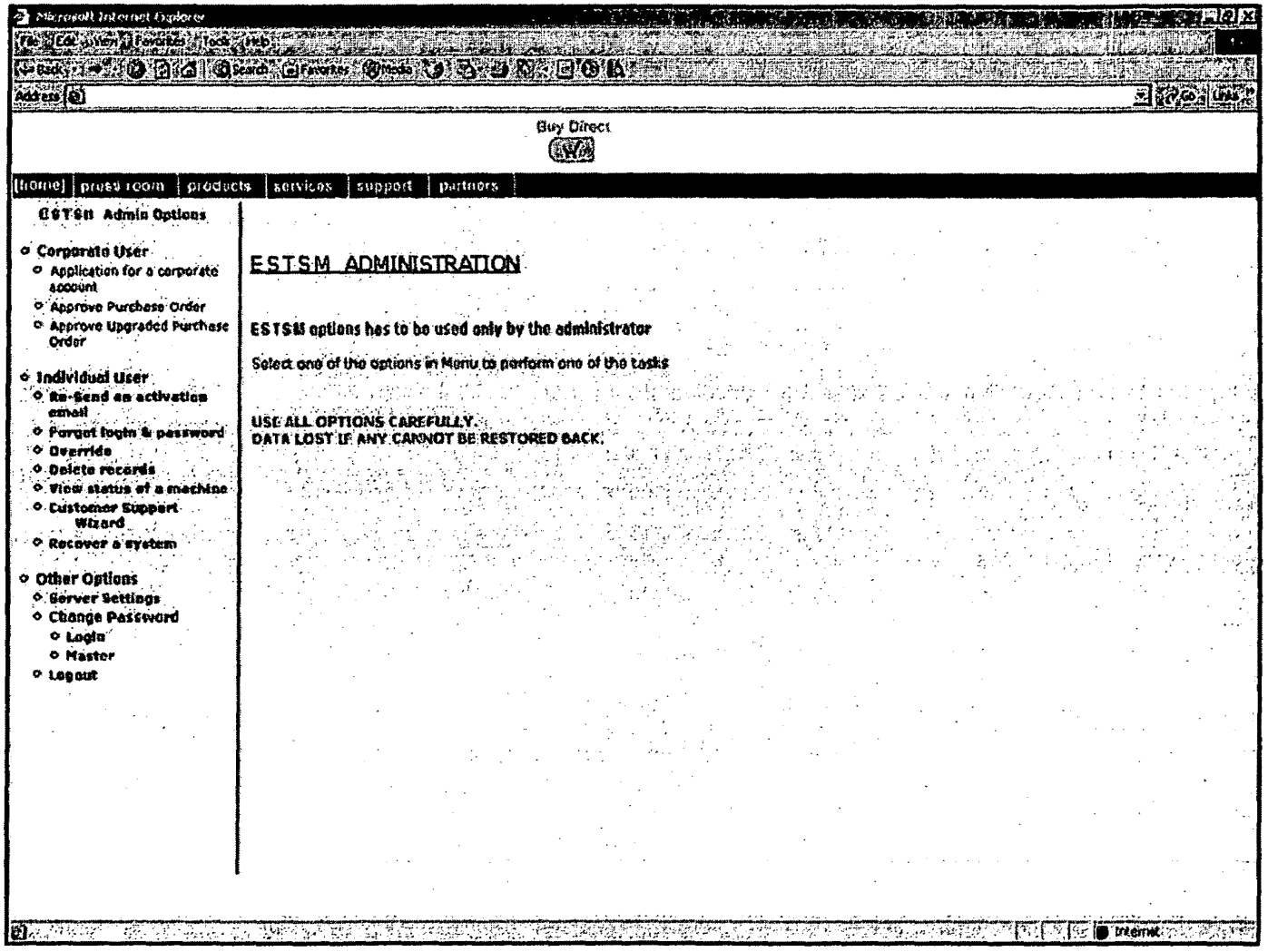


FIGURE 26

DELL EXHIBIT 1002
Page 99 of 659

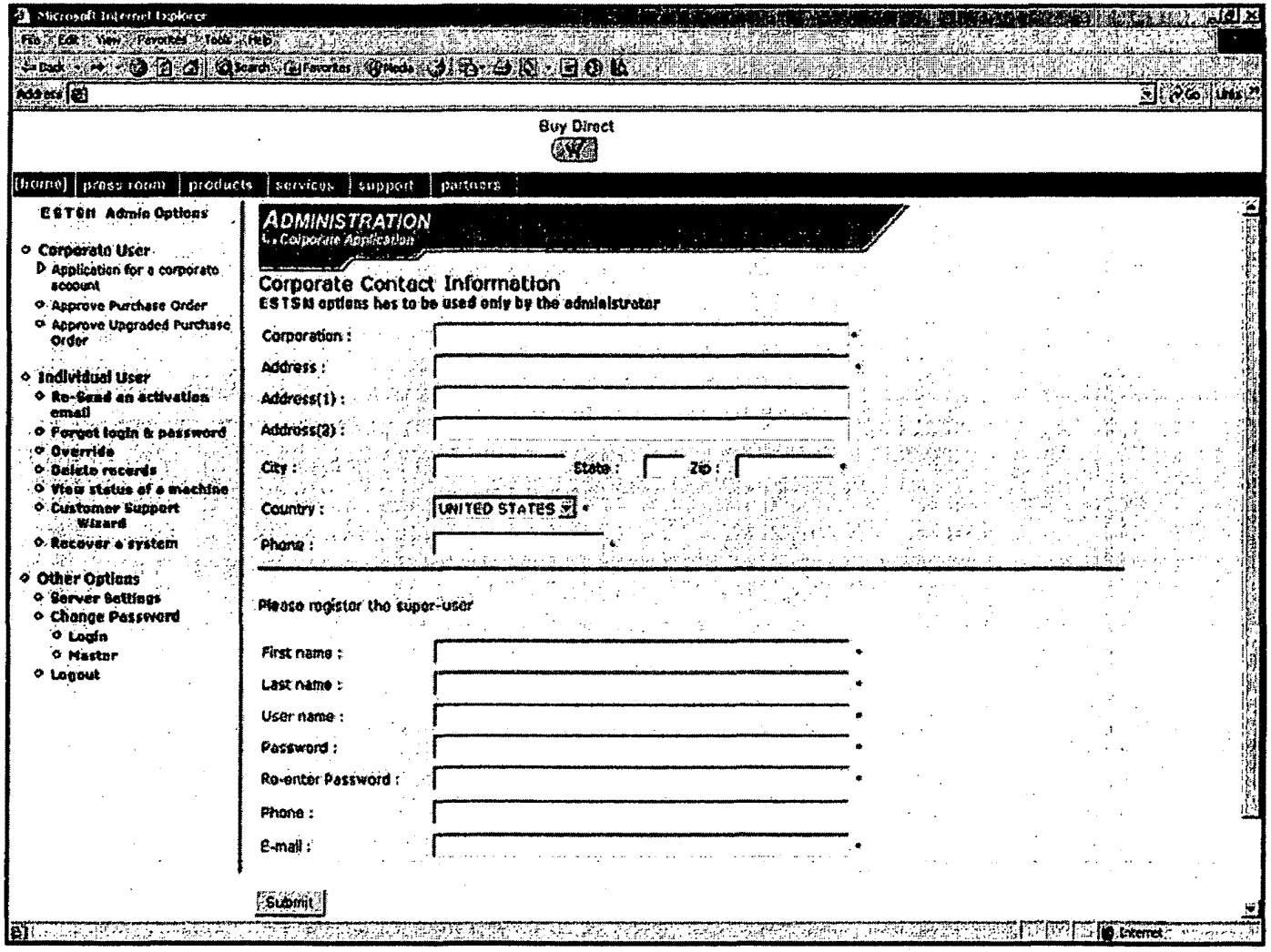


FIGURE 27

DELL EXHIBIT 1002
Page 100 of 659

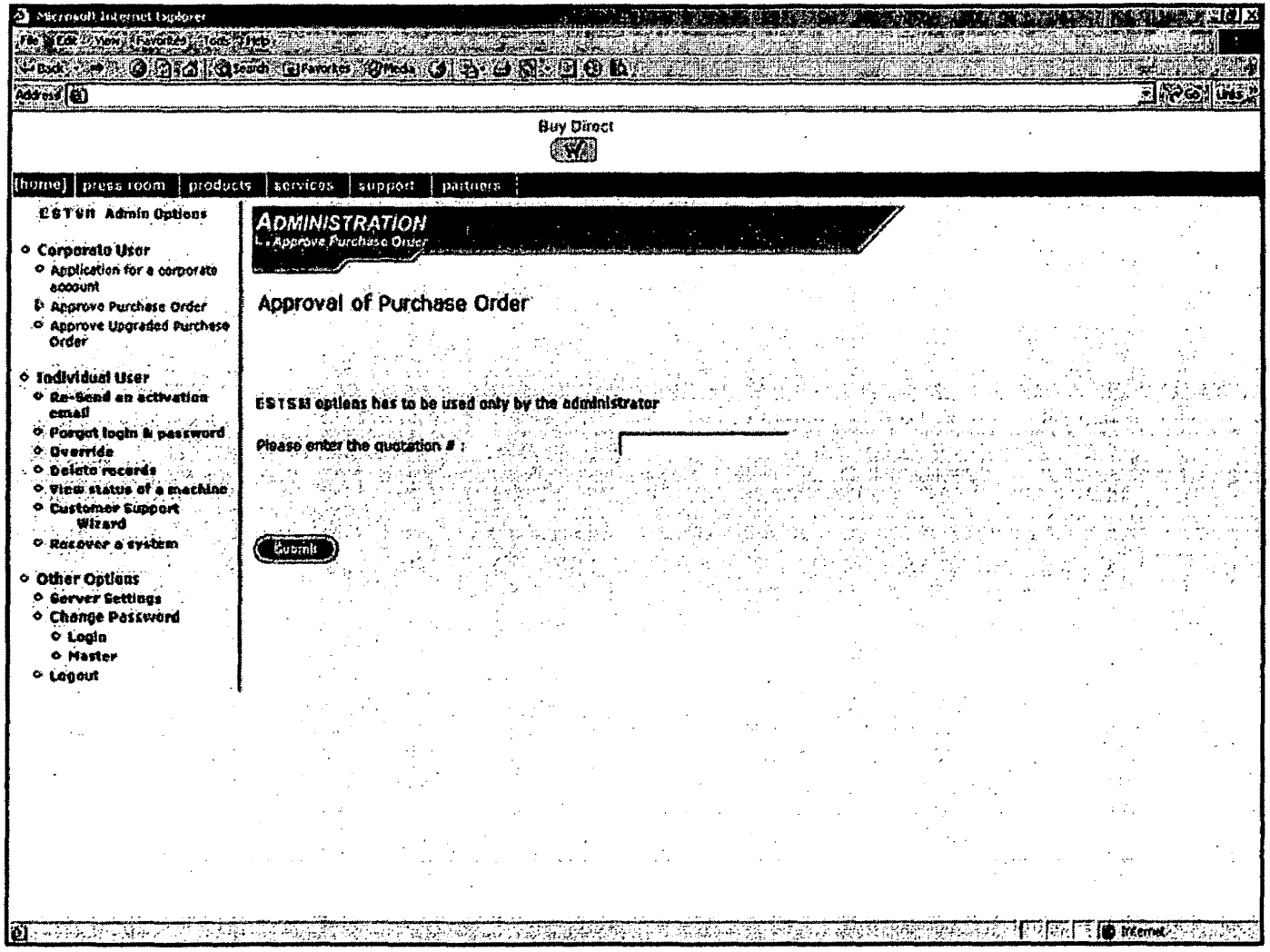

Buy Direct
[home] press room products services support partners
ESTSB Admin Options
Corporate User
Application for a corporate account
Approve Purchase Order
Approve Upgraded Purchase Order
Individual User
Re-Send an activation email
Forgot login & password
Override
Delete records
View status of a machine
Customer Support Wizard
Recover a system
Other Options
Server Settings
Change Password
Login
Master
Logout
ADMINISTRATION
Approve Purchase Order
Approval of Purchase Order
ESTSB options has to be used only by the administrator
Please enter the quotation # :
Submit

FIGURE 28a

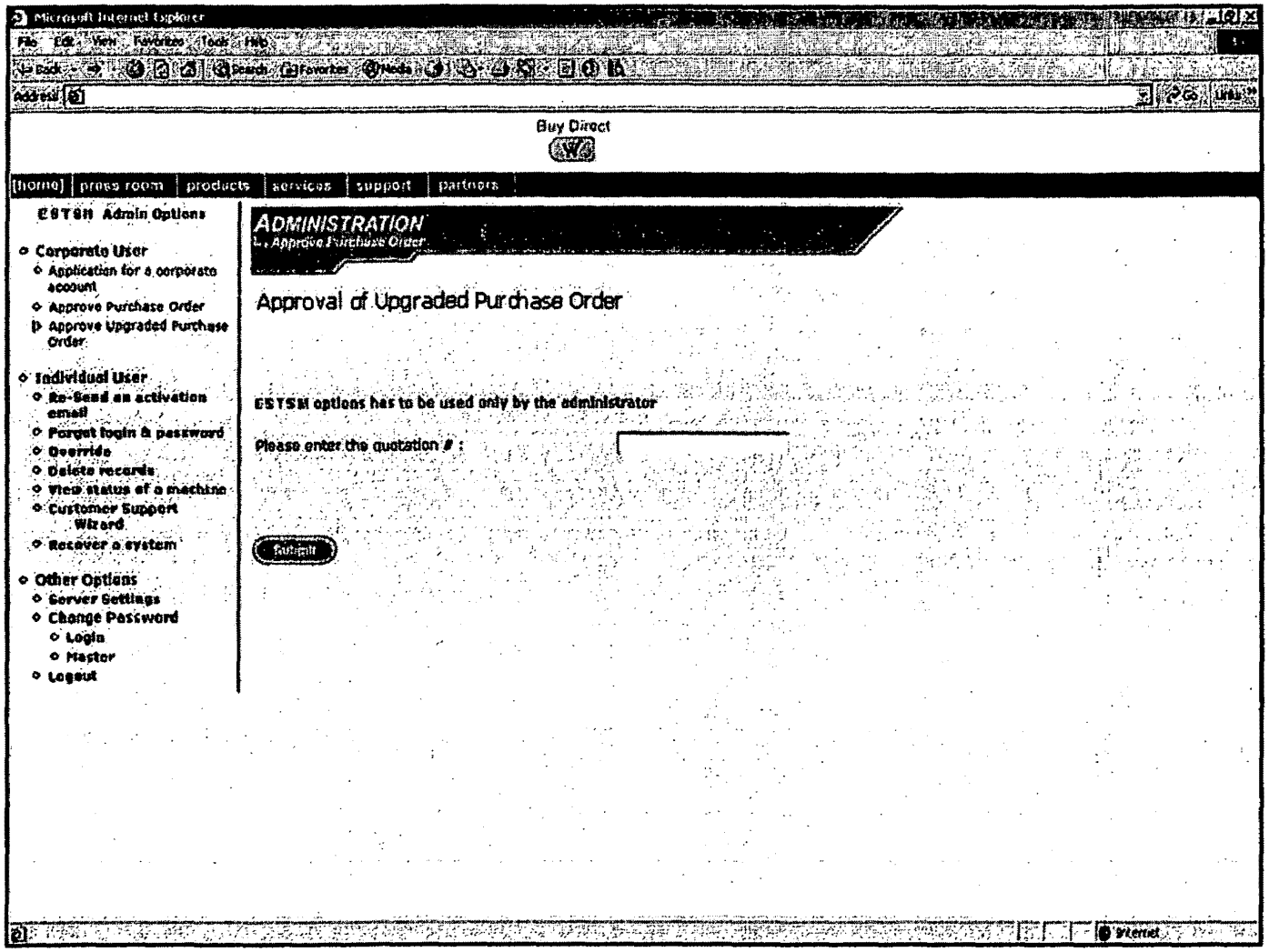


FIGURE 28b

DELL EXHIBIT 1002
Page 102 of 659

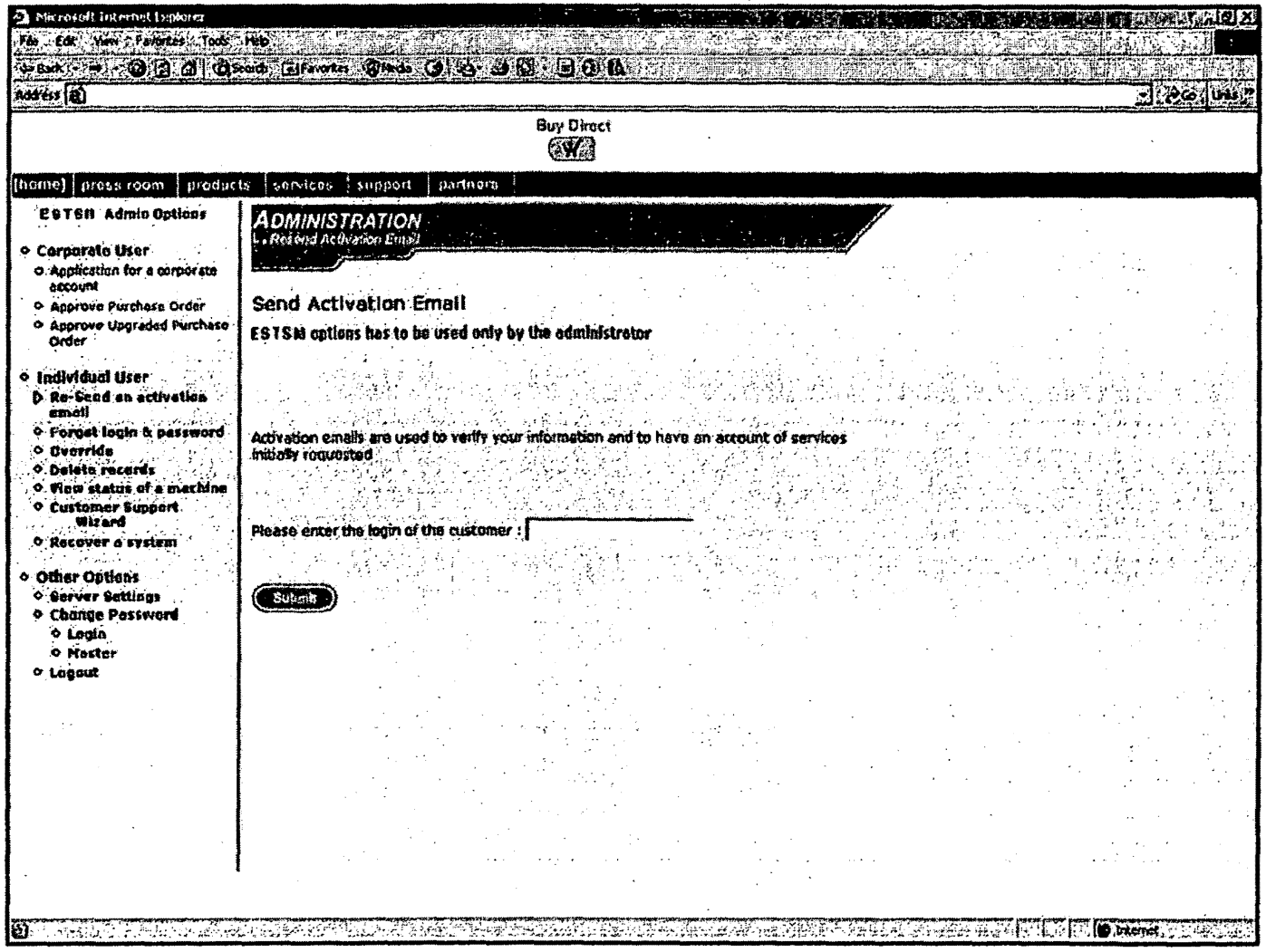


FIGURE 29

DELL EXHIBIT 1002
Page 103 of 659

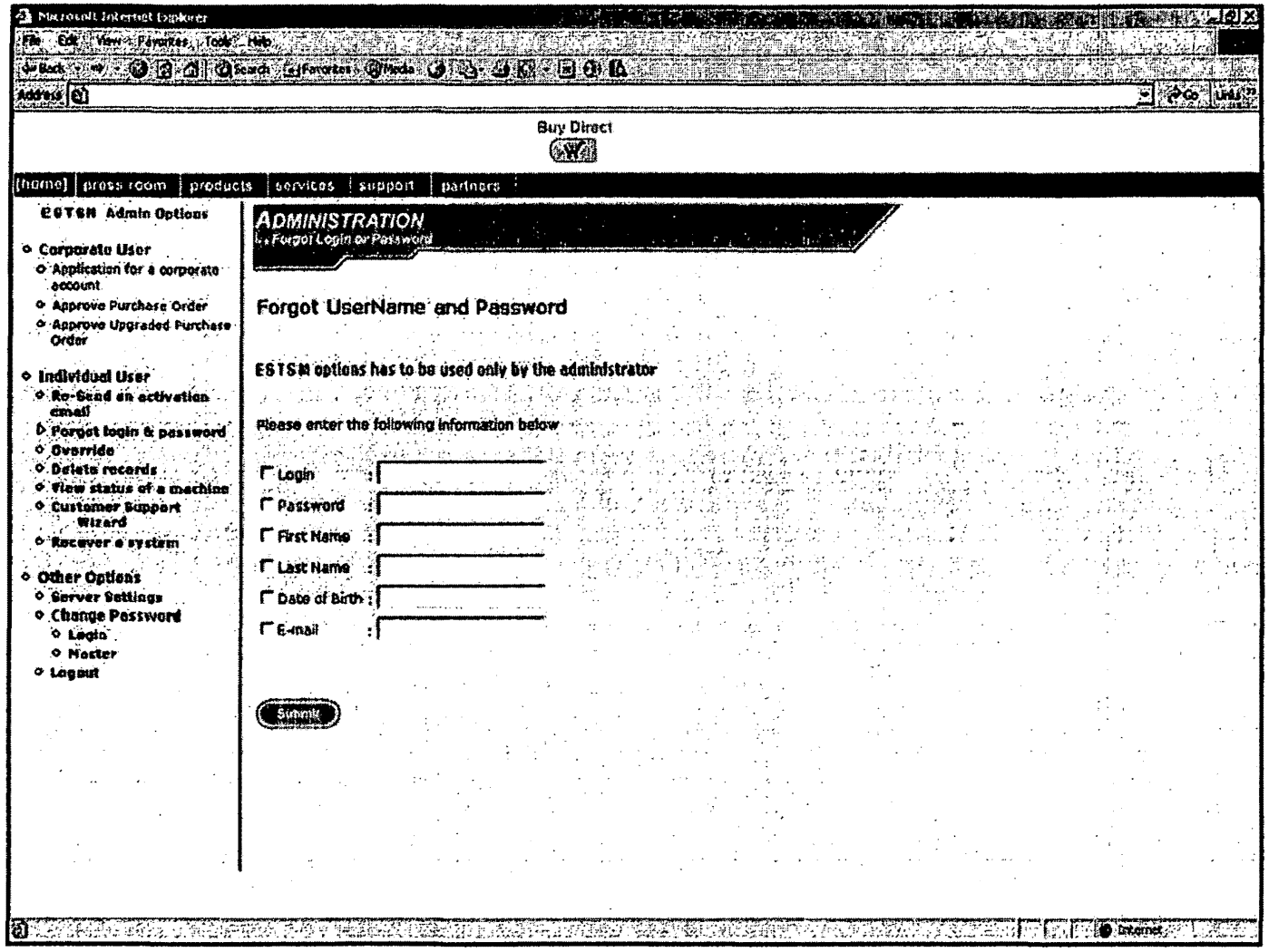

Buy Direct
[home] press room products services support partners
ESTSN Admin Options
Corporate User
Application for a corporate account
Approve Purchase Order
Approve Upgraded Purchase Order
Individual User
Re-Send an activation email
Forgot login & password
Override
Delete records
View status of a machine
Customer Support Wizard
Recover a system
Other Options
Server Settings
Change Password
Login
Master
Logout
ADMINISTRATION
Forgot Login or Password
Forgot UserName and Password
ESTSN options has to be used only by the administrator
Please enter the following information below
Login :
Password :
First Name :
Last Name :
Date of Birth :
E-mail :
Submit

FIGURE 30

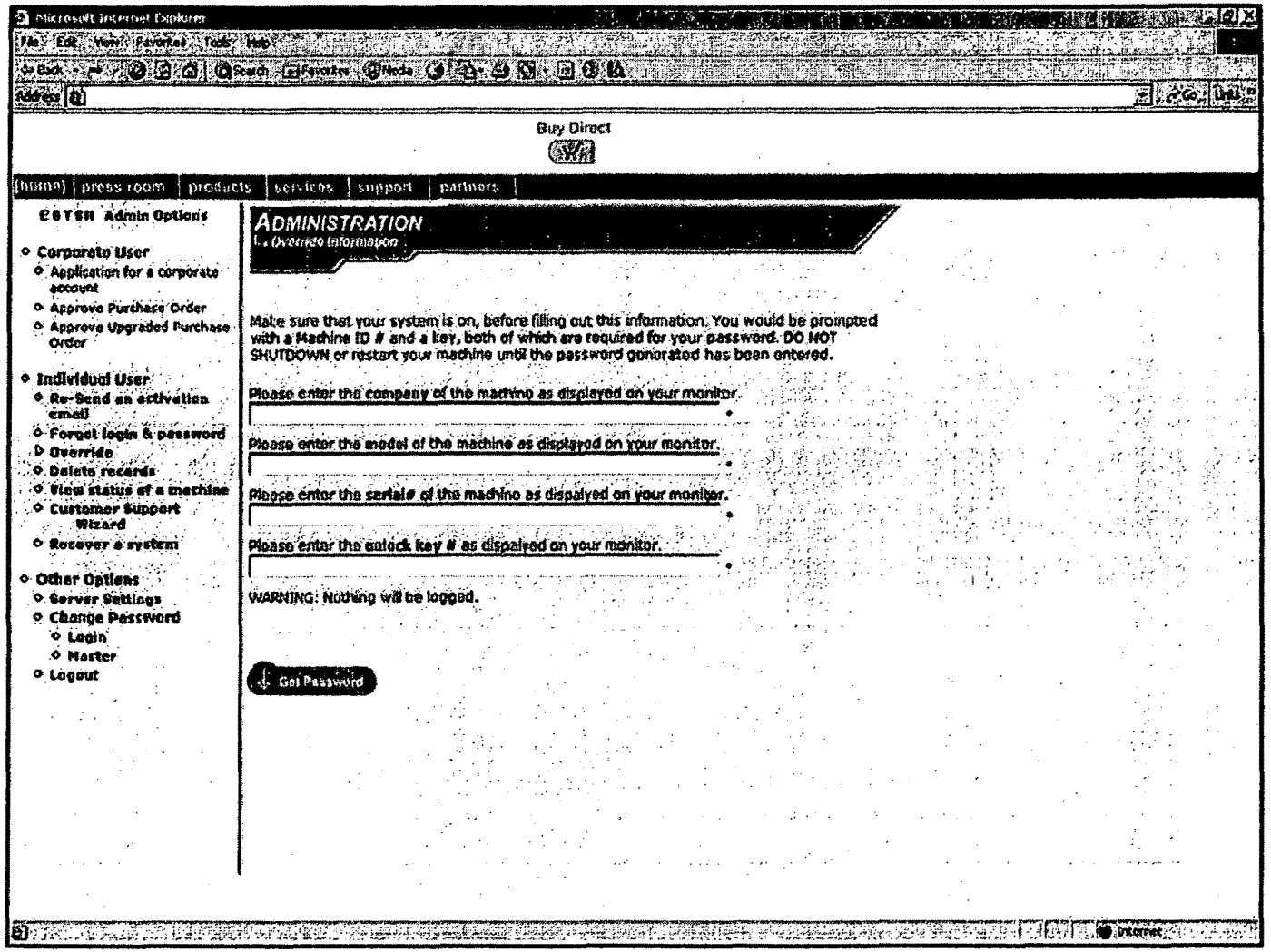


FIGURE 31

DELL EXHIBIT 1002
Page 105 of 659

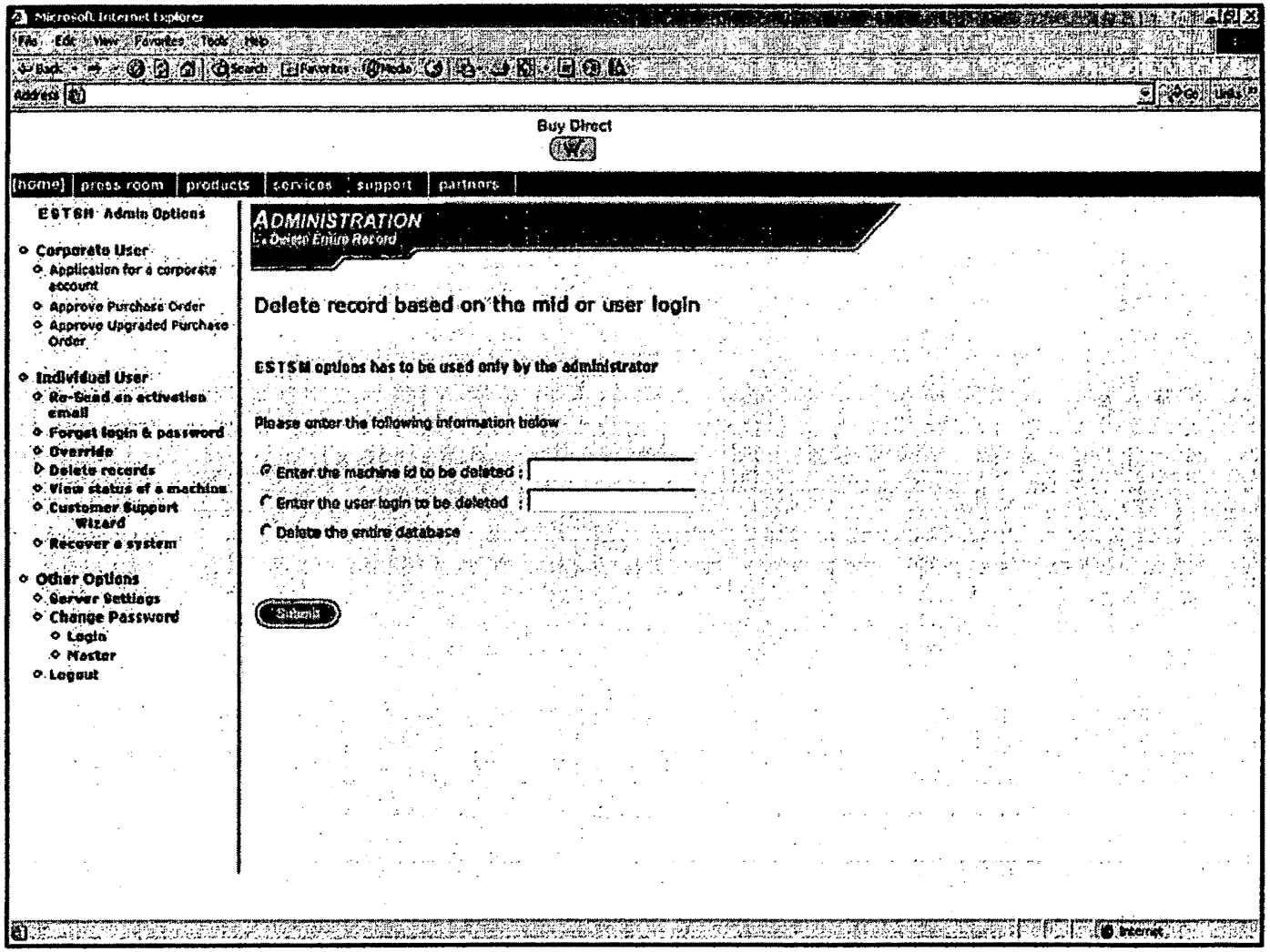


FIGURE 32

DELL EXHIBIT 1002
Page 106 of 659

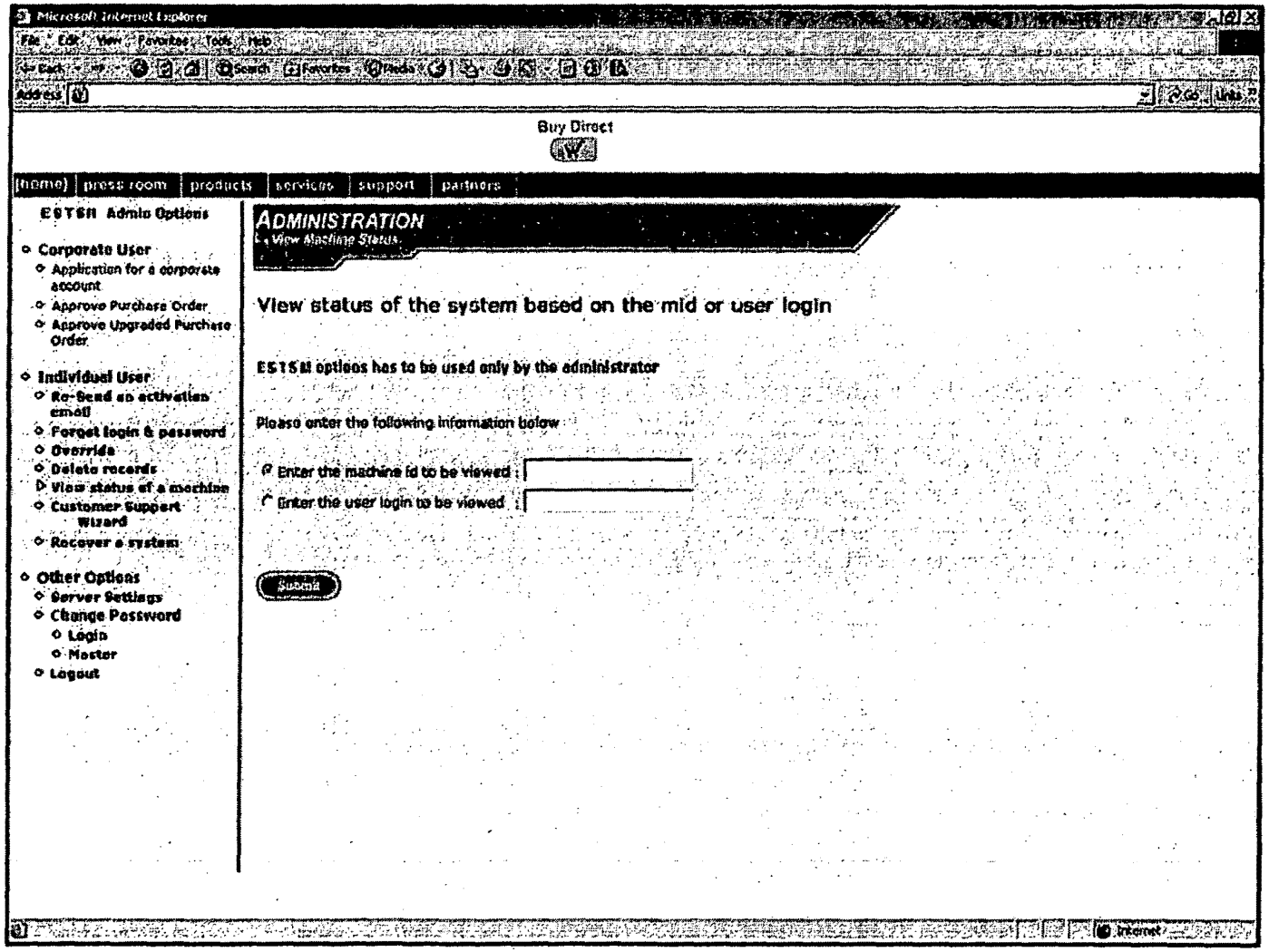


FIGURE 33

DELL EXHIBIT 1002
Page 107 of 659

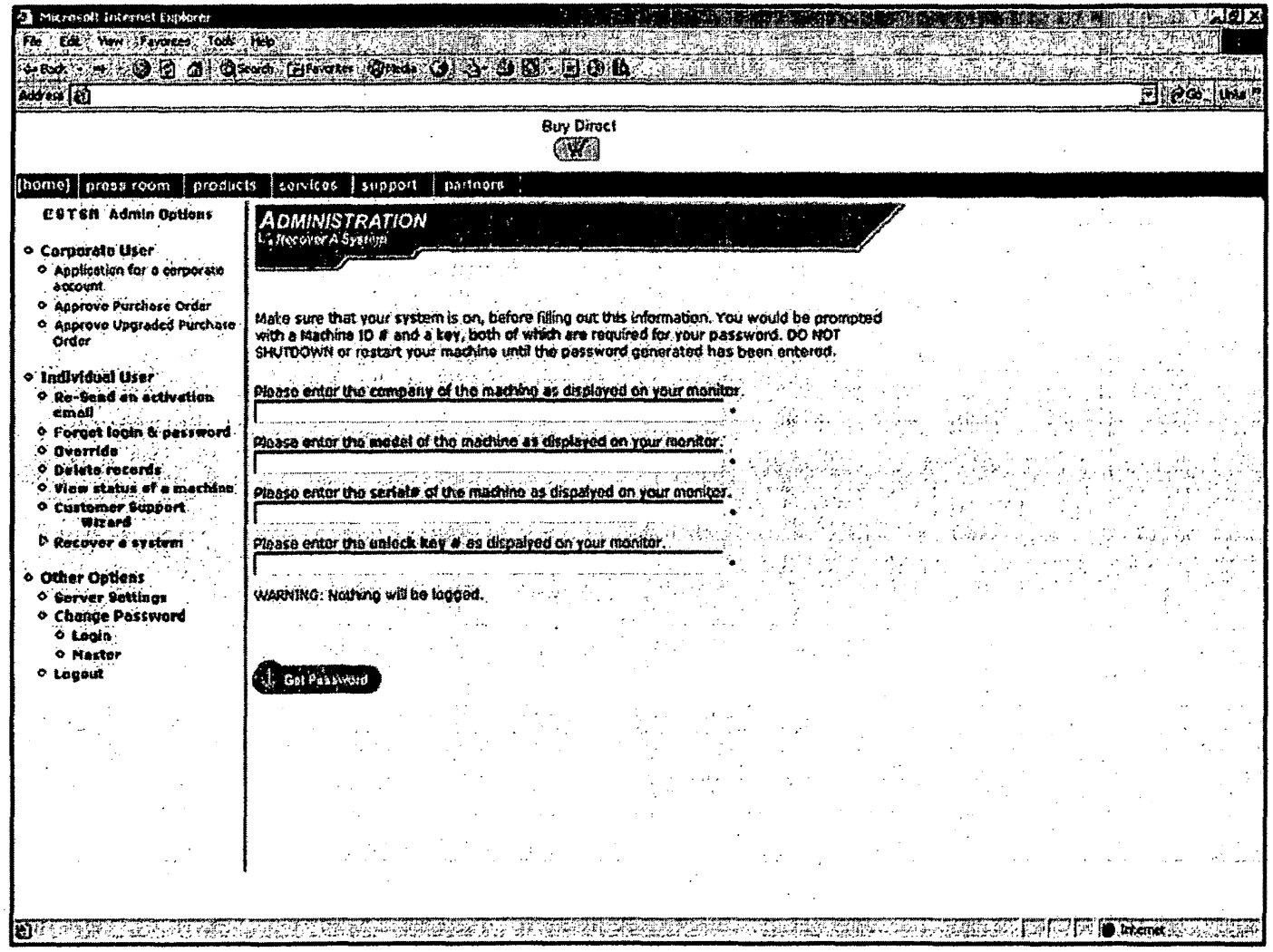


FIGURE 34

DELL EXHIBIT 1002
Page 108 of 659

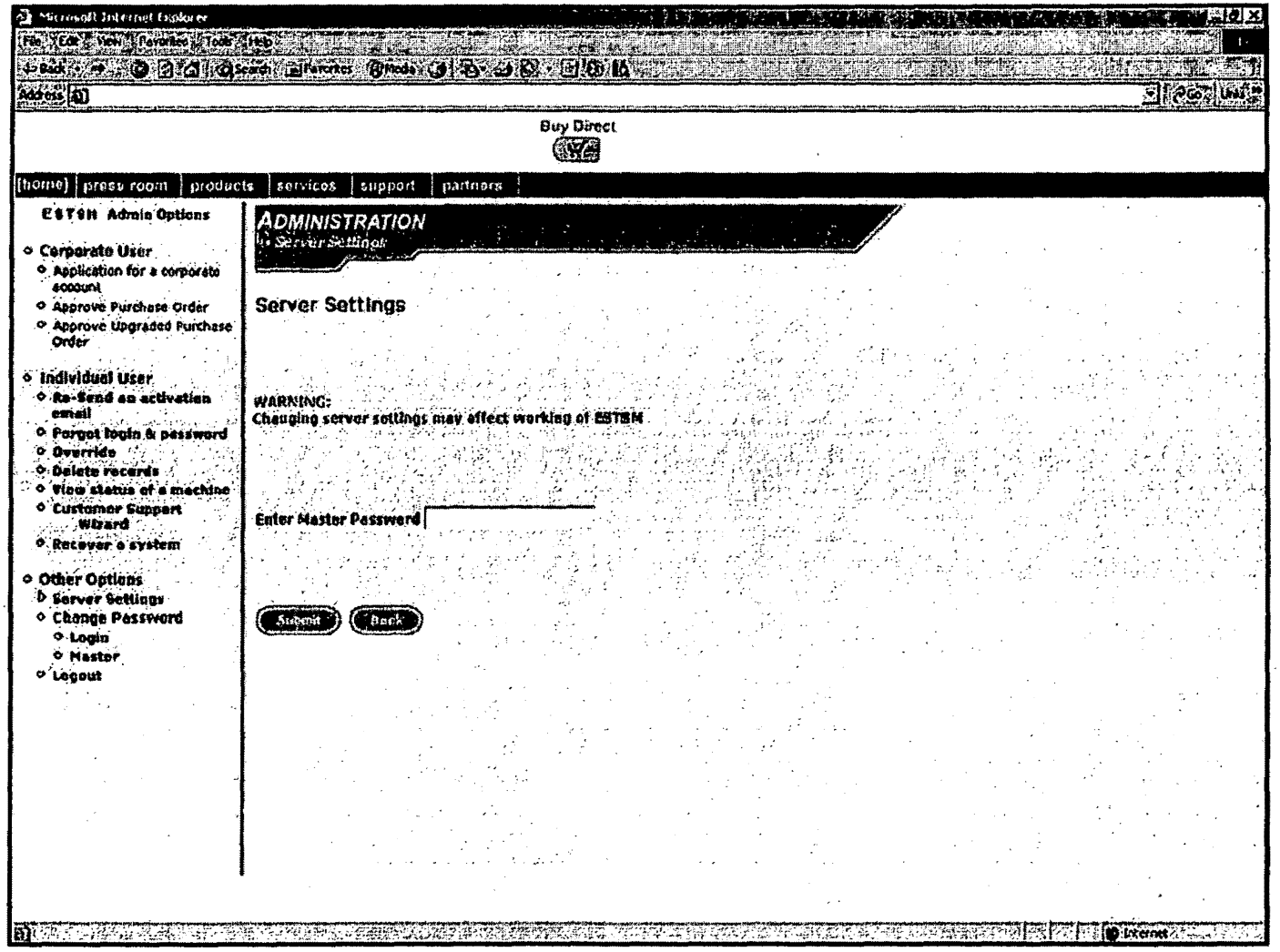


FIGURE 35

DELL EXHIBIT 1002
Page 109 of 659

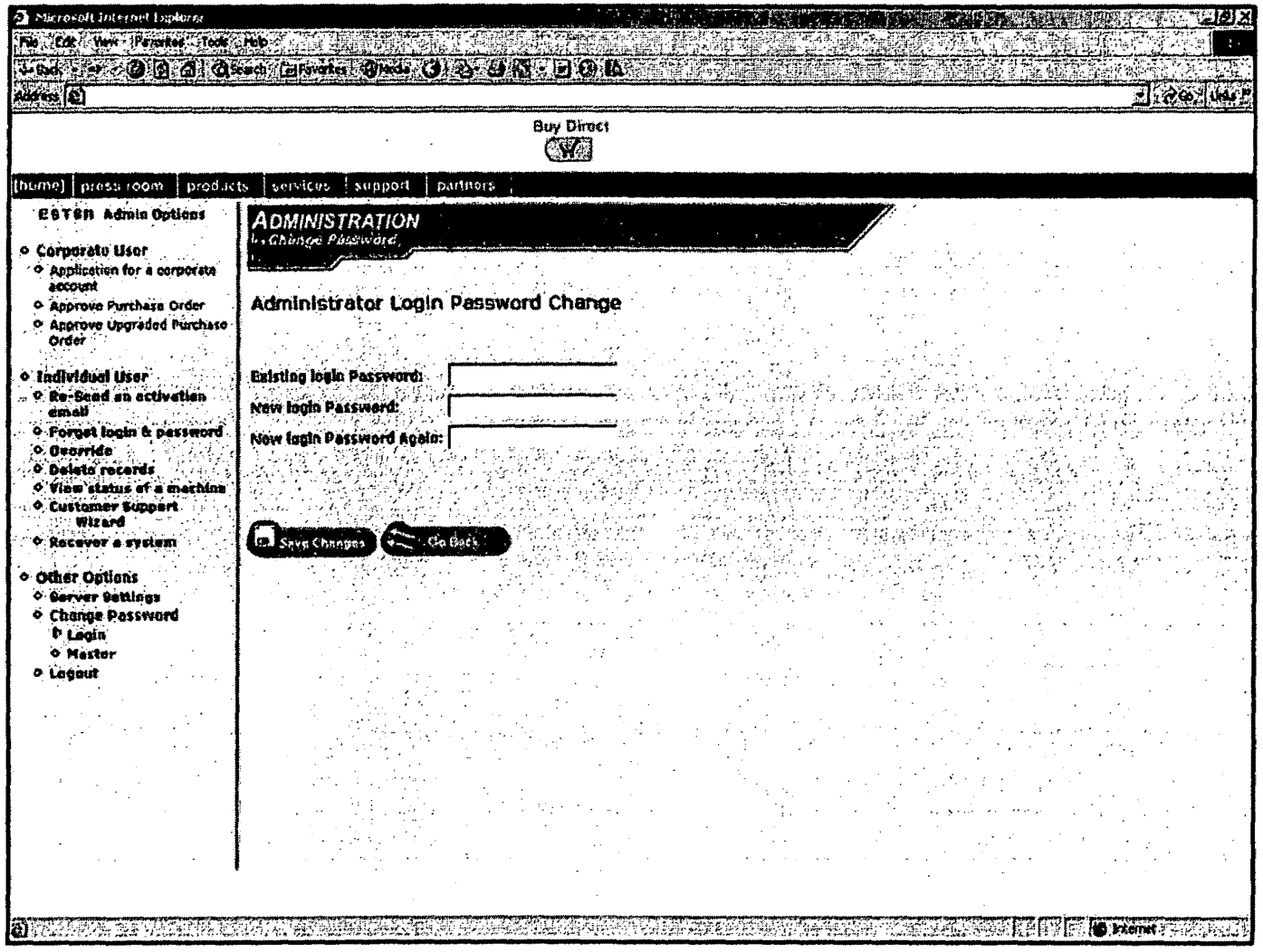


FIGURE 36a

DELL EXHIBIT 1002
Page 110 of 659

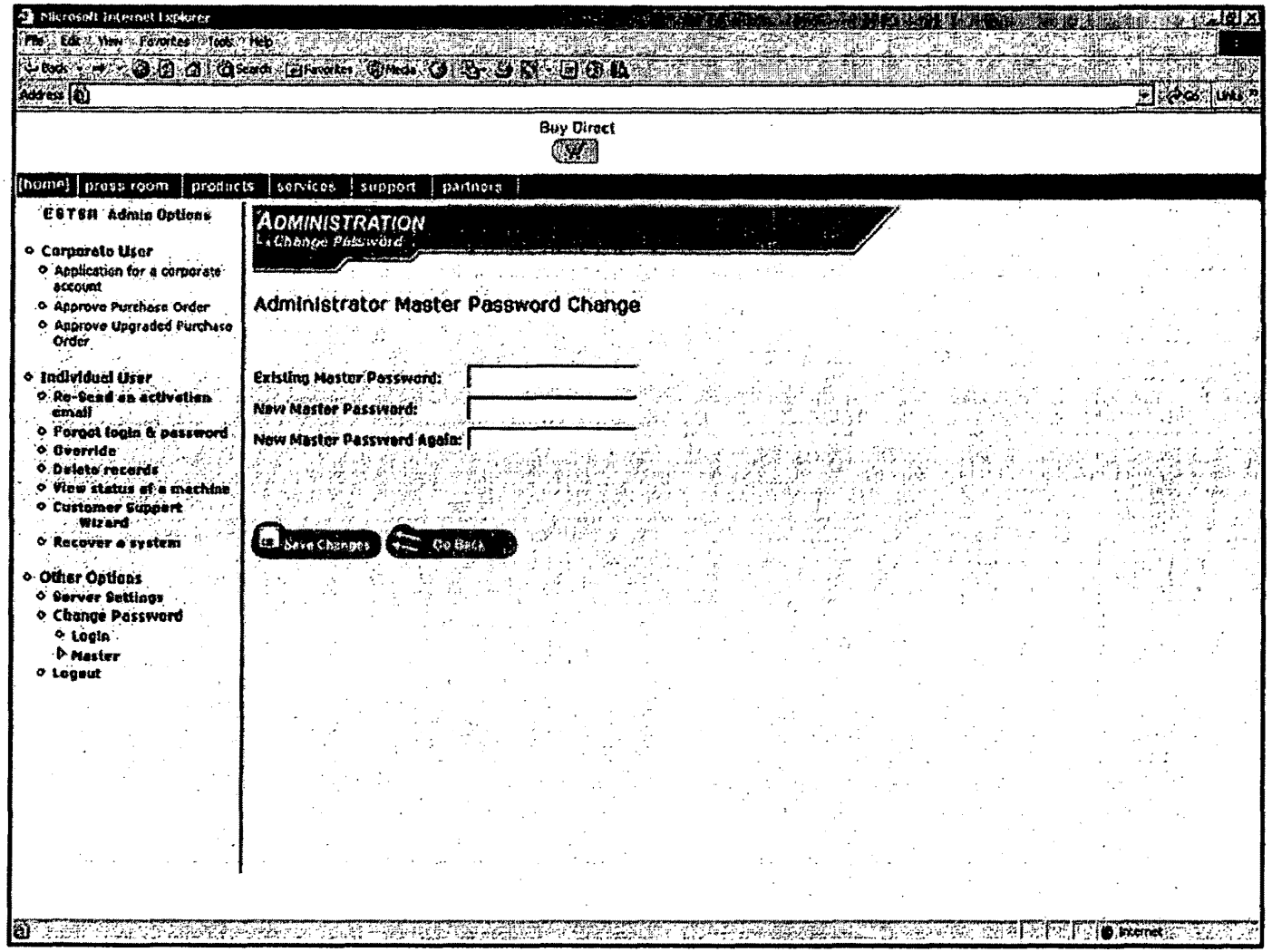


FIGURE 36b

DELL EXHIBIT 1002
Page 111 of 659

NOT REGISTERED TO ACTIVE

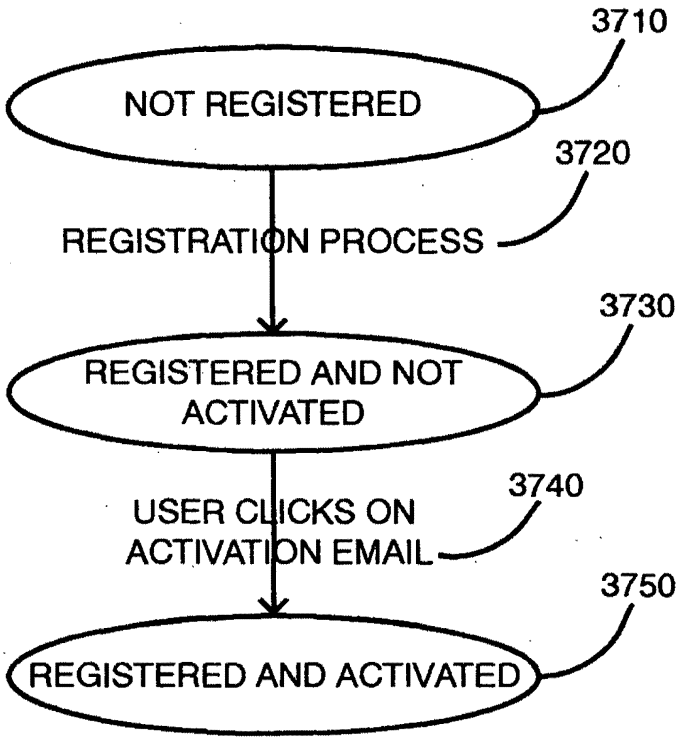


FIGURE 37

NOT REGISTERED TO REGISTERED AND ACTIVE

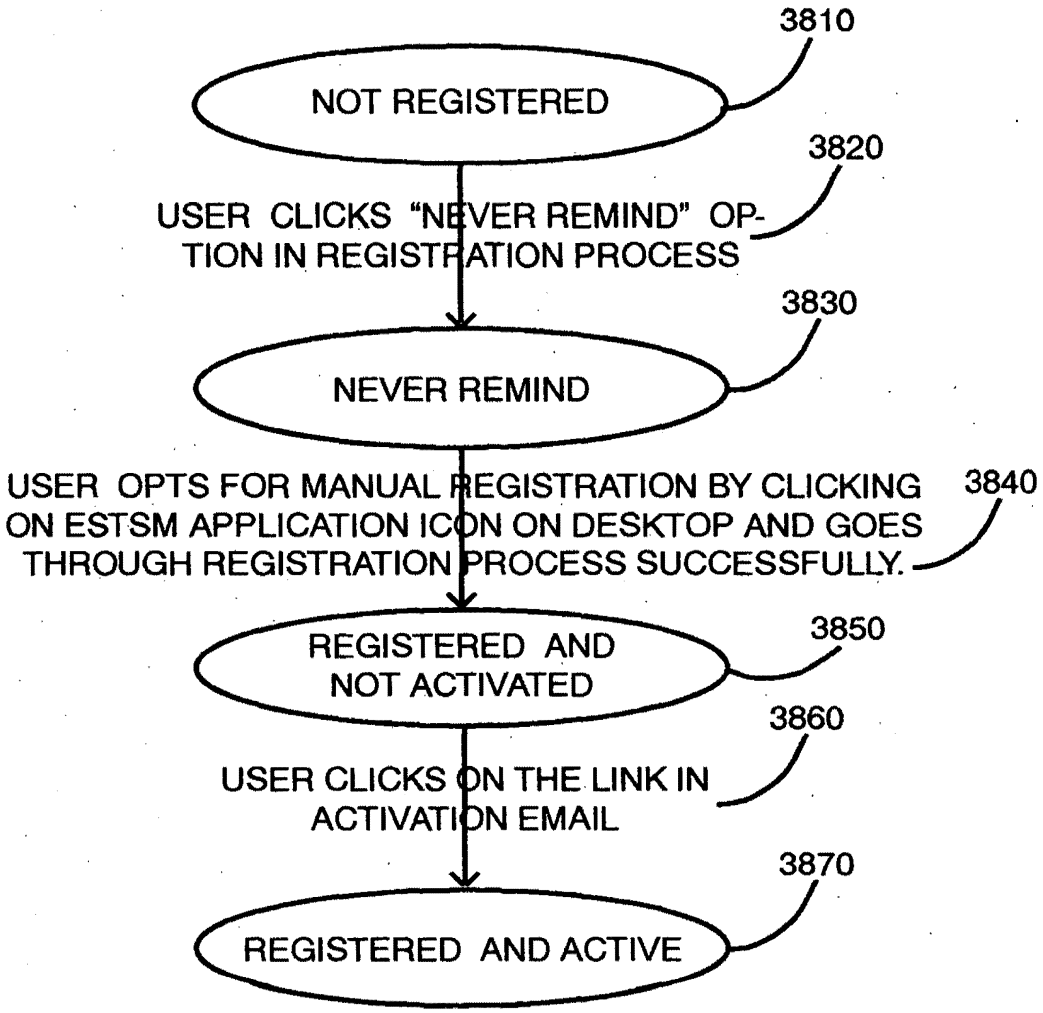


FIGURE 38

REGISTERED AND ACTIVE TO DE REGISTERED

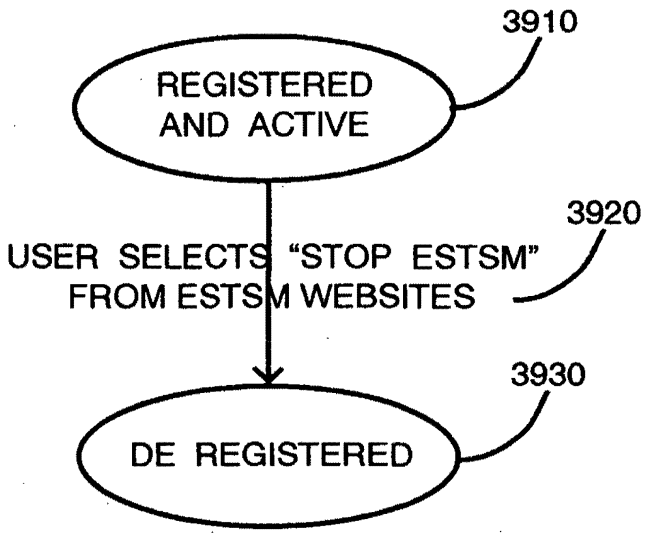


FIGURE 39

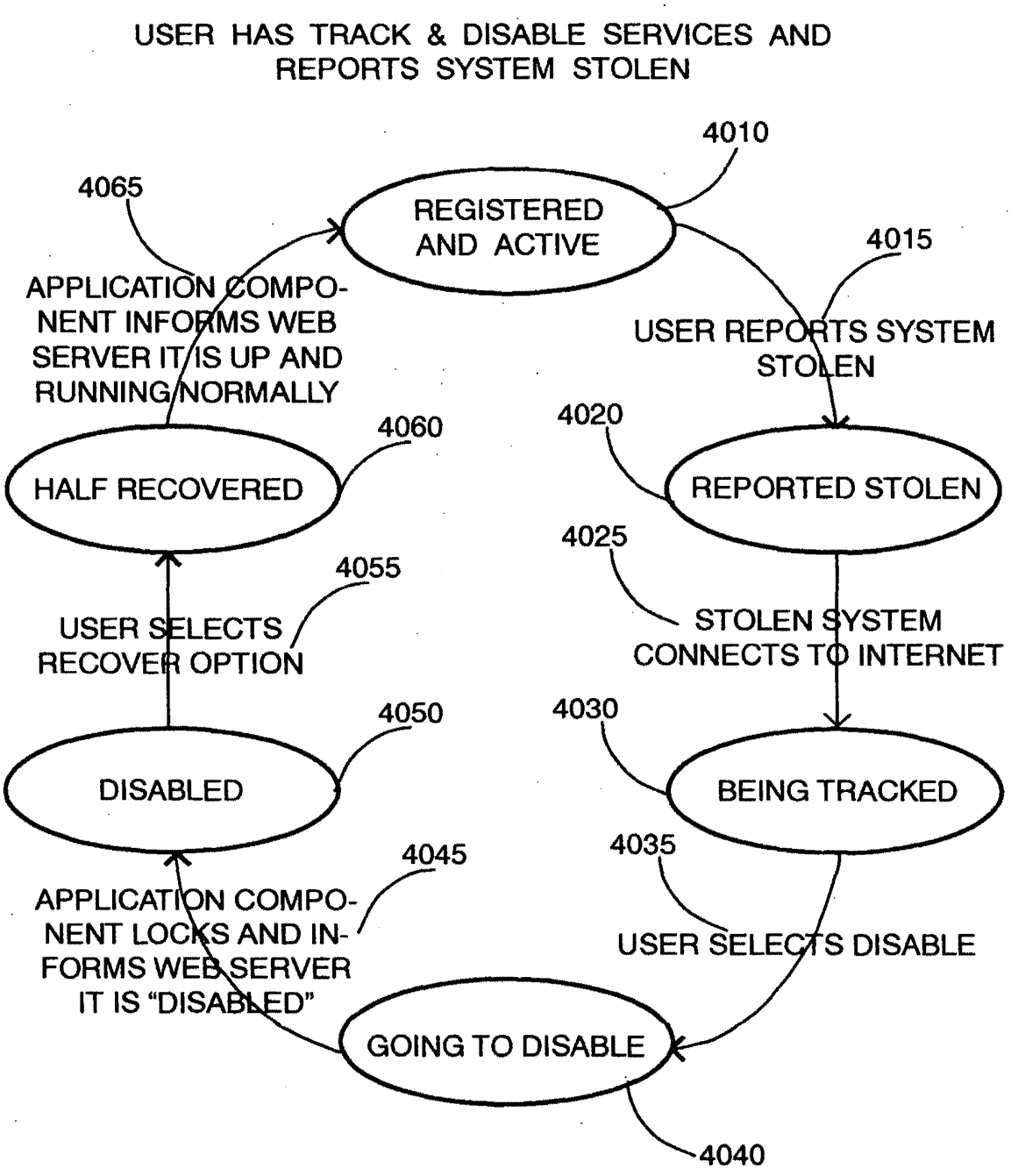

USER HAS TRACK & DISABLE SERVICES AND REPORTS SYSTEM STOLEN
4010
REGISTERED AND ACTIVE
4065
APPLICATION COMPONENT INFORMS WEB SERVER IT IS UP AND RUNNING NORMALLY
4015
USER REPORTS SYSTEM STOLEN
4020
REPORTED STOLEN
4060
HALF RECOVERED
4025
STOLEN SYSTEM CONNECTS TO INTERNET
4055
USER SELECTS RECOVER OPTION
4030
BEING TRACKED
4050
DISABLED
4035
USER SELECTS DISABLE
4045
APPLICATION COMPONENT LOCKS AND INFORMS WEB SERVER IT IS "DISABLED"
GOING TO DISABLE
4040

FIGURE 40

REGISTERED AND ACTIVE TO OVERRIDE

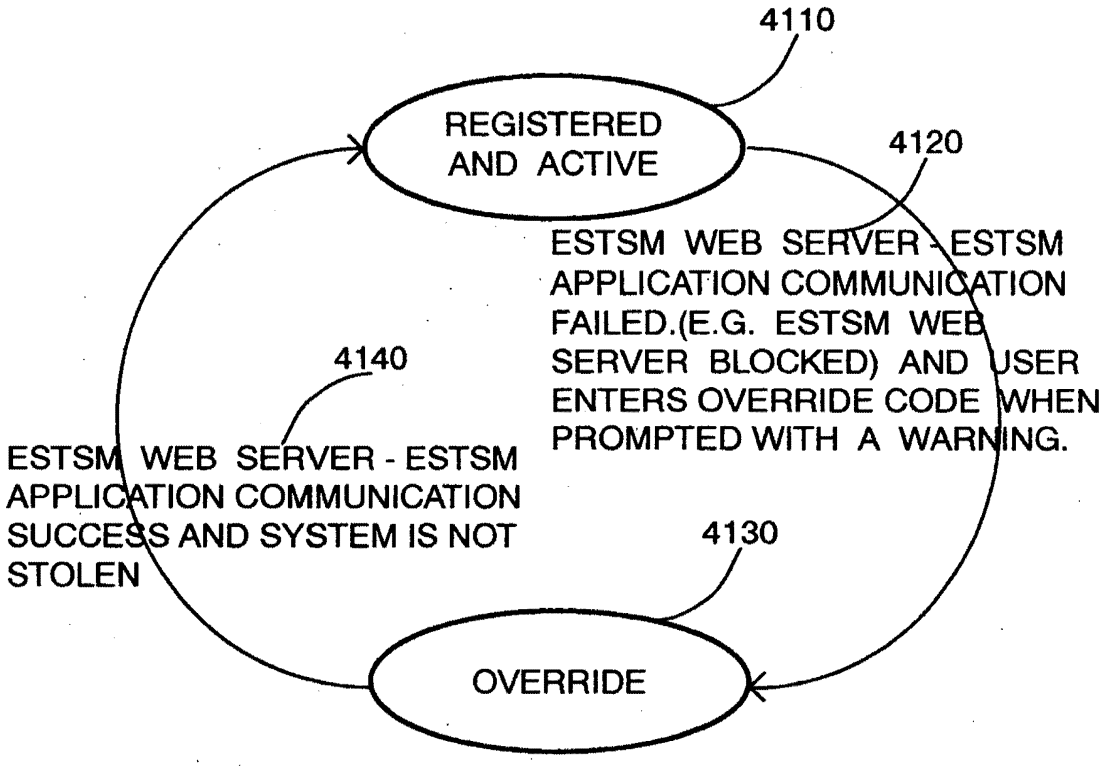


FIGURE 41

USER HAS DATA DESTROY SERVICE AND REPORTS SYSTEM STOLEN

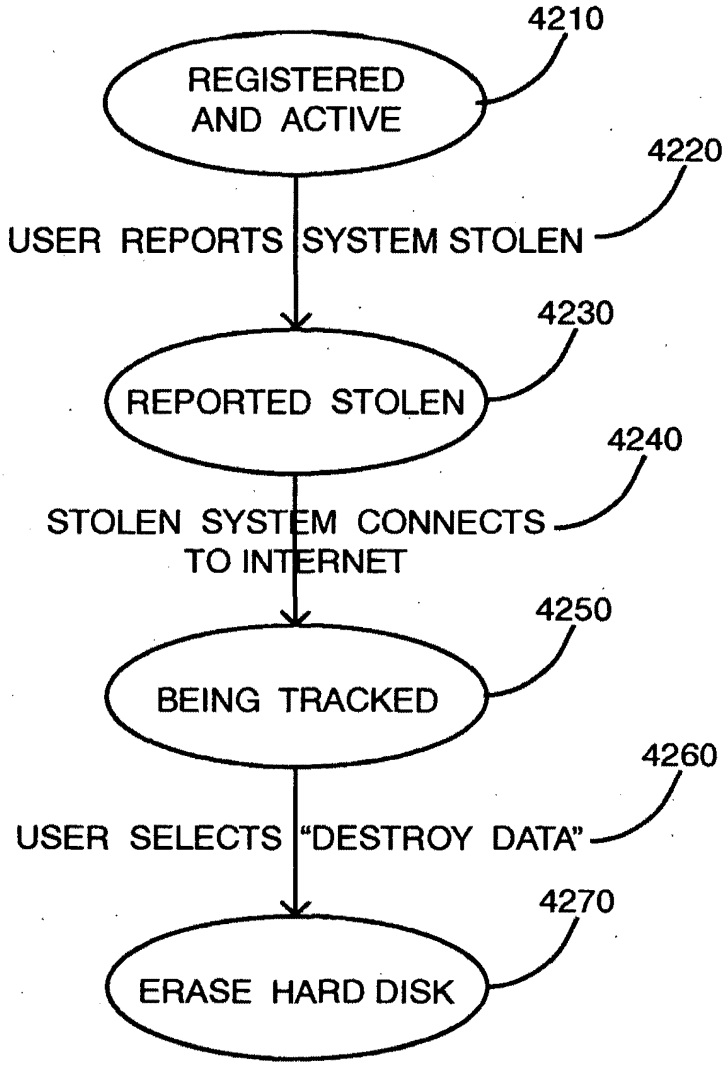


FIGURE 42

REGISTERED AND ACTIVE TO USER REMOVED

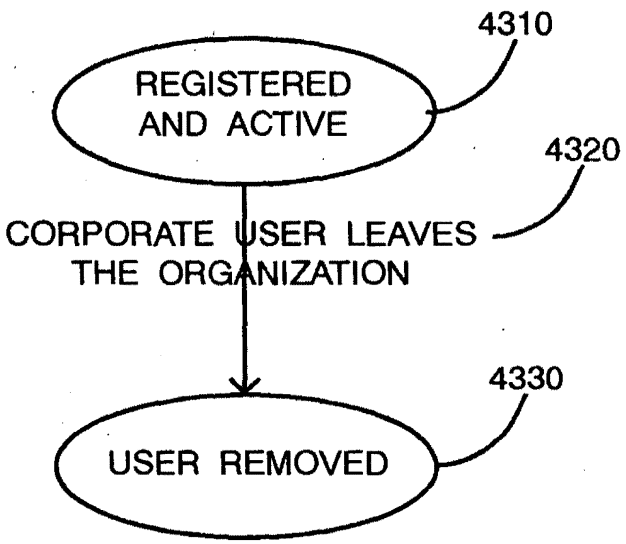


FIGURE 43

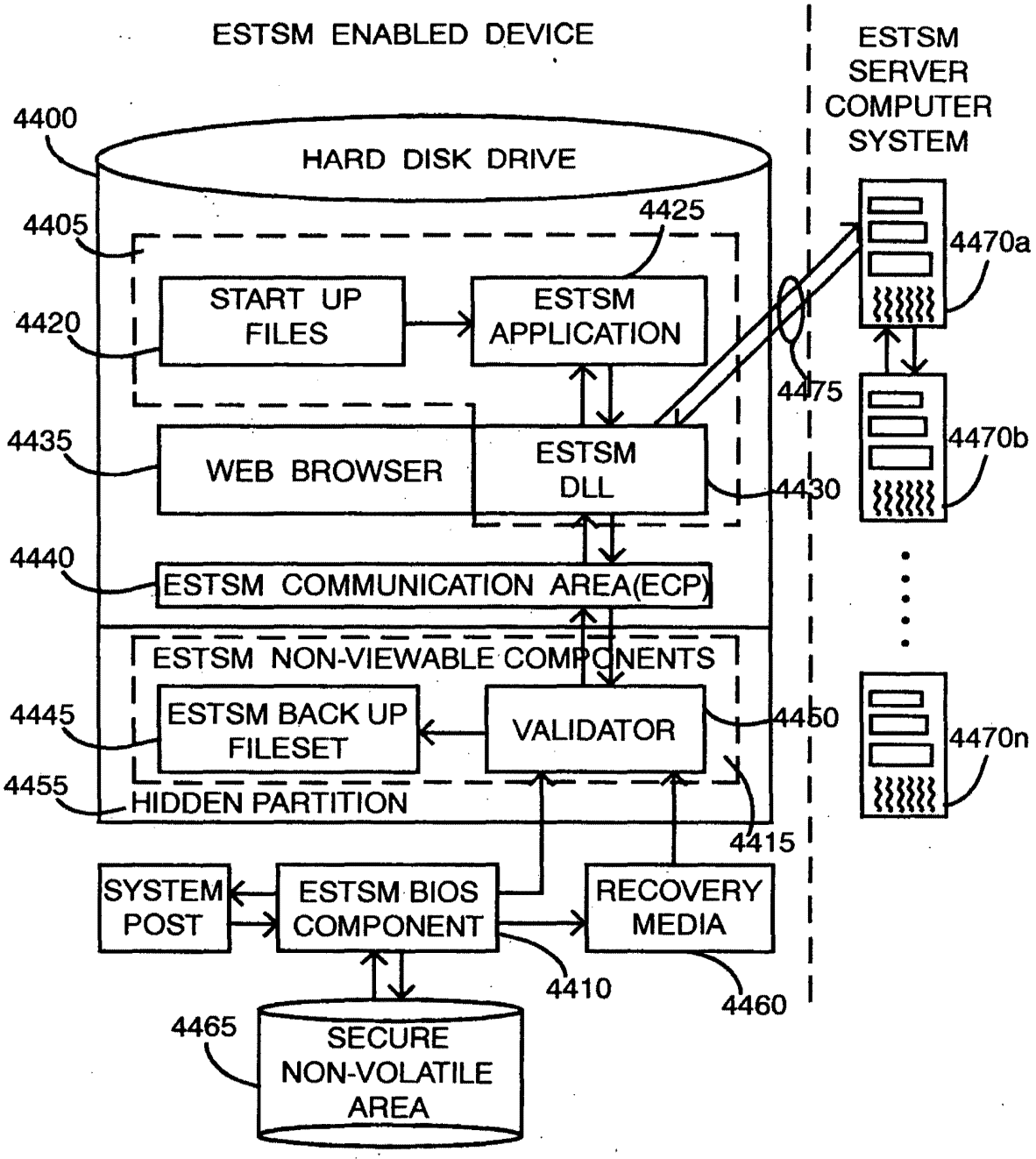

ESTSM ENABLED DEVICE
ESTSM SERVER COMPUTER SYSTEM
4400
HARD DISK DRIVE
4405
4425
START UP FILES
ESTSM APPLICATION
4420
4470a
4475
4435
WEB BROWSER
ESTSM DLL
4430
4470b
4440
ESTSM COMMUNICATION AREA(ECP)
ESTSM NON-VIEWABLE COMPONENTS
4445
ESTSM BACK UP FILESET
VALIDATOR
4450
4470n
4455
HIDDEN PARTITION
4415
SYSTEM POST
ESTSM BIOS COMPONENT
RECOVERY MEDIA
4410
4460
4465
SECURE NON-VOLATILE AREA

FIGURE 44

ESTSM ENABLED PDA

ESTSM ENABLED PDA

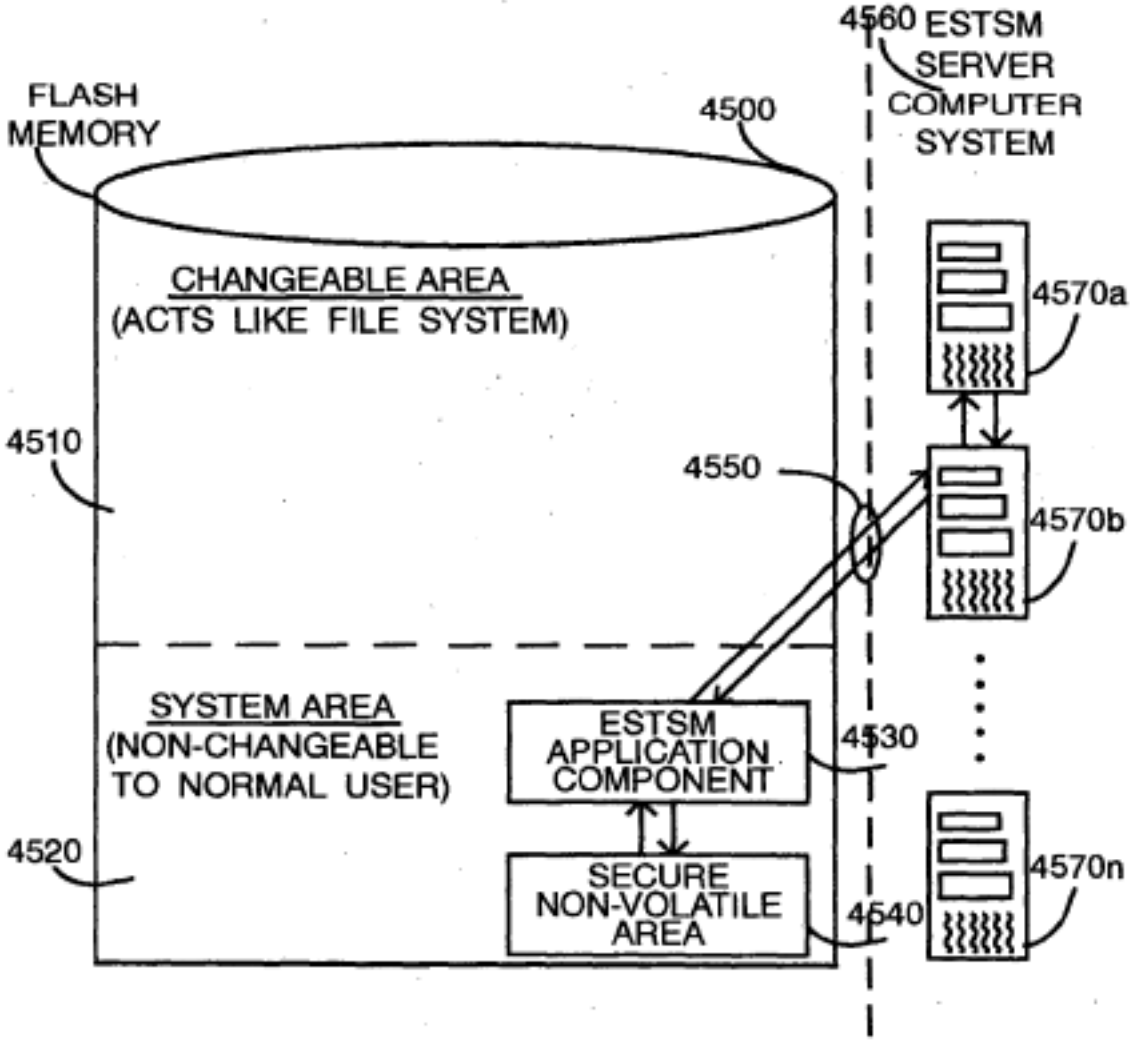


FIGURE 45

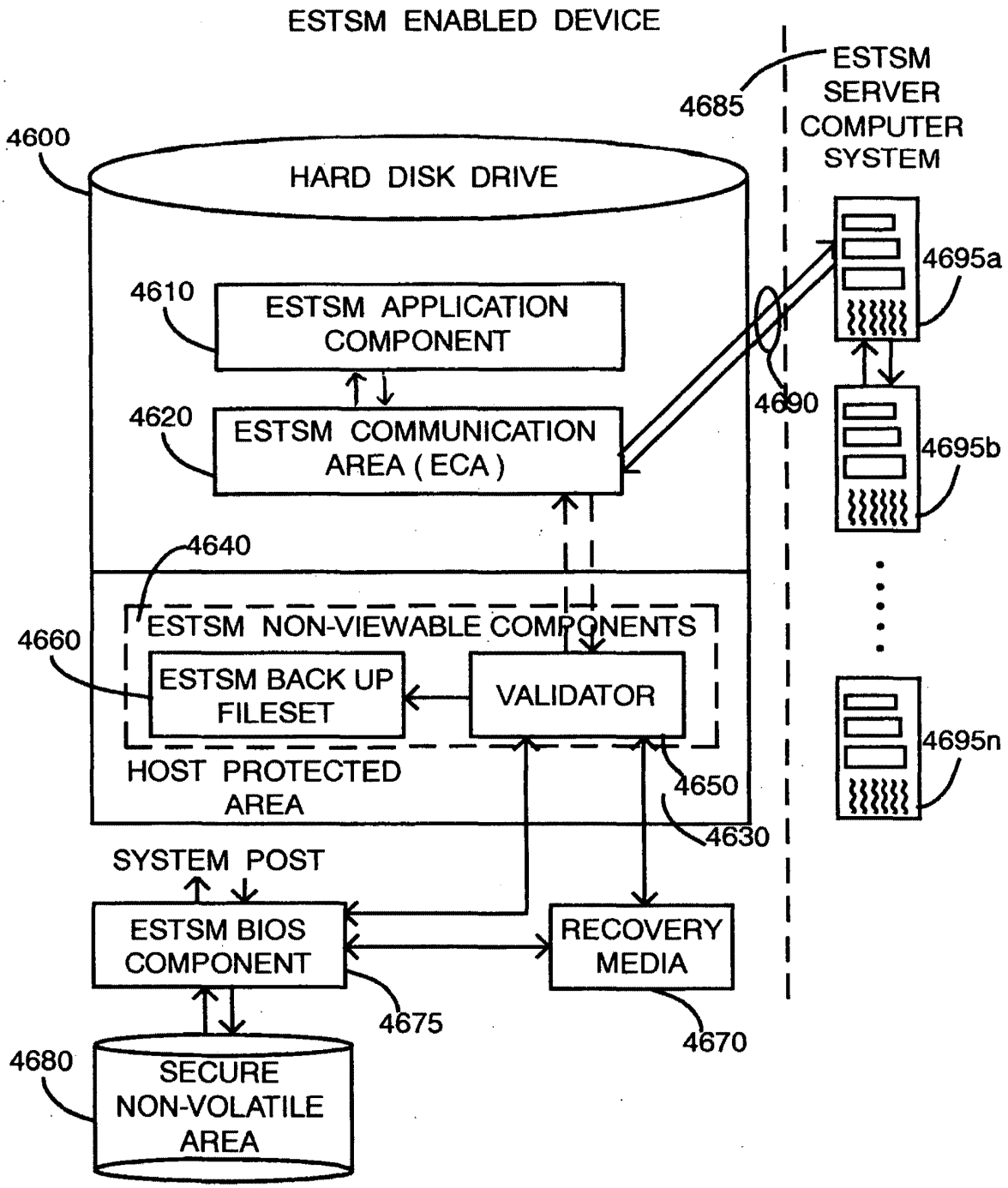

ESTSM ENABLED DEVICE
4685
ESTSM SERVER COMPUTER SYSTEM
4600
HARD DISK DRIVE
4695a
4610
ESTSM APPLICATION COMPONENT
4620
ESTSM COMMUNICATION AREA (ECA)
4690
4695b
4640
ESTSM NON-VIEWABLE COMPONENTS
4660
ESTSM BACK UP FILESET
VALIDATOR
HOST PROTECTED AREA
4650
4630
4695n
SYSTEM POST
ESTSM BIOS COMPONENT
RECOVERY MEDIA
4675
4670
4680
SECURE NON-VOLATILE AREA

FIGURE 46

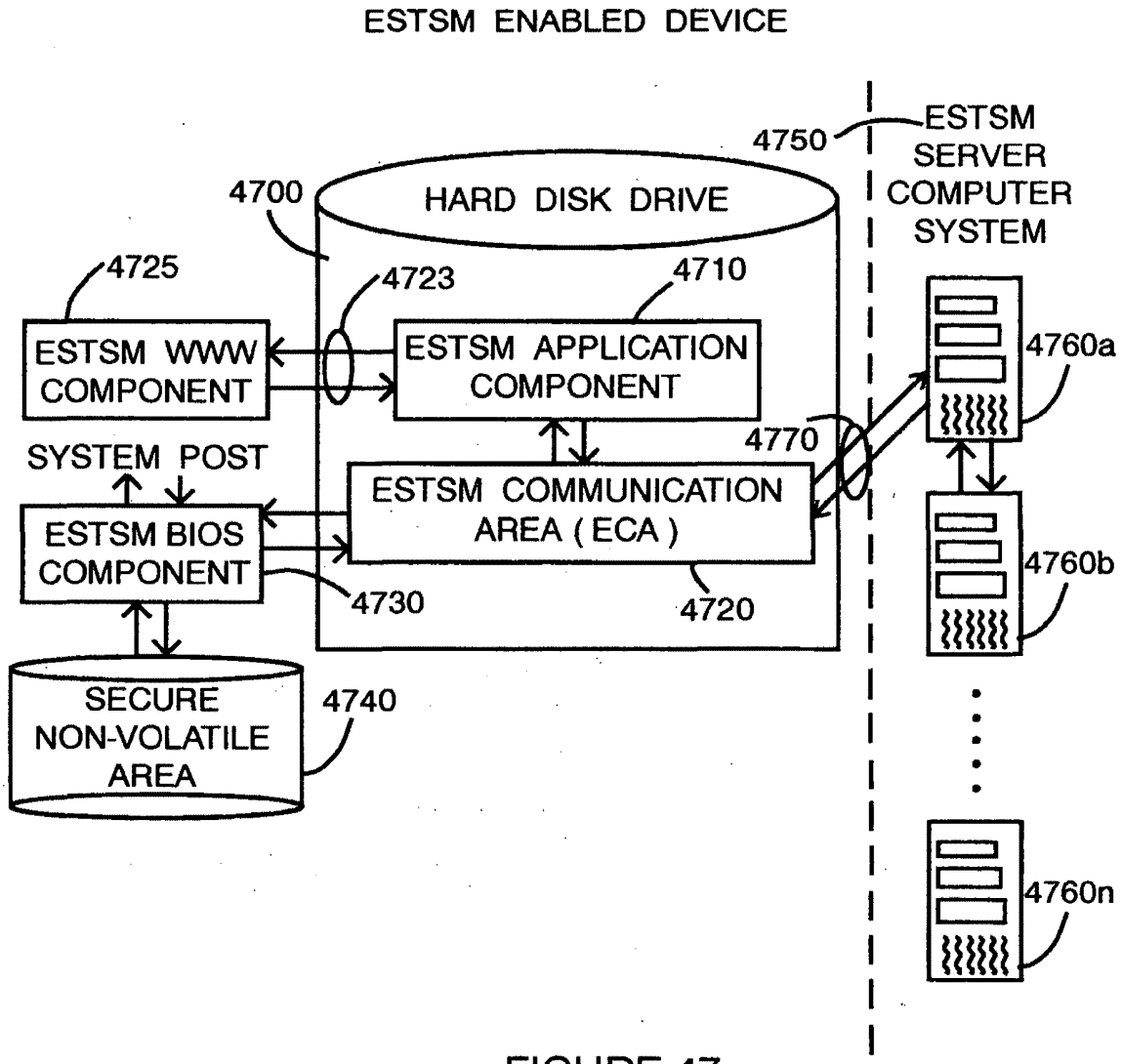

ESTSM ENABLED DEVICE
4750
ESTSM SERVER COMPUTER SYSTEM
4700
HARD DISK DRIVE
4725
4723
4710
ESTSM WWW COMPONENT
ESTSM APPLICATION COMPONENT
4760a
4770
SYSTEM POST
ESTSM COMMUNICATION AREA (ECA)
ESTSM BIOS COMPONENT
4760b
4730
4720
SECURE NON-VOLATILE AREA
4740
4760n

FIGURE 47

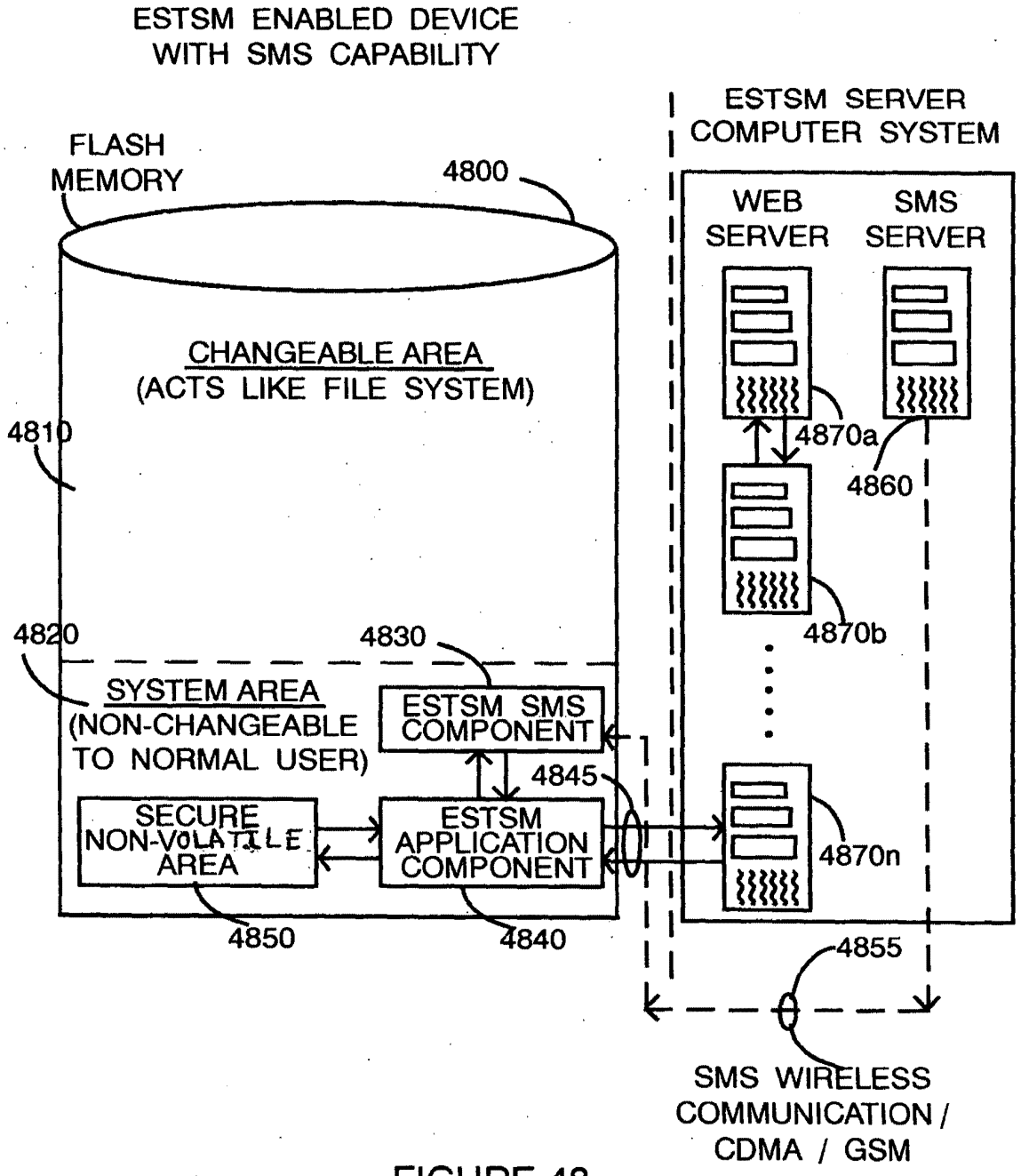

ESTSM ENABLED DEVICE
WITH SMS CAPABILITY
ESTSM SERVER
COMPUTER SYSTEM
FLASH
MEMORY
4800
WEB
SERVER
SMS
SERVER
CHANGEABLE AREA
(ACTS LIKE FILE SYSTEM)
4810
4870a
4860
4870b
4820
4830
SYSTEM AREA
(NON-CHANGEABLE
TO NORMAL USER)
ESTSM SMS
COMPONENT
4845
SECURE
NON-VOLATILE
AREA
ESTSM
APPLICATION
COMPONENT
4870n
4850
4840
4855
SMS WIRELESS
COMMUNICATION /
CDMA / GSM

FIGURE 48

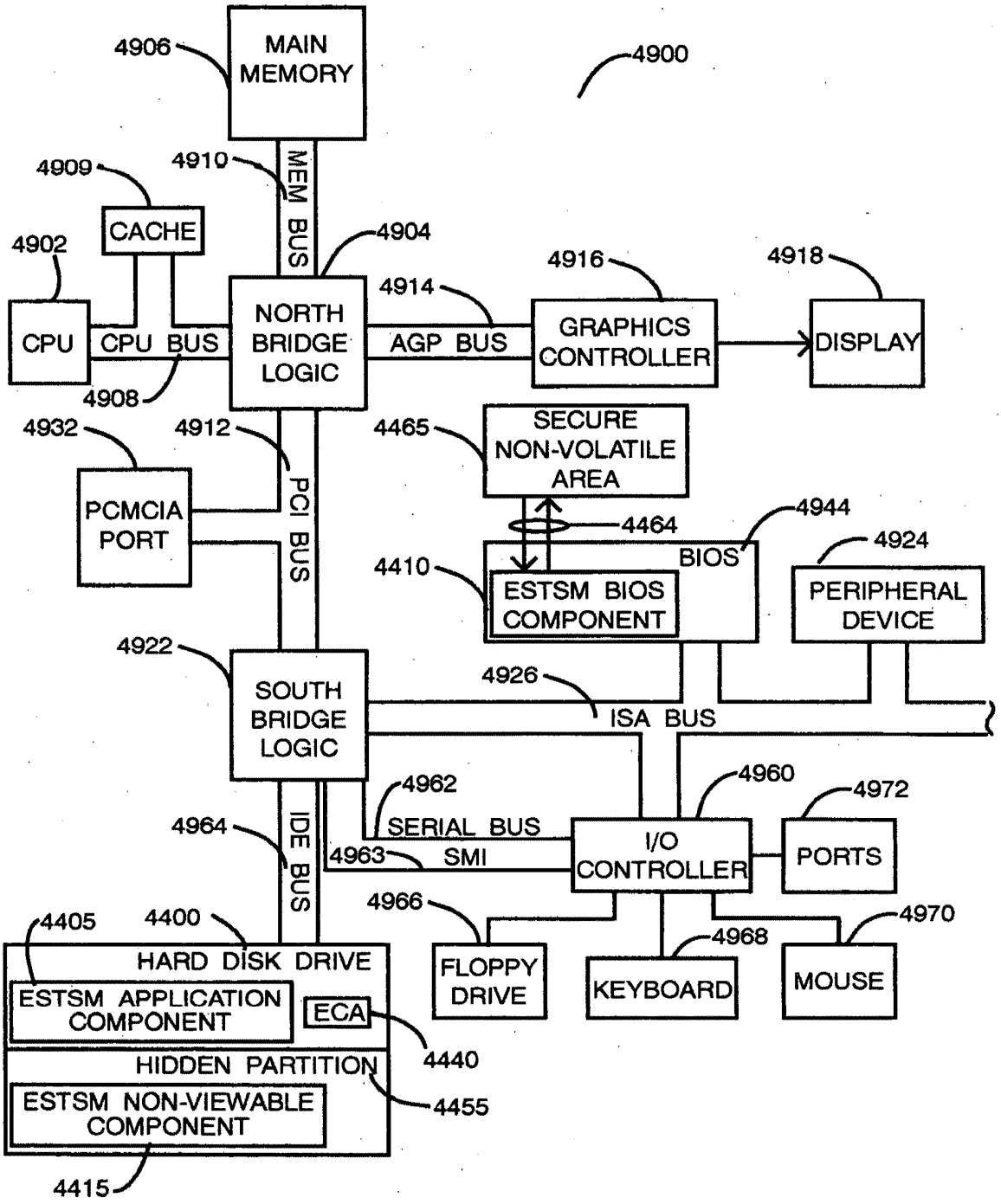

4906
MAIN MEMORY
4900
4909
4910
MEM BUS
CACHE
4902
4904
4916
4918
4914
CPU
CPU BUS
NORTH BRIDGE LOGIC
AGP BUS
GRAPHICS CONTROLLER
DISPLAY
4908
4932
4912
4465
SECURE NON-VOLATILE AREA
PCMCIA PORT
PCI BUS
4464
4944
BIOS
4924
4410
ESTSM BIOS COMPONENT
PERIPHERAL DEVICE
4922
4926
SOUTH BRIDGE LOGIC
ISA BUS
4962
4960
4972
4964
SERIAL BUS
IDE BUS
4963
SMI
I/O CONTROLLER
PORTS
4966
4970
4405
4400
4968
HARD DISK DRIVE
FLOPPY DRIVE
KEYBOARD
MOUSE
ESTSM APPLICATION COMPONENT
ECA
4440
HIDDEN PARTITION
4455
ESTSM NON-VIEWABLE COMPONENT
4415

FIGURE 49

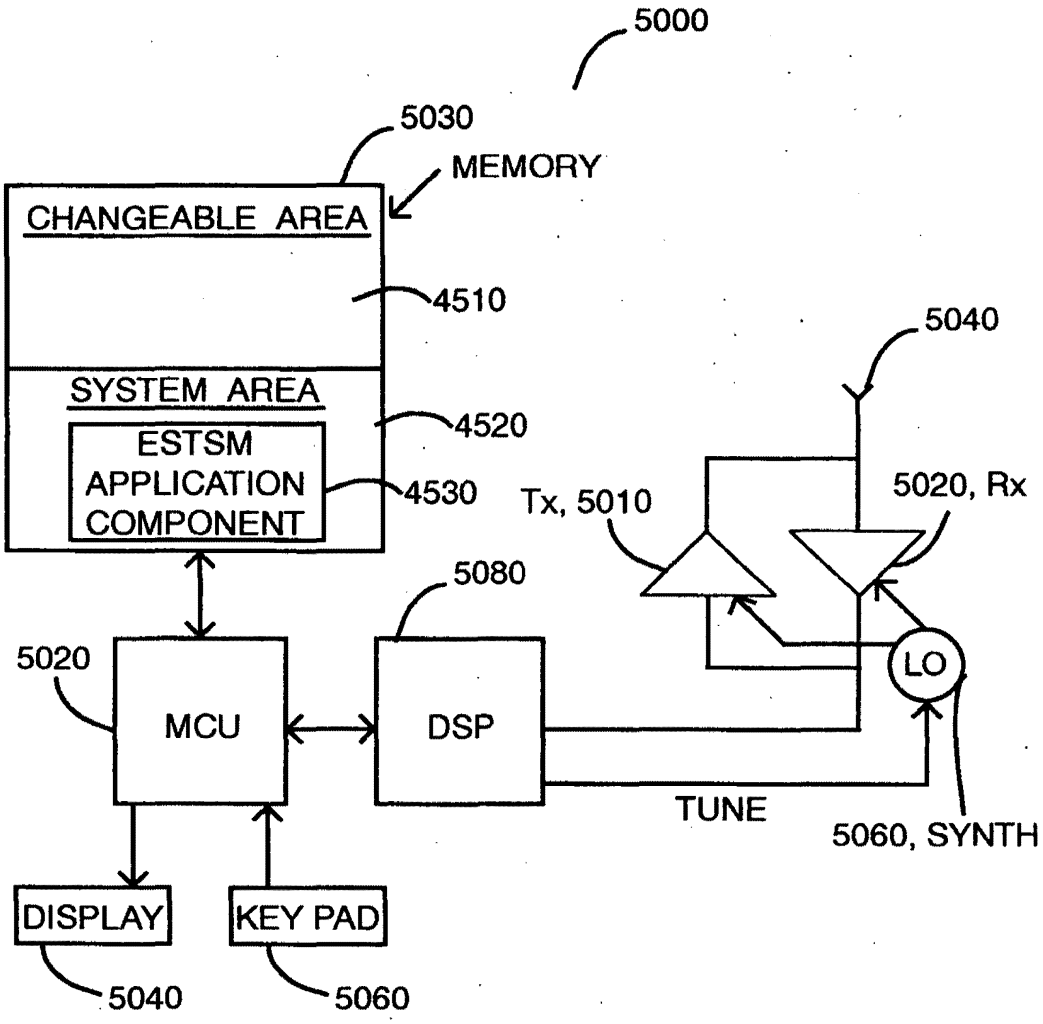

5000
5030
MEMORY
CHANGEABLE AREA
4510
SYSTEM AREA
4520
ESTSM
APPLICATION
COMPONENT
4530
5040
Tx, 5010
5020, Rx
5080
5020
MCU
DSP
LO
TUNE
5060, SYNTH
DISPLAY
KEY PAD
5040
5060

FIGURE 50

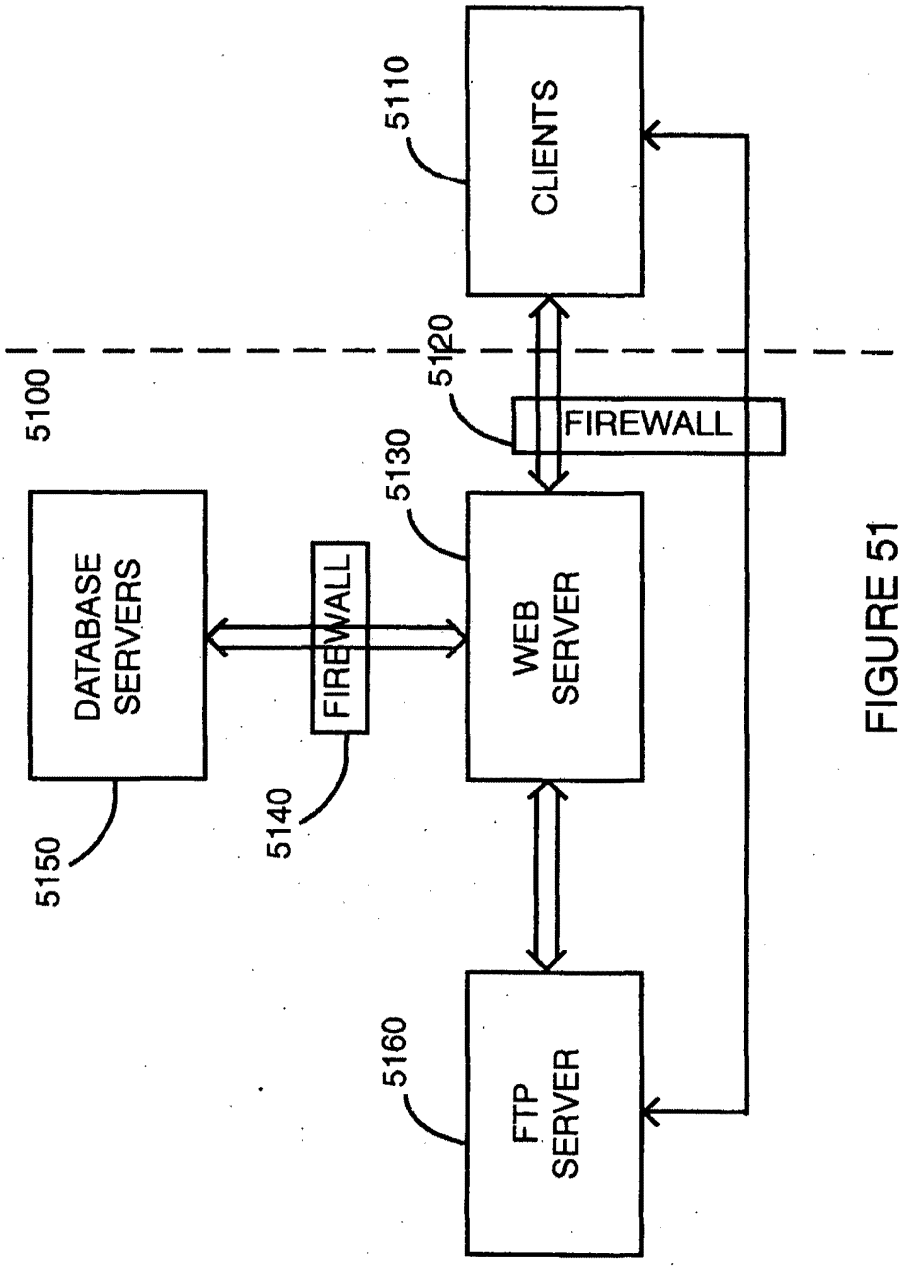

5110
CLIENTS
5120
FIREWALL
5100
5130
WEB SERVER
DATABASE SERVERS
FIREWALL
5140
5150
5160
FTP SERVER

FIGURE 51

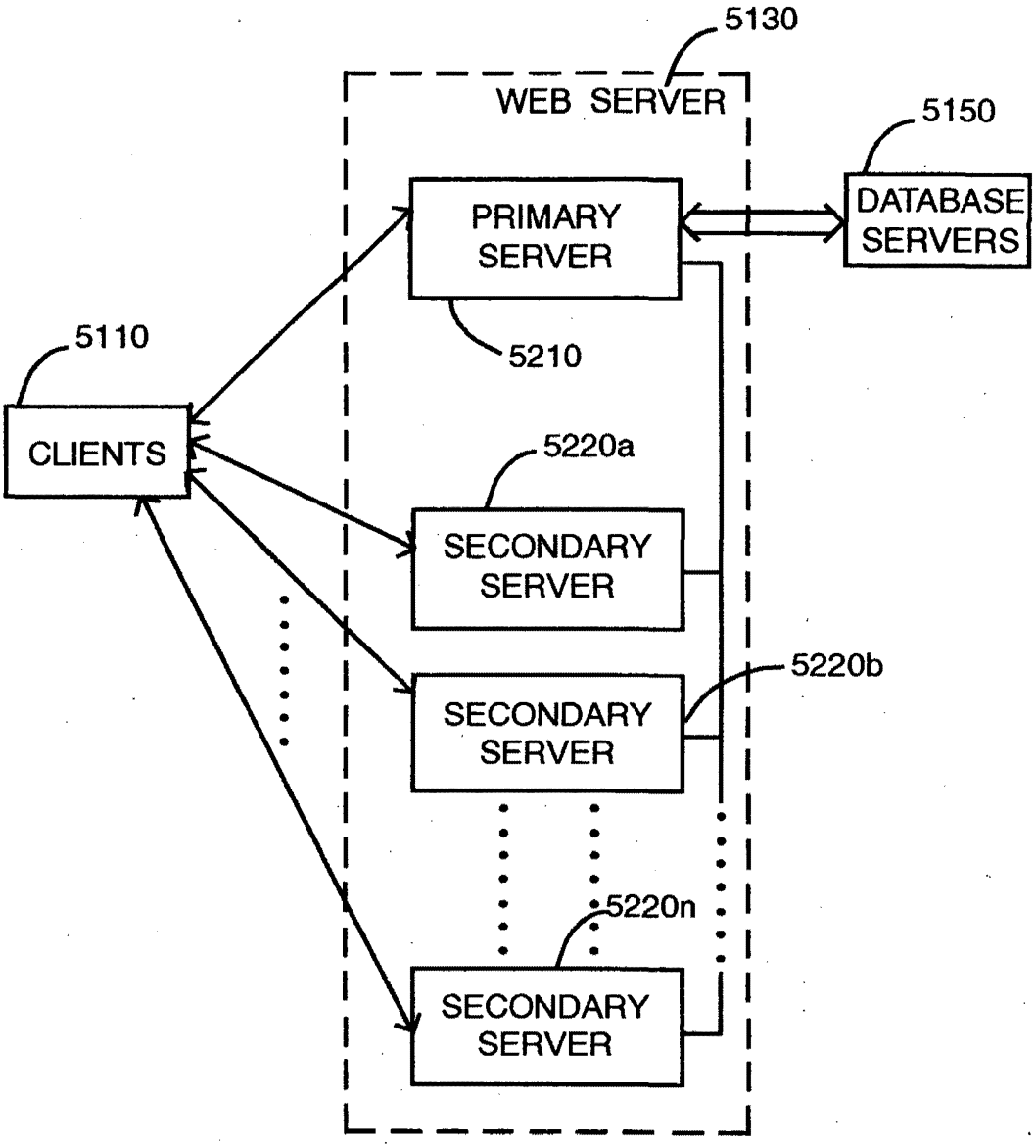

5130
WEB SERVER
5150
DATABASE SERVERS
PRIMARY SERVER
5210
5110
CLIENTS
5220a
SECONDARY SERVER
5220b
SECONDARY SERVER
5220n
SECONDARY SERVER

FIGURE 52

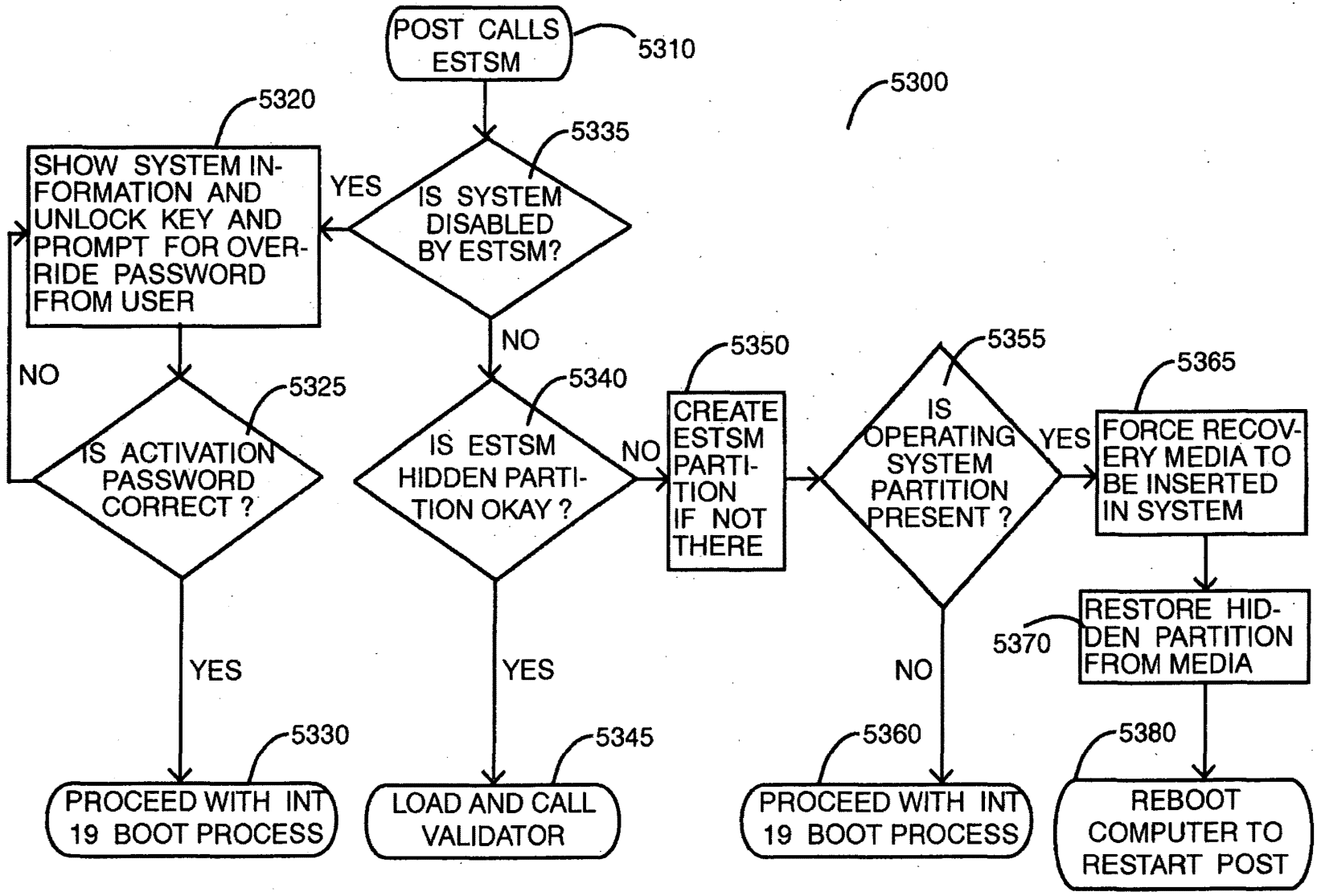

POST CALLS ESTSM
5310
5300
5320
SHOW SYSTEM INFORMATION AND UNLOCK KEY AND PROMPT FOR OVERRIDE PASSWORD FROM USER
5335
IS SYSTEM DISABLED BY ESTSM?
YES
NO
NO
5325
IS ACTIVATION PASSWORD CORRECT ?
5340
IS ESTSM HIDDEN PARTITION OKAY ?
NO
5350
CREATE ESTSM PARTITION IF NOT THERE
5355
IS OPERATING SYSTEM PARTITION PRESENT ?
YES
5365
FORCE RECOVERY MEDIA TO BE INSERTED IN SYSTEM
5370
RESTORE HIDDEN PARTITION FROM MEDIA
YES
YES
NO
5330
PROCEED WITH INT 19 BOOT PROCESS
5345
LOAD AND CALL VALIDATOR
5360
PROCEED WITH INT 19 BOOT PROCESS
5380
REBOOT COMPUTER TO RESTART POST

FIGURE 53

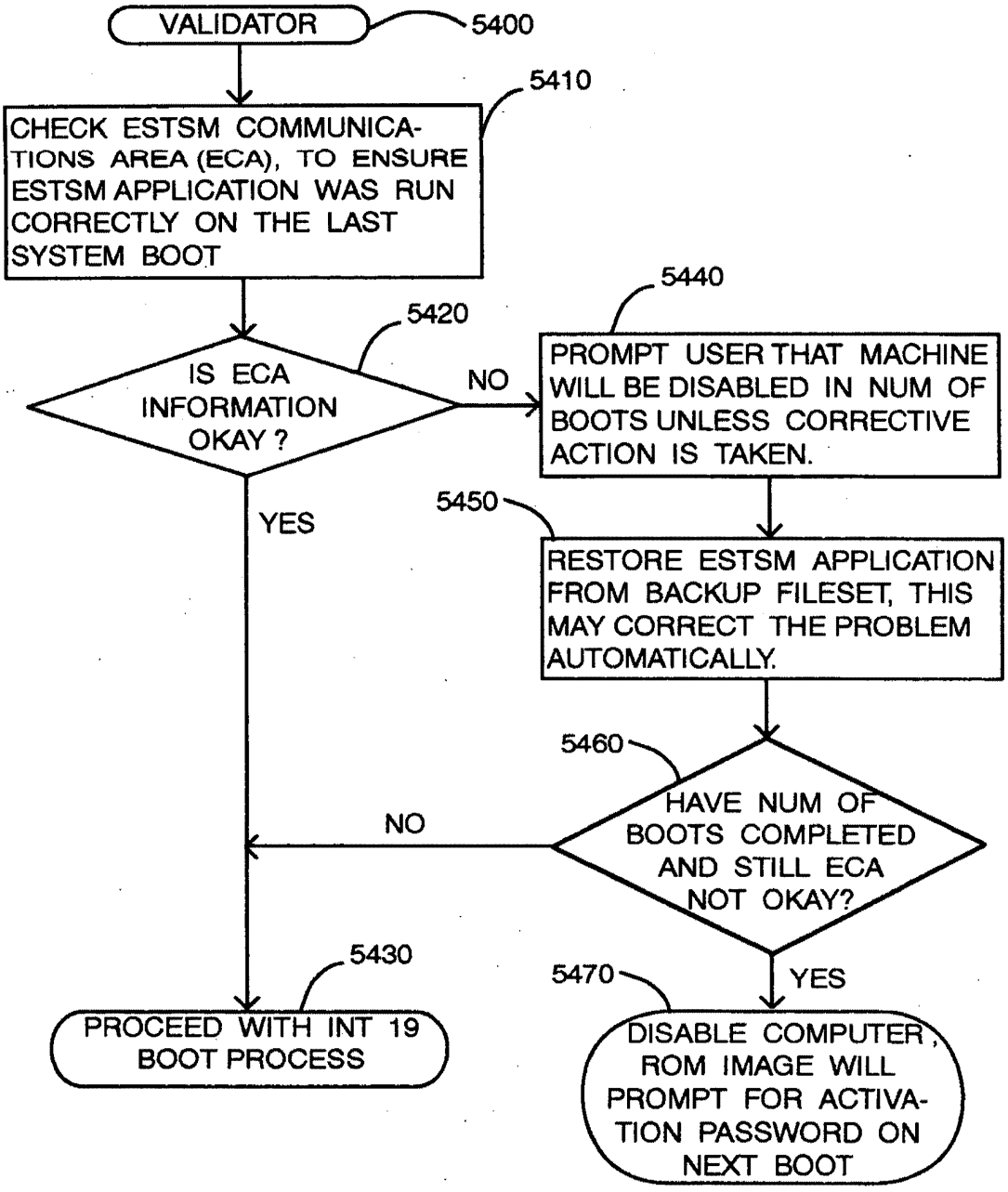

VALIDATOR
5400
5410
CHECK ESTSM COMMUNICATIONS AREA (ECA), TO ENSURE ESTSM APPLICATION WAS RUN CORRECTLY ON THE LAST SYSTEM BOOT
5420
IS ECA INFORMATION OKAY ?
NO
5440
PROMPT USER THAT MACHINE WILL BE DISABLED IN NUM OF BOOTS UNLESS CORRECTIVE ACTION IS TAKEN.
YES
5450
RESTORE ESTSM APPLICATION FROM BACKUP FILESET, THIS MAY CORRECT THE PROBLEM AUTOMATICALLY.
5460
HAVE NUM OF BOOTS COMPLETED AND STILL ECA NOT OKAY?
NO
YES
5430
PROCEED WITH INT 19 BOOT PROCESS
5470
DISABLE COMPUTER, ROM IMAGE WILL PROMPT FOR ACTIVATION PASSWORD ON NEXT BOOT

FIGURE 54

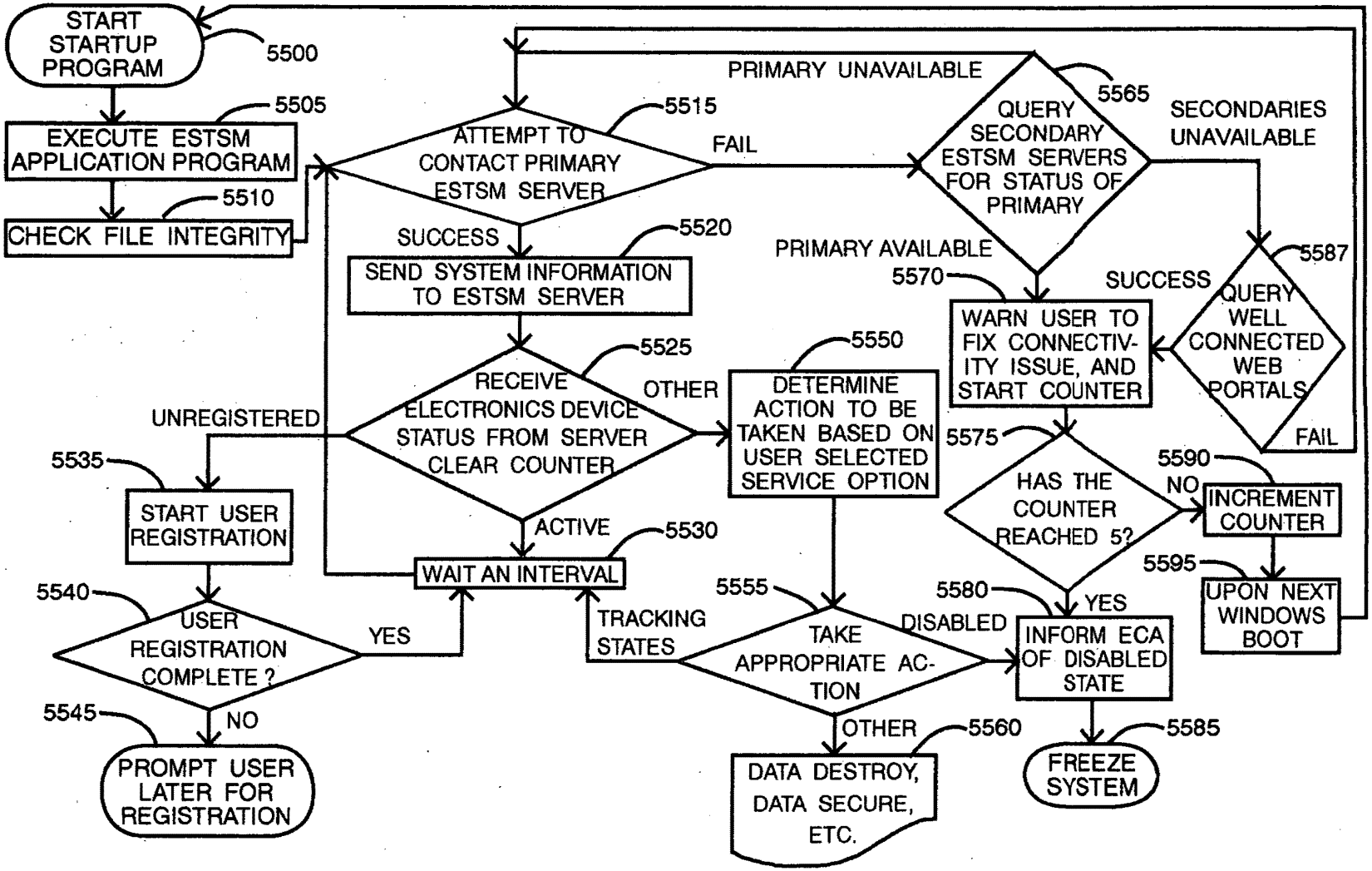


FIGURE 55

DELL EXHIBIT 1002
Page 130 of 659

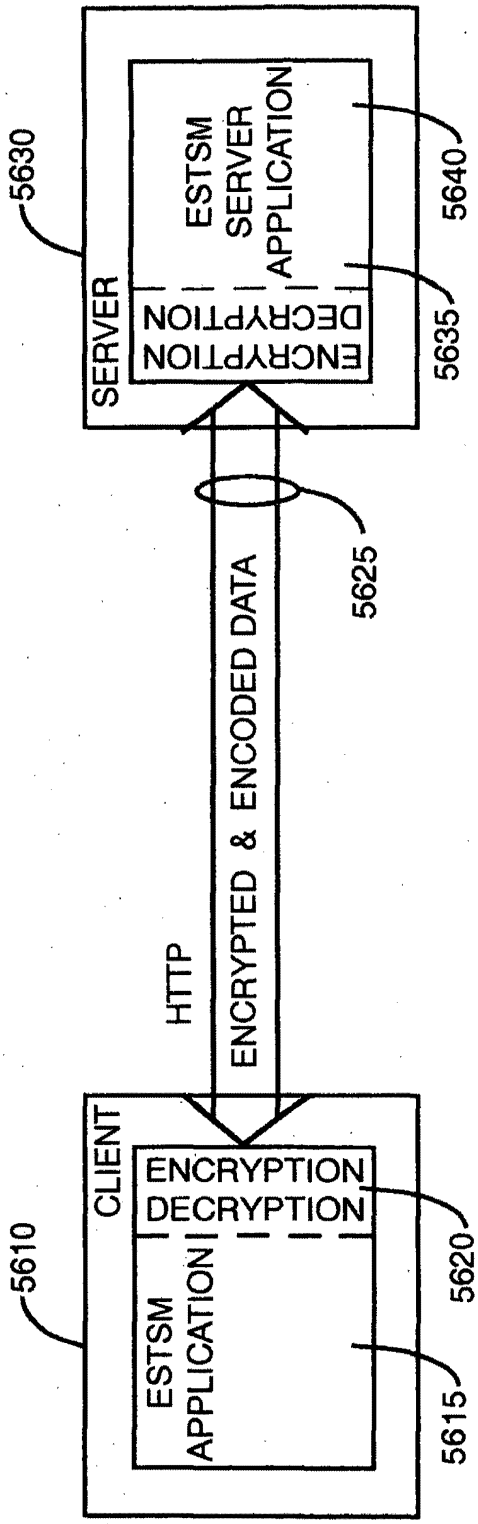

5630
SERVER
ESTSM SERVER APPLICATION
5640
ENCRYPTION DECRYPTION
5635
5625
HTTP
ENCRYPTED & ENCODED DATA
5610
CLIENT
ENCRYPTION DECRYPTION
5620
ESTSM APPLICATION
5615

FIGURE 56

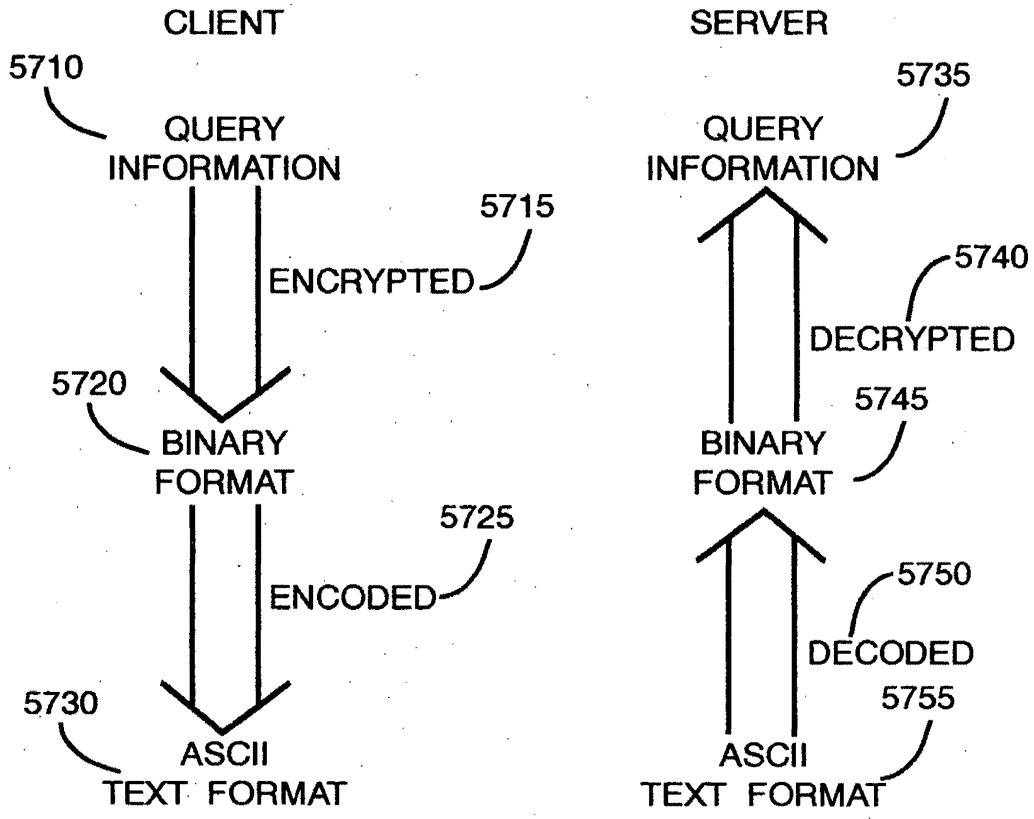

CLIENT
SERVER
5710
QUERY INFORMATION
5715
ENCRYPTED
5720
BINARY FORMAT
5725
ENCODED
5730
ASCII TEXT FORMAT
5735
QUERY INFORMATION
5740
DECRYPTED
5745
BINARY FORMAT
5750
DECODED
5755
ASCII TEXT FORMAT

FIGURE 57

ENCODE
(CALLS ENC (N < 8) FUNCTION)

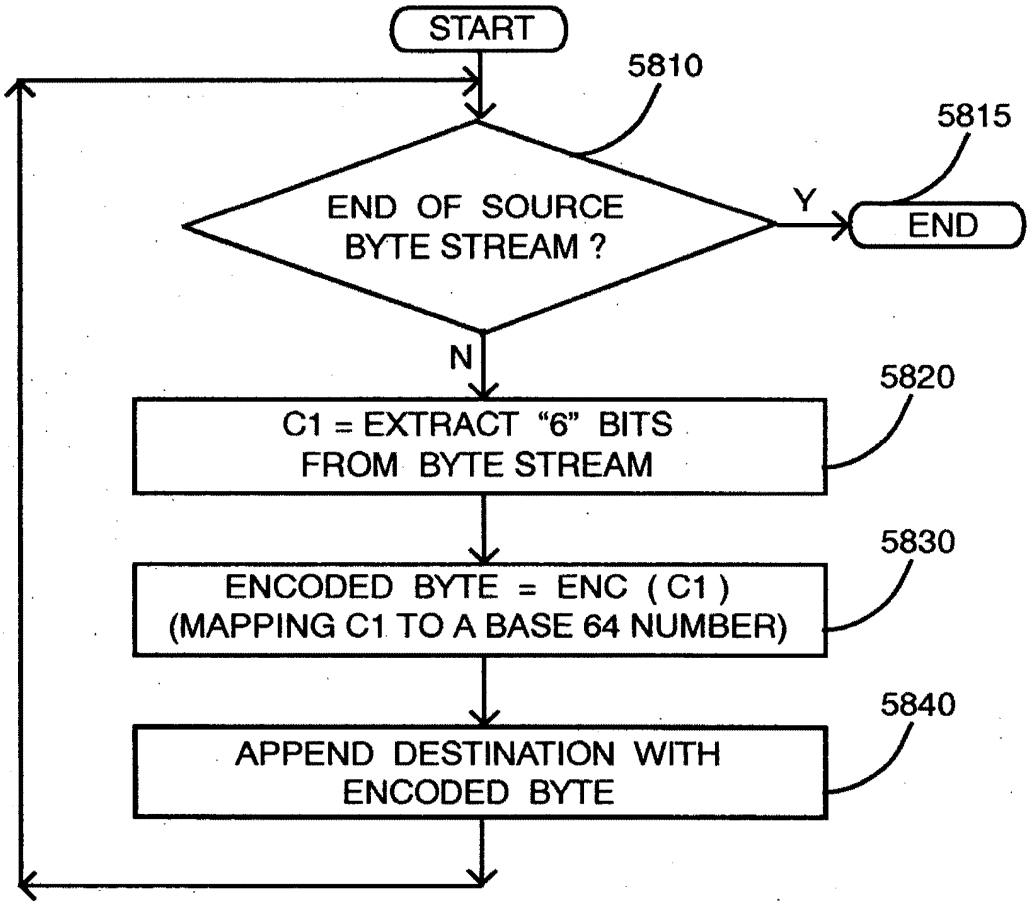


FIGURE 58

DECODE
(CALLS DECODE (N < 8) FUNCTION)

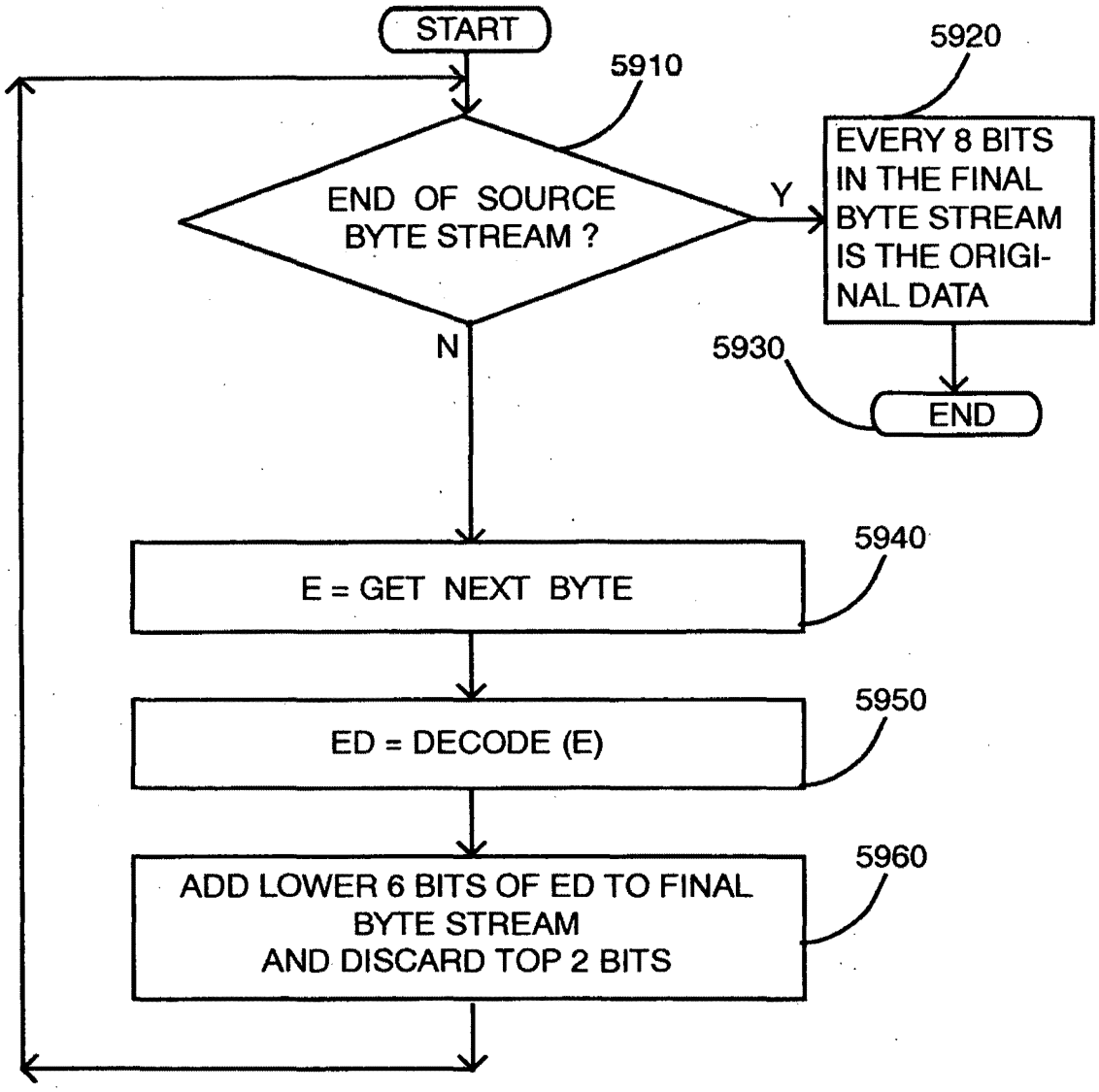


FIGURE 59

ENCRYPTION AND ENCODING OF SMS

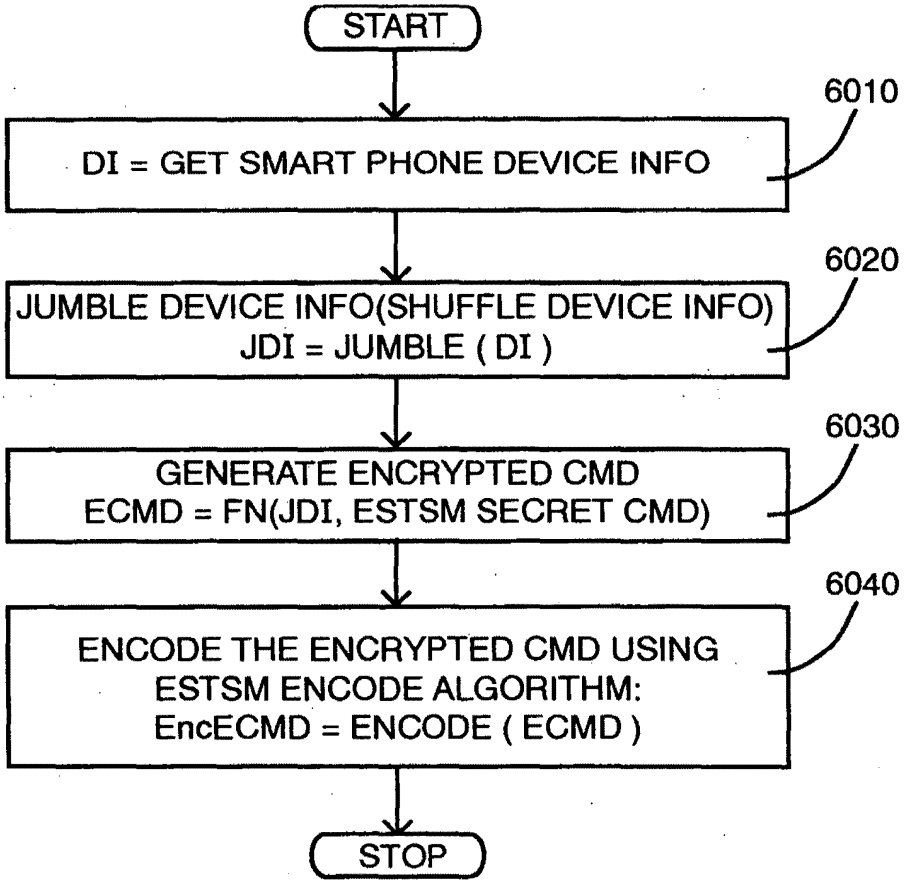


FIGURE 60

DECRYPTION AND DECODING OF SMS

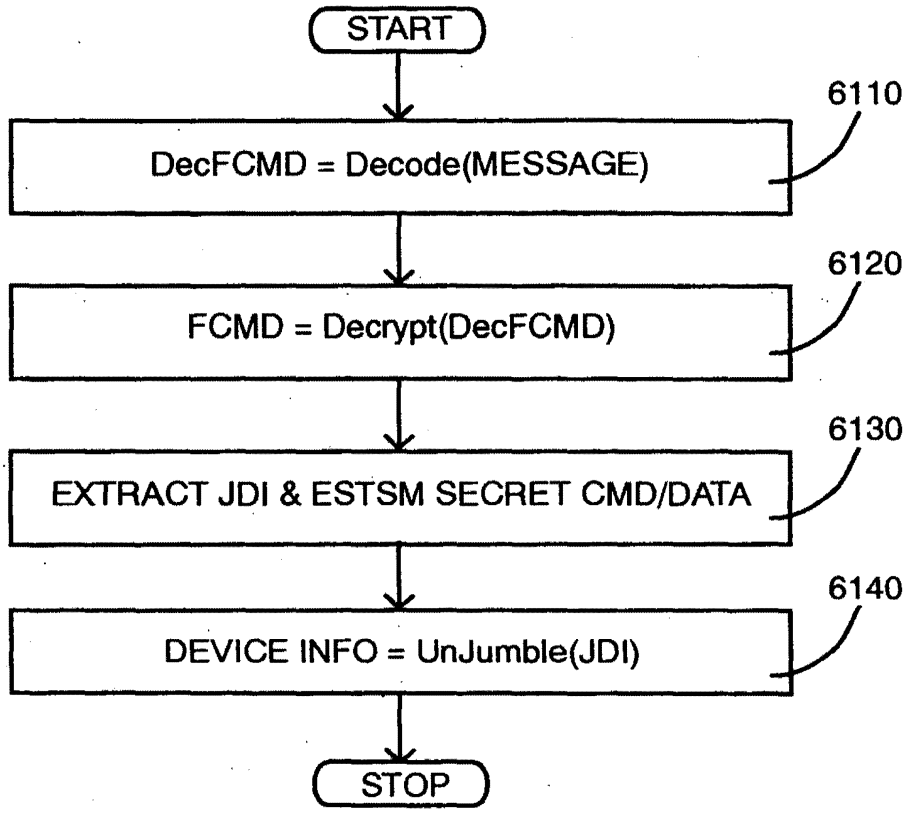


FIGURE 61

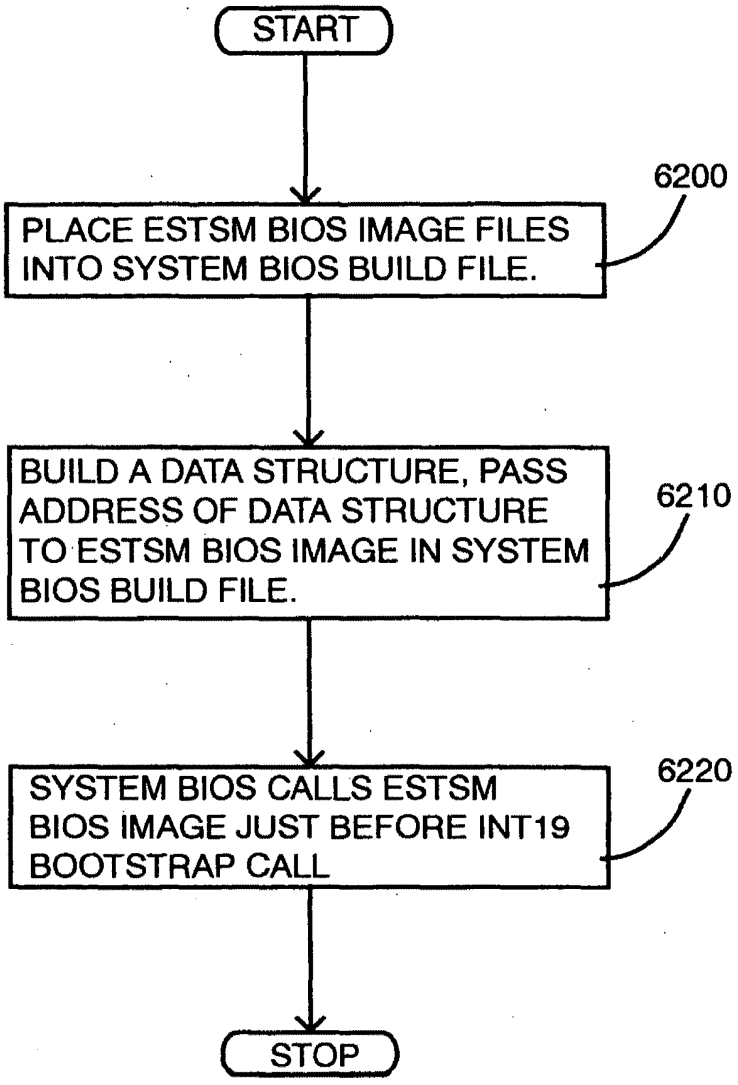

START
6200
PLACE ESTSM BIOS IMAGE FILES INTO SYSTEM BIOS BUILD FILE.
BUILD A DATA STRUCTURE, PASS ADDRESS OF DATA STRUCTURE TO ESTSM BIOS IMAGE IN SYSTEM BIOS BUILD FILE.
6210
SYSTEM BIOS CALLS ESTSM BIOS IMAGE JUST BEFORE INT19 BOOTSTRAP CALL
6220
STOP

FIGURE 62a

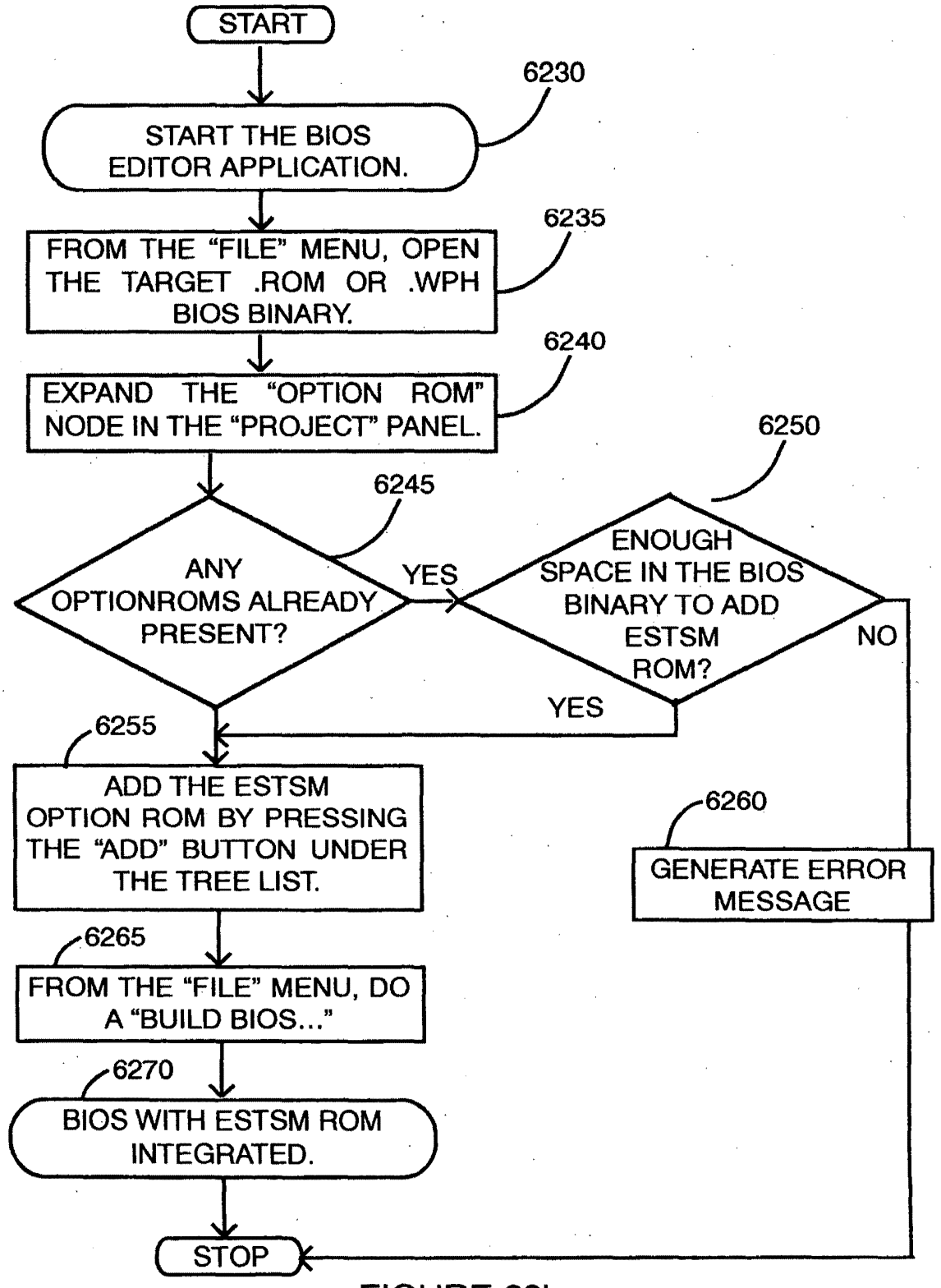

START
6230
START THE BIOS EDITOR APPLICATION.
6235
FROM THE "FILE" MENU, OPEN THE TARGET .ROM OR .WPH BIOS BINARY.
6240
EXPAND THE "OPTION ROM" NODE IN THE "PROJECT" PANEL.
6245
ANY OPTIONROMS ALREADY PRESENT?
YES
6250
ENOUGH SPACE IN THE BIOS BINARY TO ADD ESTSM ROM?
NO
YES
6255
ADD THE ESTSM OPTION ROM BY PRESSING THE "ADD" BUTTON UNDER THE TREE LIST.
6260
GENERATE ERROR MESSAGE
6265
FROM THE "FILE" MENU, DO A "BUILD BIOS..."
6270
BIOS WITH ESTSM ROM INTEGRATED.
STOP

FIGURE 62b

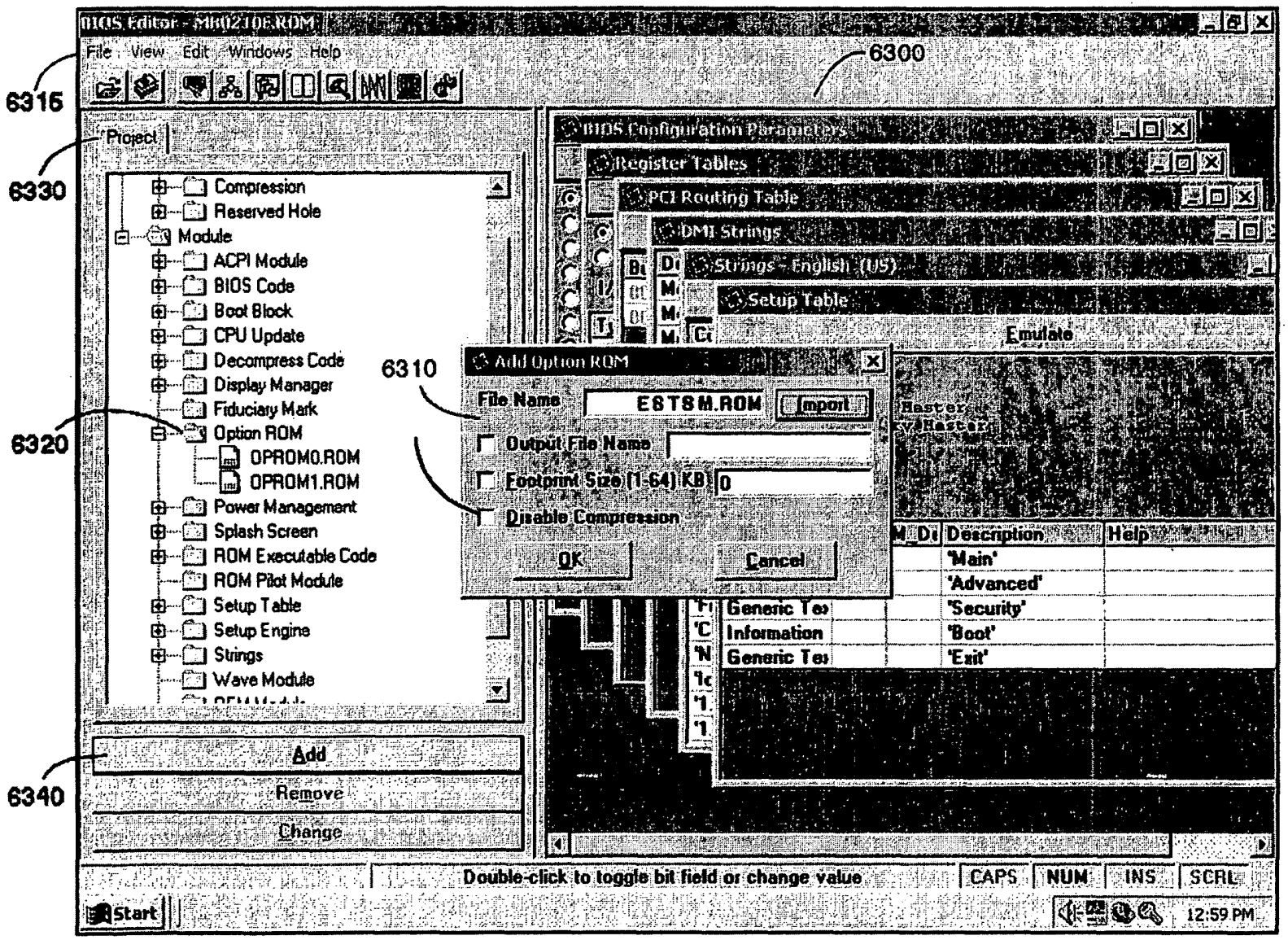

6315
6300
6330
6320
6310
6340
File View Edit Windows Help
Project
Compression
Reserved Hole
Module
ACPI Module
BIOS Code
Boot Block
CPU Update
Decompress Code
Display Manager
Fiduciary Mark
Option ROM
OPROM0.ROM
OPROM1.ROM
Power Management
Splash Screen
ROM Executable Code
ROM Pilot Module
Setup Table
Setup Engine
Strings
Wave Module
Add
Remove
Change
BIOS Configuration Parameters
Register Tables
PCI Routing Table
DMI Strings
Strings - English (US)
Setup Table
Emulate
Add Option ROM
File Name
E8TSM.ROM
Import
Output File Name
Footprint Size (1-64) KB
0
Disable Compression
OK
Cancel
Description
Help
'Main'
'Advanced'
'Security'
'Boot'
'Exit'
Generic Te
Information
Generic Te
Double-click to toggle bit field or change value
CAPS
NUM
INS
SCRL
Start
12:59 PM

FIGURE 63

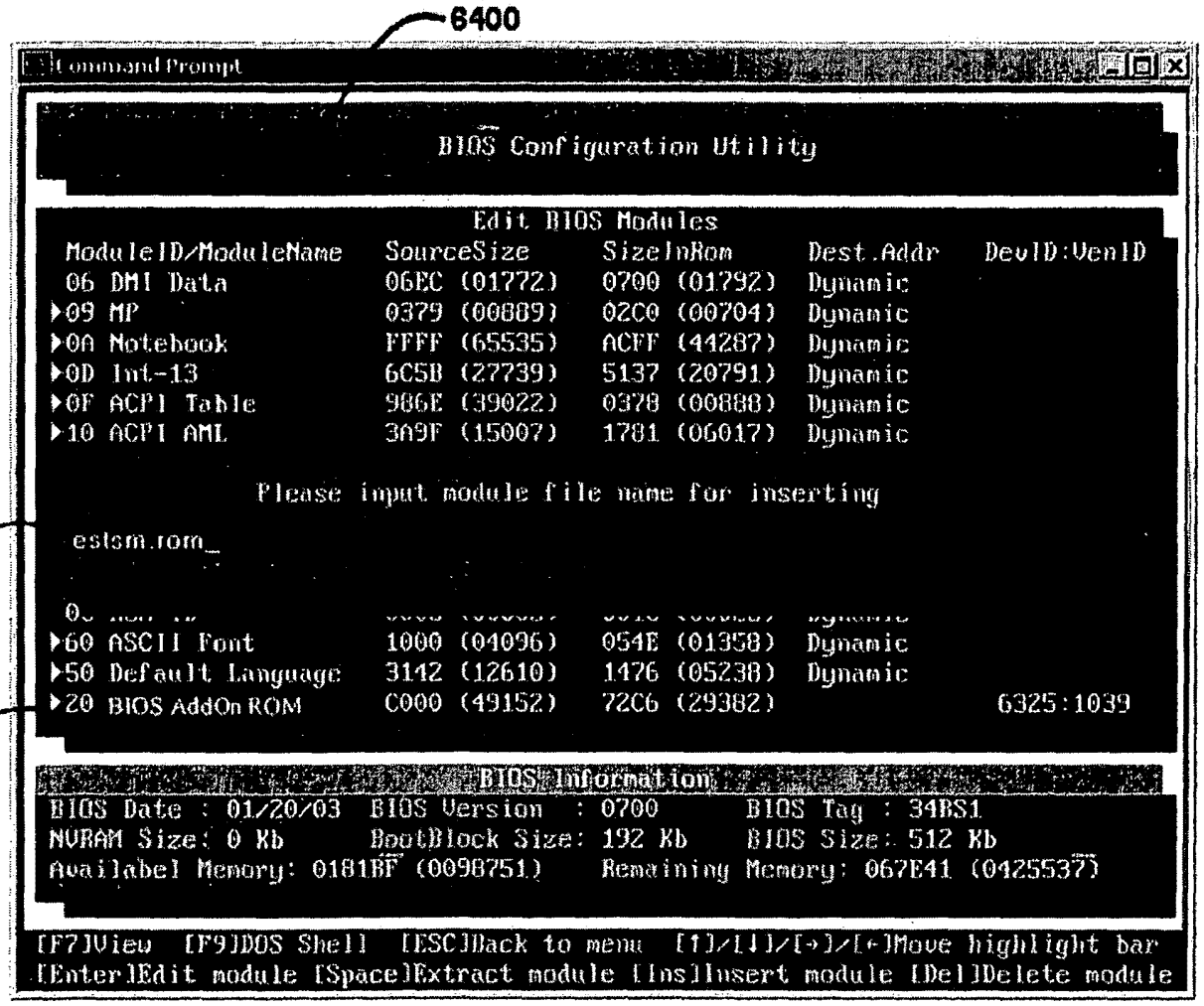


FIGURE 64

DELL EXHIBIT 1002
Page 140 of 659

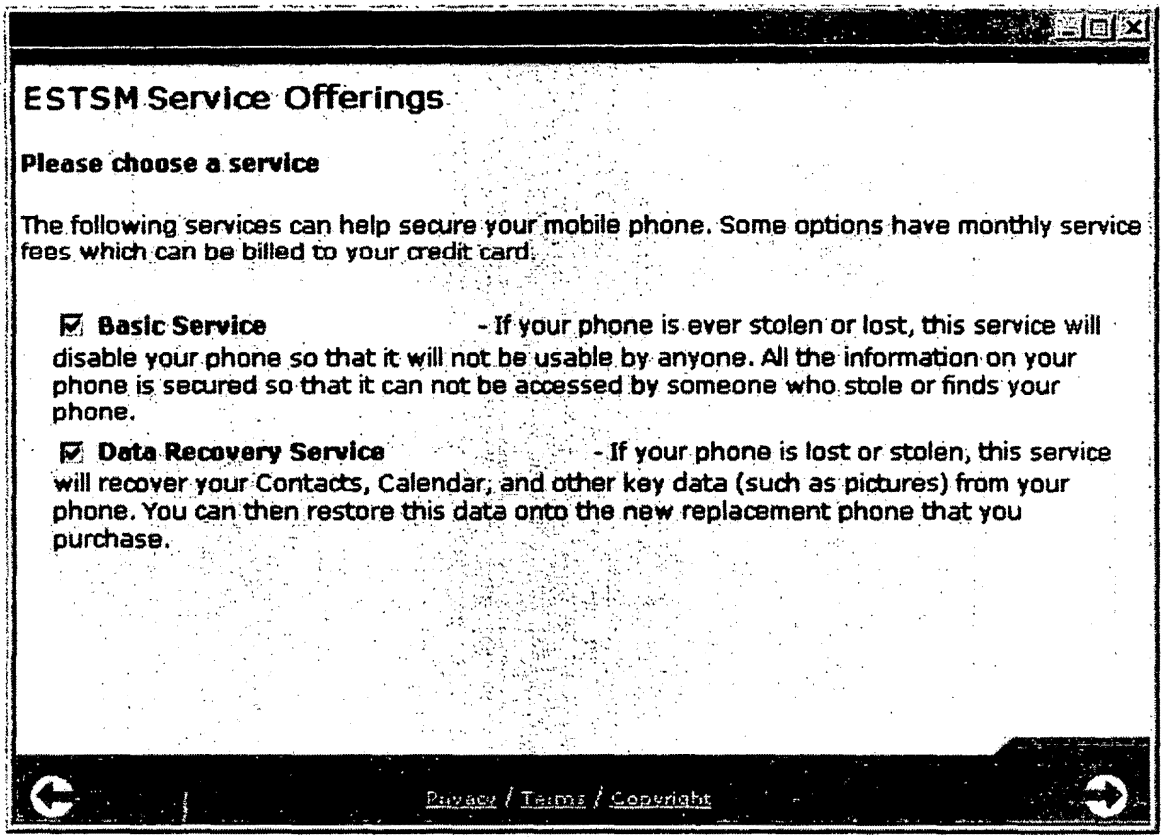

ESTSM Service Offerings
Please choose a service
The following services can help secure your mobile phone. Some options have monthly service fees which can be billed to your credit card.
Basic Service - If your phone is ever stolen or lost, this service will disable your phone so that it will not be usable by anyone. All the information on your phone is secured so that it can not be accessed by someone who stole or finds your phone.
Data Recovery Service - If your phone is lost or stolen, this service will recover your Contacts, Calendar, and other key data (such as pictures) from your phone. You can then restore this data onto the new replacement phone that you purchase.
Privacy / Terms / Copyright

FIGURE 65

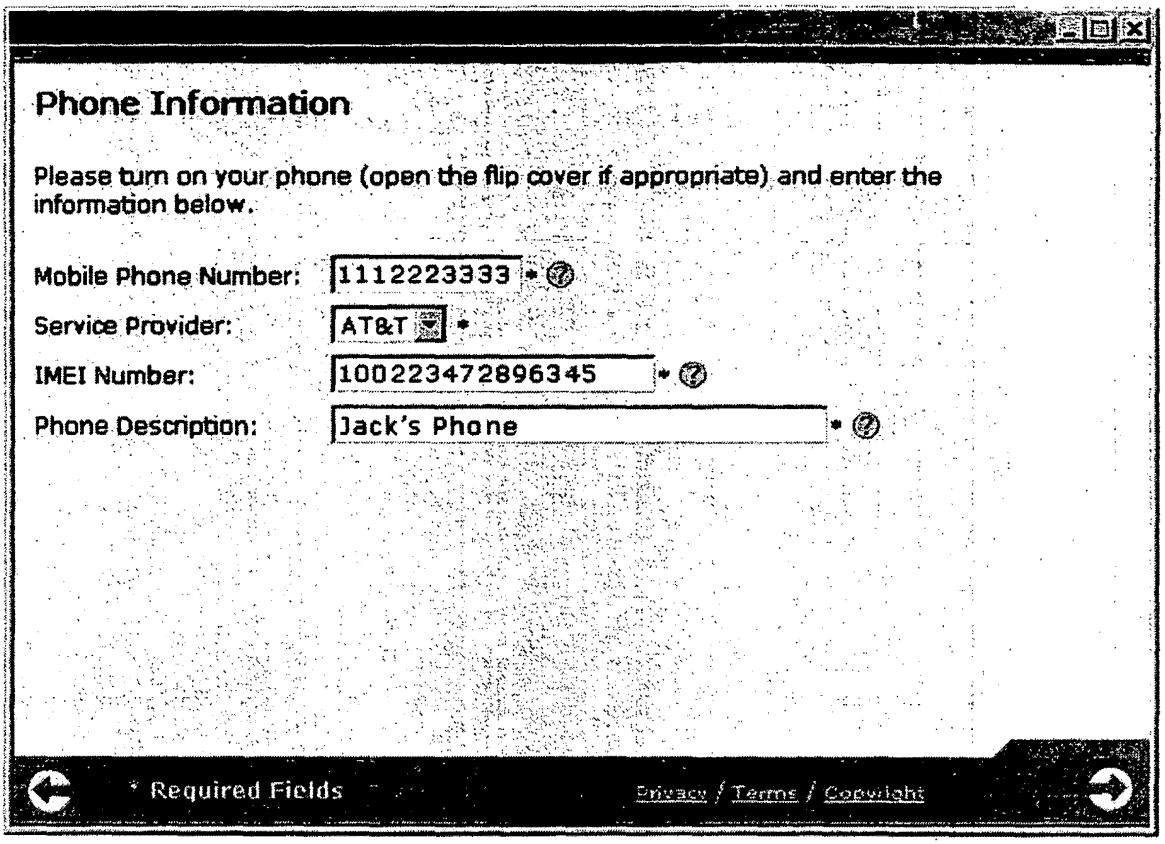

Phone Information
Please turn on your phone (open the flip cover if appropriate) and enter the information below.
Mobile Phone Number:
1112223333
Service Provider:
AT&T
IMEI Number:
100223472896345
Phone Description:
Jack's Phone
* Required Fields
Privacy / Terms / Copyright

FIGURE 66

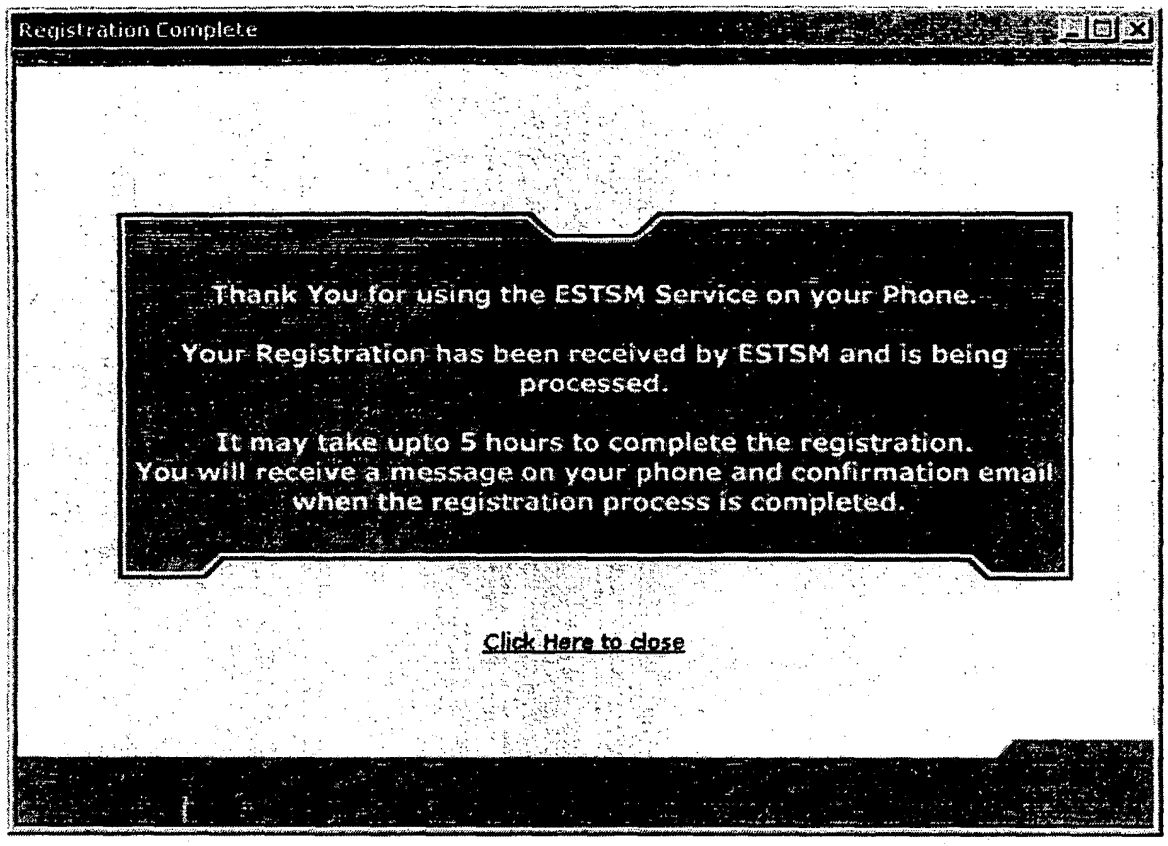

Registration Complete
Thank You for using the ESTSM Service on your Phone.
Your Registration has been received by ESTSM and is being processed.
It may take upto 5 hours to complete the registration.
You will receive a message on your phone and confirmation email when the registration process is completed.
Click Here to close

FIGURE 67

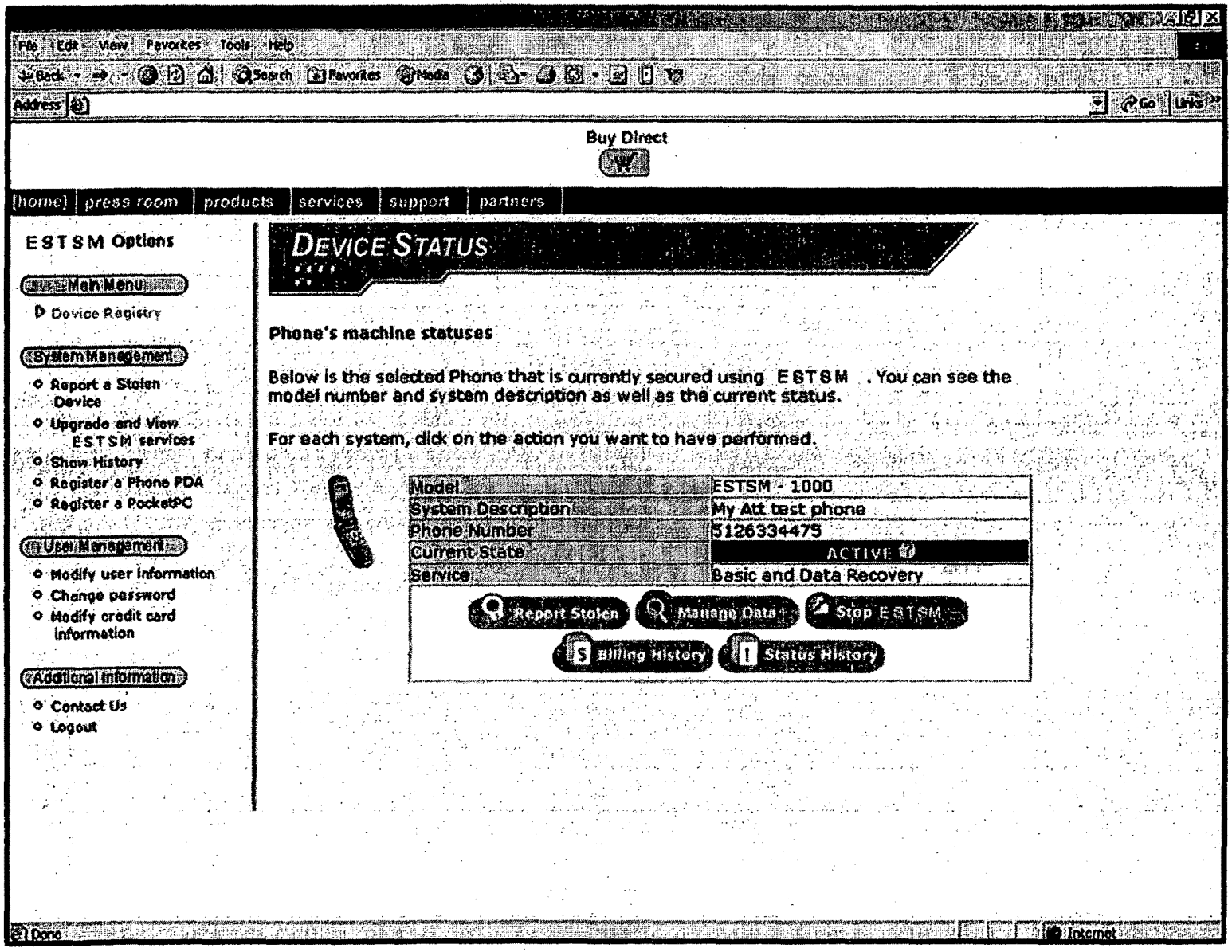


FIGURE 68

DELL EXHIBIT 1002
Page 144 of 659

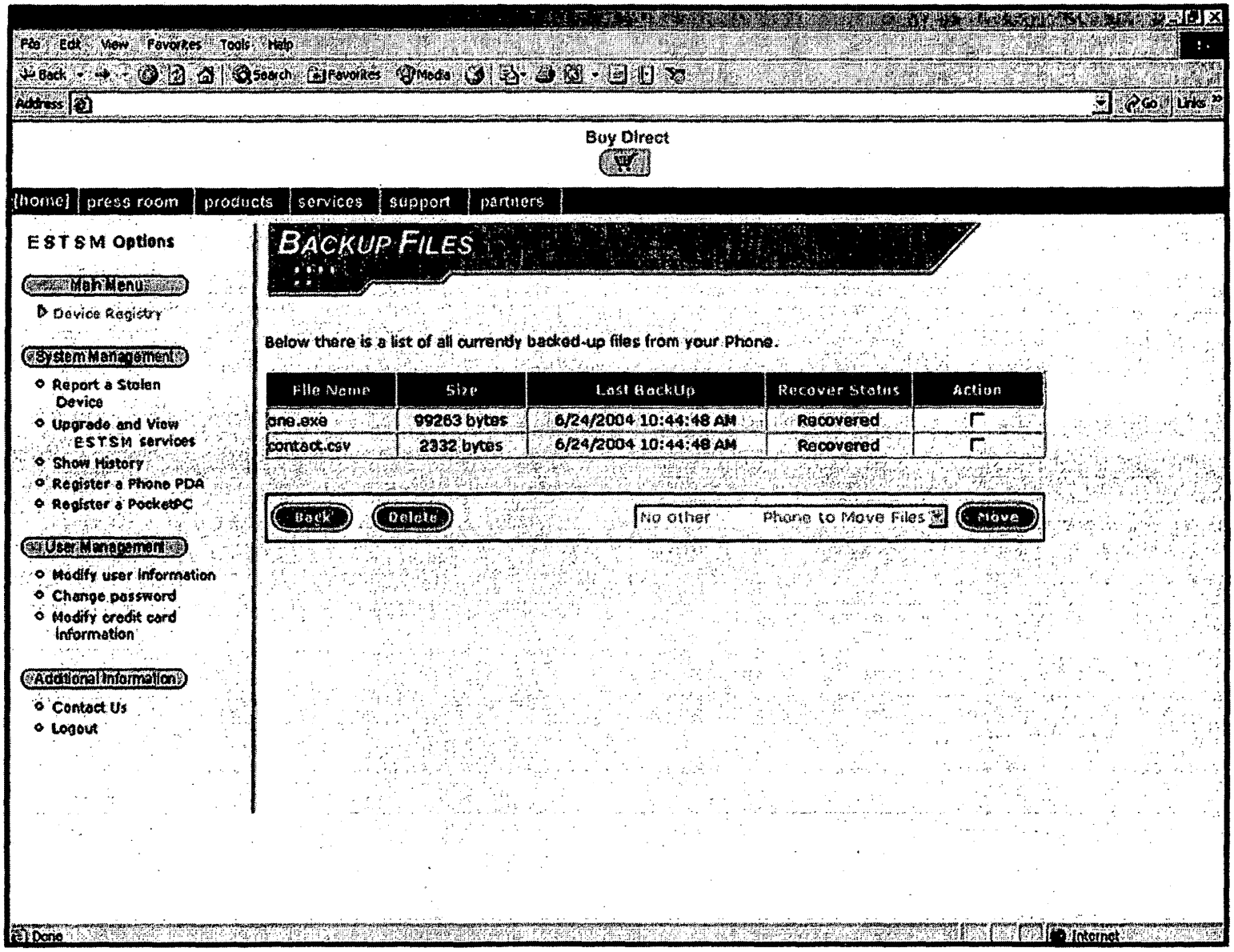

File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
Buy Direct
[home] press room products services support partners
ESTSM Options
Main Menu
Device Registry
System Management
Report a Stolen Device
Upgrade and View ESTSM services
Show History
Register a Phone PDA
Register a PocketPC
User Management
Modify user information
Change password
Modify credit card information
Additional Information
Contact Us
Logout
BACKUP FILES
Below there is a list of all currently backed-up files from your Phone.
File Name | Size | Last BackUp | Recover Status | Action
one.exe | 99263 bytes | 6/24/2004 10:44:48 AM | Recovered
contact.csv | 2332 bytes | 6/24/2004 10:44:48 AM | Recovered
Back
Delete
No other Phone to Move Files
Move
Done
Internet

FIGURE 69

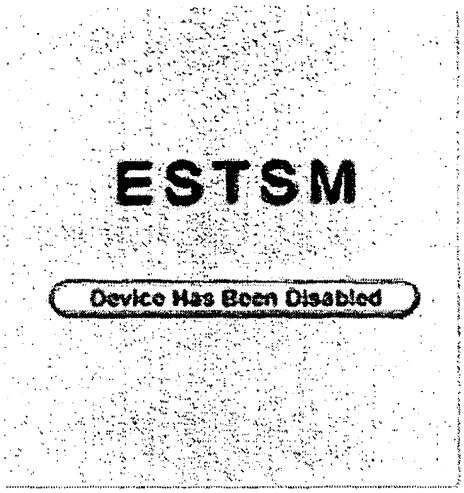


FIGURE 70

CONTROL FLOW DIAGRAM FOR MOBILE DEVICES

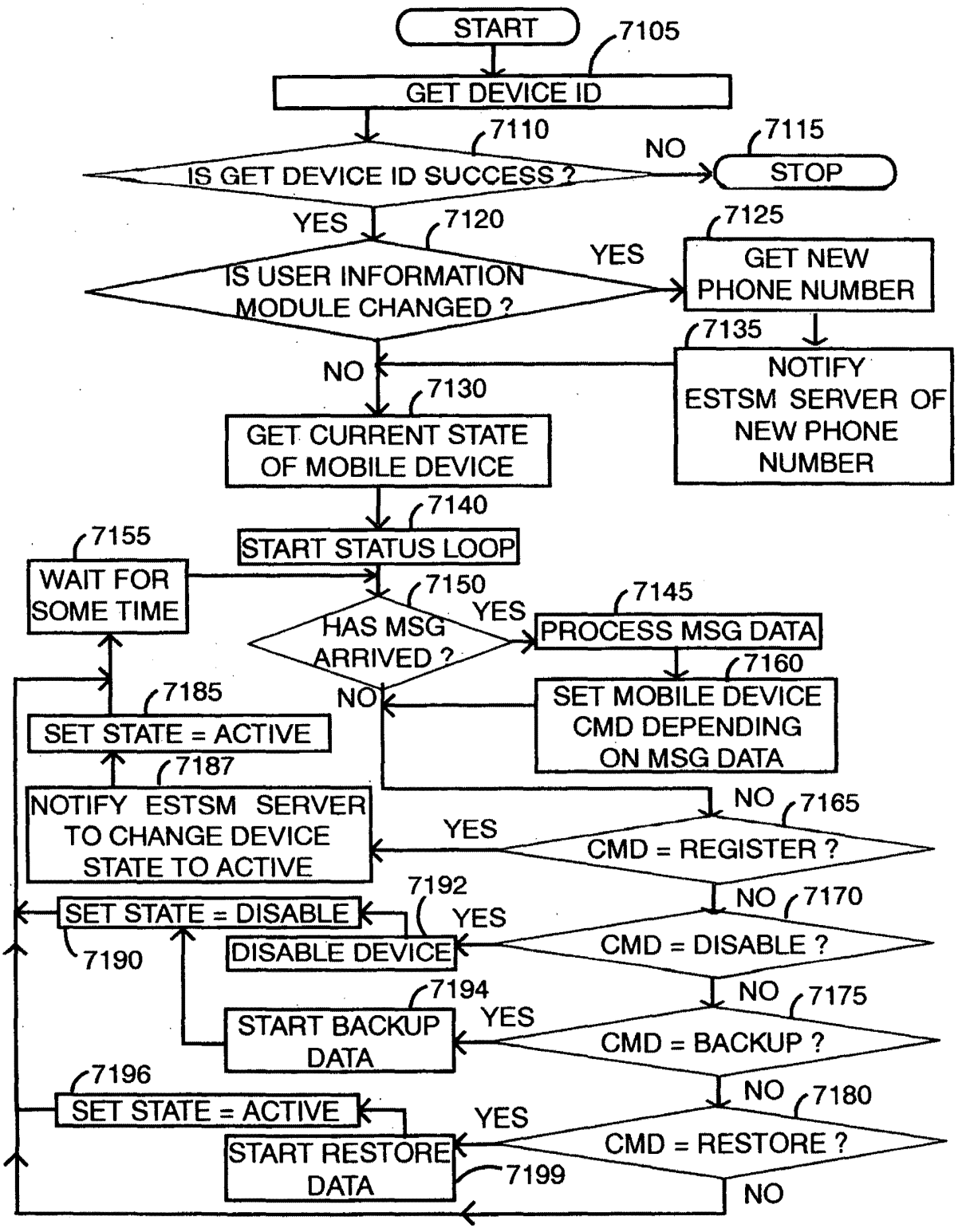


FIGURE 71

STATE DIAGRAM FOR MOBILE DEVICES

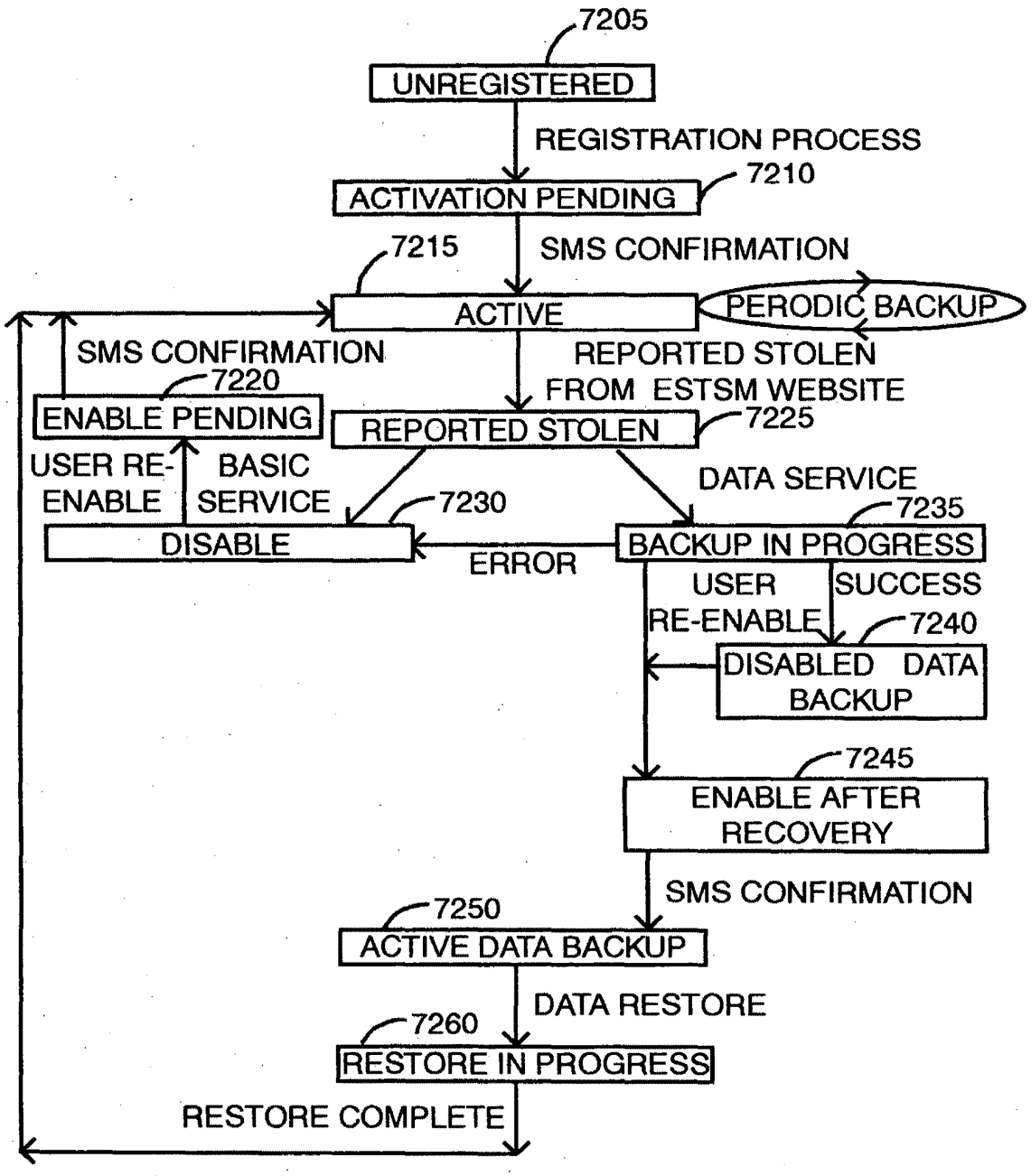


FIGURE 72

Docket No.
SOFP:101US

Declaration and Power of Attorney For Patent Application

English Language Declaration

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled
ELECTRONIC DEVICE SECURITY AND TRACKING SYSTEM AND METHOD

the specification of which

(check one)

☒ is attached hereto.

☐ was filed on _____ as United States Application No. or PCT International Application Number _____

and was amended on _____
(if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or (f), or 365(b) of any foreign application(s) for patent, or plant breeder's rights certificate(s), or 365(a) of any PCT International application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent, inventor's or plant breeder's rights certificate(s), or any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s)			Priority Not Claimed
(Number)	(Country)	(Day/Month/Year Filed)	☐
(Number)	(Country)	(Day/Month/Year Filed)	☐
(Number)	(Country)	(Day/Month/Year Filed)	☐

BEST AVAILABLE COPY

I hereby claim the benefit under 35 U.S.C. Section 119(e) of any United States provisional application(s) listed below:

60/497,182	08/23/2003
(Application Serial No.)	(Filing Date)
(Application Serial No.)	(Filing Date)
(Application Serial No.)	(Filing Date)

I hereby claim the benefit under 35 U. S. C. Section 120 of any United States application(s), or Section 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. Section 112, I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, C. F. R., Section 1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application:

(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)
(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)
(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

BEST AVAILABLE COPY

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. *(list name and registration number)*

Indranil CHOWDHURY Reg. No. 47,490

Send Correspondence to: **Attn: Apurva M. Bhansali**
Softex, Inc.
9300 Jollyville Rd.; Suite 201
Austin, TX 78759

Direct Telephone Calls to: *(name and telephone number)*
Indranil CHOWDHURY (281) 980-0259

Full name of sole or first inventor **Apurva Mahendrakumar Bhansali**
Sole or first inventor's signature Date 8/17/04
Residence **U.S.A.**
Citizenship **U.S.A.**
Post Office Address **7205 Foxtree Cove**
Austin, TX 78750-7919

Full name of second inventor, if any **Manoj Kumar Jain**
Second inventor's signature Date 08/17/04
Residence **U.S.A.**
Citizenship **India**
Post Office Address **11113 Comiso Pala Path**
Austin TX 78726

BEST AVAILABLE COPY

Full name of third inventor, if any
Shradha Dube

Third inventor's signature
Shradha Dube

Date
17th Aug '04

Residence
U.S.A.

Citizenship
India

Post Office Address
11113 Comiso Pala Path

Austin, TX 78726

Full name of fourth inventor, if any
Gayathri Rangarajan

Fourth inventor's signature

Date
AUG/17/2004

Residence
U.S.A.

Citizenship
India

Post Office Address
13401 Metric Blvd.; Apt. 323

Austin, TX 78727

Full name of fifth inventor, if any
Mehul Ramjibhai Patel

Fifth inventor's signature

Date
08/17/04

Residence
U.S.A.

Citizenship
India

Post Office Address
2801 Wells Branch Pkwy #1431

Austin, TX 78728

Full name of sixth inventor, if any
Rayesh Kashinath Raikar

Sixth inventor's signature

Date
08/18/04

Residence
U.S.A.

Citizenship
India

Post Office Address
9500 Jollyville Road; Apt. 283

Austin, TX 78759

BEST AVAILABLE COPY

Full name of seventh inventor, if any
Kamal Mansukhlal Dhanani

Seventh inventor's signature

Date
08/18/04

Residence
U.S.A.

Citizenship
India

Post Office Address
12349 Metric Blvd. #414

Austin, TX 78758

Full name of eighth inventor, if
Ranjit Kapila

Eighth inventor's signature

Date
8/18/04

Residence
U.S.A.

Citizenship
U.S.A.

Post Office Address
10300 Jollyville Rd.; Apt. 724

Austin, TX 78759

Full name of ninth inventor, if any
Elza Abraham

Ninth inventor's signature

Date

Residence
U.S.A.

Citizenship
India

Post Office Address
1333 Eldridge Pkwy.; Apt. 1312

Houston, TX 77077

Full name of tenth inventor, if any
Thomas David Tucker

Tenth inventor's signature

Date
8-17-2004

Residence
U.S.A.

Citizenship
U.S.A.

Post Office Address
10505 South IH 35 ; Apt. 2236

Austin, TX 78747

BEST AVAILABLE COPY

Full name of seventh inventor, if any
Kamal Manmukhlal Dhanani

Seventh inventor's signature — Date

Residence
U.S.A.

Citizenship
India

Post Office Address
12349 Metric Blvd. #414

Austin, TX 78758

Full name of eighth inventor, if
Ranjit Kapilla

Eighth inventor's signature — Date

Residence
U.S.A.

Citizenship
U.S.A.

Post Office Address
10300 Jollyville Rd.; Apt. 724

Austin, TX 78759

Full name of ninth inventor, if any
Elza Abraham VARGHESE

Ninth inventor's signature — Date
Elza Abraham Varghese — 8/17/04

Residence
U.S.A.

Citizenship
India

Post Office Address
1333 Eldridge Pkwy.; Apt. 1312

Houston, TX 77077

Full name of tenth inventor, if any
Thomas David Tucker

Tenth inventor's signature — Date

Residence
U.S.A.

Citizenship
U.S.A.

Post Office Address
10505 South IH 35 ; Apt. 2236

Austin, TX 78747

BEST AVAILABLE COPY

PATENT APPLICATION SERIAL NO. _____

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE
FEE RECORD SHEET

07/13/2006 MBERHE 00000005 11484100

01 FC:2011	150.00	OP
02 FC:2111	250.00	OP
03 FC:2311	100.00	OP
04 FC:2202	800.00	OP
05 FC:2201	500.00	OP
06 FC:2081	125.00	OP

PTO-1556
(5/87)

*U.S. Government Printing Office: 2002 — 489-267/69033

PTO/SB/06 (12-04)
Approved for use through 7/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875 Effective December 8, 2004

Application or Docket Number: 11484100

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	150.00		N/A	300.00
SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A	$250		N/A	$500
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	$100		N/A	$200
TOTAL CLAIMS (37 CFR 1.16(i))	52 minus 20 =	32	X$ 25 =	800	OR	X$50 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	8 minus 3 =	5	X100 =	500		X200 =	
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			125			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))			+180=			+360=	
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	1925		TOTAL	

APPLICATION AS AMENDED – PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	X$ 25 =		OR	X$50 =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X100 =		OR	X200 =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					+180=		OR	+360=	
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	X$ 25 =		OR	X$50 =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X100 =		OR	X200 =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					+180=		OR	+360=	
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2

U.S. UTILITY PATENT APPLICATION
ATTORNEY DOCKET NO. SOFP:115US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In the Matter of United States Patent Application:

Applicant(s): BHANSALI et al. Examiner: TBA

Application No.: TBA Art Unit: TBA

Filed: July 11, 2006

For: **ELECTRONIC DEVICE SECURITY AND TRACKING SYSTEM AND METHOD**

Certificate of Mailing by Express Mail
I certify that this Information Disclosure Statement is being deposited on July 11, 2006 with the U.S. Postal Service as "Express Mail Post Office to Addressee" service under 37 C.F.R. §1.10 and is addressed to the Commissioner for Patents, PO Box 1450, Alexandria, VA 22313-1450.

Indranil Chowdhury, Esq.
Registration No. 47, 490

INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Honorable Sir:

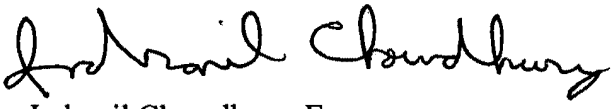
This Information Disclosure Statement is submitted in compliance with 37 C.F.R. §§ 1.56 and 1.97 through 1.98.

Record is attached of published art for consideration during prosecution of the above-identified patent application. No representation is made or intended that a search has been made or, if made, was complete, or that no more pertinent art than that listed is available. It is expected that the Patent and Trademark Office will conduct an independent search for relevant prior art.

Unless otherwise indicated, or unless references cited are U.S. patents or patent application publications, a full text copy of the entire reference of published art is attached. Where specifically indicated, an equivalent English language patent or publication is attached in lieu of the translation.

In accordance with the Patent and Trademark Office Notice of August 15, 1980, also enclosed is a completed Form PTO-A820 (Form PTO-1449).

Respectfully submitted,



Indranil Chowdhury, Esq.
Registration No. 47, 490
Attorney for Applicants
Tel. No. (281) 980-0259

Attn: Apurva M. Bhansali
Softex, Inc.
9300 Jollyville Rd.
Suite 201
Austin, TX 78759

Dated: July 11, 2006

Enclosures

DELL EXHIBIT 1002
Page 158 of 659

PTO/SB/08A (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	TBA
Filing Date	July 11, 2006
First Named Inventor	Apurva M. Bhansali
Art Unit	TBA
Examiner Name	TBA
Attorney Docket Number	SOFP:115US

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US- 5,715,174	02/03/1998	Cotichini et al.	
		US- 5,764,892	06/09/1998	Cain et al.	
		US- 5,802,280	09/01/1998	Cotichini et al.	
		US- 6,244,758 B1	06/12/2001	Solymar et al.	
		US- 6,269,392 B1	07/31/2001	Cotichini et al.	
		US- 6,300,863 B1	10/09/2001	Cotichini et al.	
		US- 6,507,914 B1	01/14/2003	Cain et al.	
		US- 20020194500	12/19/2002	Bajikar	
		US- 20030172306	09/11/2003	Cain et al.	
		US- 20030005316	01/02/2003	Girard	
		US- 20050216757 A1	09/29/2005	Gardner	
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

15866
071106
U.S. PTO

PTO/SB/05 (09-04)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office. U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.	SOFP:115US
First Inventor	Apurva M. Bhansali
Title	Electronic Device Security ...
Express Mail Label No.	EQ112282385US

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

1. [✓] **Fee Transmittal Form** (e.g., PTO/SB/17)
   (Submit an original and a duplicate for fee processing)
2. [✓] **Applicant claims small entity status.** See 37 CFR 1.27.
3. [✓] **Specification** [*Total Pages* 66]
   Both the claims and abstract must start on a new page
   (For information on the preferred arrangement, see MPEP 608.01(a))
4. [✓] **Drawing(s)** (*35 U.S.C. 113*) [*Total Sheets* 79]
5. **Oath or Declaration** [*Total Sheets* 6]
   a. [ ] Newly executed (original or copy)
   b. [✓] A copy from a prior application (37 CFR 1.63(d))
   (for continuation/divisional with Box 18 completed)
   i. [ ] DELETION OF INVENTOR(S)
   Signed statement attached deleting inventor(s) name in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).
6. [ ] **Application Data Sheet.** See 37 CFR 1.76
7. [ ] **CD-ROM or CD-R** in duplicate, large table or Computer Program *(Appendix)*
   [ ] Landscape Table on CD
8. **Nucleotide and/or Amino Acid Sequence Submission**
   (if applicable, items a. – c. are required)
   a. [ ] Computer Readable Form (CRF)
   b. Specification Sequence Listing on:
      i. [ ] CD-ROM or CD-R (2 copies); or
      ii. [ ] Paper
   c. [ ] Statements verifying identity of above copies

ADDRESS TO: **Commissioner for Patents**
P.O. Box 1450
Alexandria VA 22313-1450

ACCOMPANYING APPLICATION PARTS

9. [ ] **Assignment Papers** (cover sheet & document(s))
   Name of Assignee _____
10. [ ] **37 CFR 3.73(b) Statement** *(when there is an assignee)* [✓] **Power of Attorney**
11. [ ] **English Translation Document** *(if applicable)*
12. [✓] **Information Disclosure Statement** (PTO/SB/08 or PTO-1449)
    [ ] Copies of citations attached
13. [ ] **Preliminary Amendment**
14. [✓] **Return Receipt Postcard** (MPEP 503)
    (Should be specifically itemized)
15. [ ] **Certified Copy of Priority Document(s)**
    (if foreign priority is claimed)
16. [ ] **Nonpublication Request** under 35 U.S.C. 122(b)(2)(B)(i). Applicant must attach form PTO/SB/35 or equivalent.
17. [ ] Other: _____

113007 U.S.PTO
11/484100
071106

18. If a CONTINUING APPLICATION, *check appropriate box, and supply the requisite information below and in the first sentence of the specification following the title, or in an Application Data Sheet under 37 CFR 1.76:*

[ ] Continuation [✓] Divisional [ ] Continuation-in-part (CIP) of prior application No.: 10/925,161

Prior application information: *Examiner* Tolentino, Roderick *Art Unit:* 2134

19. CORRESPONDENCE ADDRESS

[ ] The address associated with Customer Number: [ ] ***OR*** [ ] Correspondence address below

Name	Apurva M. Bhansali				
Address	Softex, Inc. 9300 Jollyville Rd., Suite 201				
City	Austin	State	TX	Zip Code	78759
Country	U.S.A.	Telephone	(281) 207-5327	Fax	(281) 207-5327

Signature	Indranil Chowdhury	Date	July 11, 2006
Name (Print/Type)	Indranil Chowdhury	Registration No. (Attorney/Agent)	47,490

This collection of information is required by 37 CFR 1.53(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

071106 15866 U.S.PTO

PTO/SB/17 (01-06)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995 no persons are required to respond to a collection of information unless it displays a valid OMB control number

Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).

FEE TRANSMITTAL
For FY 2006

☑ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 1925

Complete if Known	
Application Number	TBA
Filing Date	July 11, 2006
First Named Inventor	Apurva M. Bhansali
Examiner Name	TBA
Art Unit	TBA
Attorney Docket No.	SOFP:115US

METHOD OF PAYMENT (check all that apply)

☐ Check ☑ Credit Card ☐ Money Order ☐ None ☐ Other (please identify): _____

☑ Deposit Account Deposit Account Number: 503361 Deposit Account Name: Indranil Chowdhury, P.C.

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☐ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, except for the filing fee

☑ Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17 ☑ Credit any overpayments

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION (All the fees below are due upon filing or may be subject to a surcharge.)

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

	FILING FEES		SEARCH FEES		EXAMINATION FEES		
		Small Entity		Small Entity		Small Entity	
Application Type	Fee ($)	Fee ($)	Fee ($)	Fee ($)	Fee ($)	Fee ($)	Fees Paid ($)
Utility	300	150	500	250	200	100	500
Design	200	100	100	50	130	65	
Plant	200	100	300	150	160	80	
Reissue	300	150	500	250	600	300	
Provisional	200	100	0	0	0	0	

2. EXCESS CLAIM FEES

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20 (including Reissues)	50	25
Each independent claim over 3 (including Reissues)	200	100
Multiple dependent claims	360	180

Total Claims		Extra Claims		Fee ($)		Fee Paid ($)
52	- 20 or HP =	32	x	25	=	800

HP = highest number of total claims paid for, if greater than 20.

Indep. Claims		Extra Claims		Fee ($)		Fee Paid ($)
8	- 3 or HP =	5	x	100	=	500

HP = highest number of independent claims paid for, if greater than 3.

Multiple Dependent Claims	
Fee ($)	Fee Paid ($)

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets		Extra Sheets		Number of each additional 50 or fraction thereof		Fee ($)		Fee Paid ($)
145	- 100 =	45	/ 50 =	1 (round up to a whole number)	x	125	=	125

4. OTHER FEE(S)

	Fees Paid ($)
Non-English Specification, $130 fee (no small entity discount)	
Other (e.g., late filing surcharge):	

SUBMITTED BY

Signature	Indranil Chowdhury	Registration No. (Attorney/Agent) 47,490	Telephone (281) 207-5327
Name (Print/Type)	Indranil Chowdhury		Date July 11, 2006

This collection of information is required by 37 CFR 1.136. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(c) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
11/484,100	07/11/2006	Apurva Mahendrakumar Bhansali	SOFP:115US

CONFIRMATION NO. 7749

Apurva M. Bhansali
Softex, Inc.
Suite 201
9300 Jollyville Rd.
Austin, TX78759

Title: Electronic device security and tracking system and method

Publication No. US-2006-0253904-A1
Publication Date: 11/09/2006

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 703-305-3028.

Pre-Grant Publication Division, 703-605-4283

PTO/SB/08a (05-07)
Approved for use through 09/30/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	11484100
Filing Date	2006-07-11
First Named Inventor	Bhansali
Art Unit	2134
Examiner Name	Zand, Kambiz
Attorney Docket Number	SOFP:115US

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	5680547		1997-10-21	Chang	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20030051090	A1	2003-03-13	Bonnett et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1	WO98/43151	WO	A1	1998-10-01	Cotichini et al.		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	11484100
	Filing Date	2006-07-11
	First Named Inventor	Bhansali
	Art Unit	2134
	Examiner Name	Zand, Kambiz
	Attorney Docket Number	SOFP:115US

	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	11484100
	Filing Date	2006-07-11
	First Named Inventor	Bhansali
	Art Unit	2134
	Examiner Name	Zand, Kambiz
	Attorney Docket Number	SOFP:115US

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Charles C. Claunch/	Date (YYYY-MM-DD)	2007-07-09
Name/Print	Charles C. Claunch	Registration Number	51,221

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	1954040
Application Number:	11484100
International Application Number:	
Confirmation Number:	7749
Title of Invention:	Electronic device security and tracking system and method
First Named Inventor/Applicant Name:	Apurva Mahendrakumar Bhansali
Correspondence Address:	Apurva M. Bhansali Softex, Inc. Suite 201 9300 Jollyville Rd. Austin TX 78759 US 2812075327 -
Filer:	Charles Christopher Claunch
Filer Authorized By:	
Attorney Docket Number:	SOFP:115US
Receipt Date:	09-JUL-2007
Filing Date:	11-JUL-2006
Time Stamp:	23:02:25
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes) /Message Digest	Multi Part /.zip	Pages (if appl.)
1	Miscellaneous Incoming Letter	SOFP115US_TransmittalLetter_IDS.pdf	18995 8197a35ce9b14cbb8aeff452a1d065ef94cb92e3	no	2
Warnings:					
Information:					
2	Foreign Reference	WO9843151.pdf	4162847 7c0fdce4fd728e8bebc893b489b3ac5bc368493b	no	114
Warnings:					
Information:					
3	Miscellaneous Incoming Letter	SOFP115US_TransmittalForm_IDS.pdf	49739 5bbd8a7afb4be34da6474ddc80e2c6e281966d60	no	1
Warnings:					
Information:					
4	Information Disclosure Statement (IDS) Filed	SOFP115US_IDS.pdf	787181 b4a6aa6c26de0a783186b6d266b179efebd569e2	no	4
Warnings:					
Information:					
		Total Files Size (in bytes):	5018762		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of:		Docket No.: SOFP:115US
	Apurva M. Bhansali et al.	Art Unit: 2134
Serial No:	11/484,100	Examiner: Zand, Kambiz
Filed:	July 11, 2006	Conf. No.: 7749
For:	Electronic Device Security and Tracking System and Method	

INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
Alexandria, Virginia 22313-1450

Dear Sir:

This Information Disclosure Statement is submitted in compliance with 37 C.F.R. §§ 1.56 and 1.97 through 1.98. This Information Disclosure Statement is being submitted before the mailing of a first Office action on the merits and therefore no fee is required.

Record is attached of published art for consideration during prosecution of the above-identified patent application. No representation is made or intended that a search has been made, or, if made, was complete, or that no more pertinent art that than listed is available. It is expected that the Patent and Trademark Office will conduct an independent search for relevant prior art.

Unless otherwise indicated, or unless references cited are U.S. patents or patent application publications, a full text copy of the entire reference of published art is attached. Where specifically indicated, an equivalent English language patent or publication is attached in lieu of the translation.

In accordance with the Patent and Trademark Office Notice of August 15, 1980, also enclosed is a completed form PTO/SB/08a (Form PTO-1449). The Commissioner is authorized to charge any fee that may be required by this Information Disclosure Statement to Deposit Account No. 503361 in the name of Indranil Chowdhury, P.C., referencing SOFP:115US.

Respectfully submitted,

/Charles C. Claunch/

Charles C. Claunch
Reg. No. 51,221
Indranil Chowdhury
Reg. No. 47,490
Attorneys for Applicants

Chowdhury & Georgakis, P.C.
Phone Num.: (281) 207-5327
E-mail: Ichowdhury@cgiplaw.com

DELL EXHIBIT 1002
Page 170 of 659

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 1/00

A1

(11) International Publication Number: **WO 98/43151**

(43) International Publication Date: 1 October 1998 (01.10.98)

(21) International Application Number: PCT/CA98/00278

(22) International Filing Date: 24 March 1998 (24.03.98)

(30) Priority Data:

08/826,098	24 March 1997 (24.03.97)	US
08/871,221	9 June 1997 (09.06.97)	US

(63) Related by Continuation (CON) or Continuation-in-Part (CIP) to Earlier Applications

US	08/826,098 (CIP)
Filed on	24 March 1997 (24.03.97)
US	08/871,221 (CIP)
Filed on	9 June 1997 (09.06.97)

(71) Applicant *(for all designated States except US)*: ABSOLUTE SOFTWARE CORPORATION [CA/CA]; 304 – 1212 West Broadway, Vancouver, British Columbia V6M 3V1 (CA).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: COTICHINI, Christian [CA/CA]; PH6 – 1188 Richards Street, Vancouver, British Columbia V6B 3E6 (CA). FRASER, Cain [CA/CA]; #208 – 1159 Main Street, Vancouver, British Columbia V6A 4B6 (CA). ASHWORTH, David, G. [CA/CA]; 3810 Regent Avenue, North Vancouver, British Columbia V7N 2C4 (CA). LIVINGSTON, Peter [CA/CA]; 19318 – 118 B Avenue, Pitt Meadows, British Columbia V3Y 2P7 (CA). SOLYMAR, Gabor [CA/CA]; 35 Whalings Circle, Stittsville, Ontario K2S 1S4 (CA).

(74) Agents: KNOX, John, W. et al.; Fetherstonhaugh & Co., Vancouver Centre, Suite 2200, 650 West Georgia Street, P.O. Box 11560, Vancouver, British Columbia V6B 4N8 (CA).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

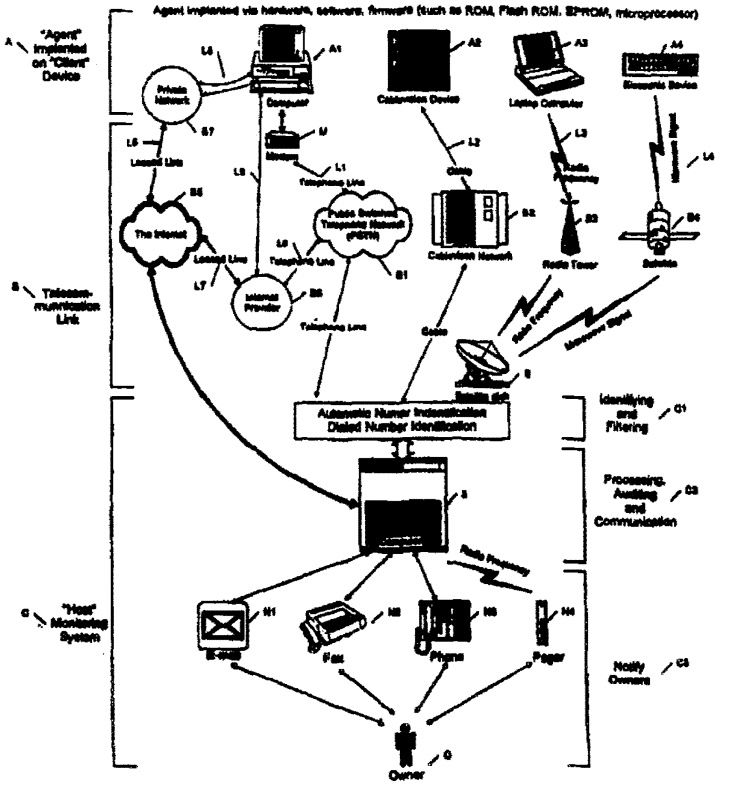
Published

With international search report.

(54) Title: METHOD AND APPARATUS TO MONITOR AND LOCATE AN ELECTRONIC DEVICE USING A SECURED INTELLIGENT AGENT VIA A GLOBAL NETWORK

(57) Abstract

A system for locating and monitoring electronic devices utilizing a security system that is secretly and transparently embedded within the software, firmware, or hardware of a computer. This security system initiates the client computer to periodically and conditionally call a host system to provide unique identifying indicia and location information. In one embodiment, the security system calls the host through a public switched telephone network (PSTN) and transmits the indicia in encoded form. In an alternative embodiment, which may be incorporated concurrently with the PSTN application, the security system calls the host system through the Internet and provides the host with indicia encoded within the DNS query sent. The host system is able to identify the calling computer from the indicia and is able to physically locate the computer through either caller identification or by referencing the Internet links which were used to connect the calling computer with the host system.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

METHOD AND APPARATUS TO MONITOR AND LOCATE AN ELECTRONIC DEVICE USING A SECURED INTELLIGENT AGENT VIA A GLOBAL NETWORK

RELATED APPLICATIONS

This application is a continuation-in-part application of co-pending U.S. application Serial No. 08/826,098 filed on March 24, 1997 which is a continuation-in-part application of copending application Serial No. 08/558,432 filed November 15, 1995 which is a continuation-in-part of Serial No. 08/339,978 filed November 15, 1994; continuation-in-part application of co-pending U.S. application Serial No. 08/871,221 filed on June 9, 1997 which is a continuation-in-part application of copending application Serial No. 08/558,432 filed November 15, 1995 which is a continuation-in-part of Serial No. 08/339,978 filed November 15, 1994.

BACKGROUND OF THE INVENTION

Many electronic devices, such as laptop computers and cellular telephones, are becoming more compact and portable. While such portability is extremely convenient for the user, it has given rise to an increased risk of theft. These electronic devices are often very expensive and are easily lost or stolen.

Previously, attempts have been made to provide means for retrieving lost or stolen items of various types. The simplest approach is marking the item with the name and the address of the owner, or some other identification such as a driver's license number. If the item falls into the hands of an honest

person, then the owner can be located. However, this approach may not deter a thief who can remove visible markings on the device.

Password protection schemes are of dubious value in discouraging theft or retrieving an item. Although the data can be protected from theft, the computer hardware cannot be found or retrieved. Another approach has been to place a radio transmitter on the item. This has been done in the context of automobile anti-theft devices. The police or a commercial organization monitors the applicable radio frequency to try to locate a stolen vehicle. This method is not suitable for smaller items such as cellular telephones or laptop computers. First, it is inconvenient to disassemble such devices in order to attempt to install a transmitter therein. Second, there may not be any convenient space available to affix such a transmitter. Furthermore, a rather elaborate monitoring service, including directional antennas or the like, is required to trace the source of radio transmissions.

It is therefore an object of the invention to provide an improved means for tracing or locating smaller lost or stolen objects, particularly laptop computers, cellular telephones, desktop computers and other small, portable electronic devices or expensive home and office electronic equipment. It is also an object of the invention to provide an improved means for tracing such electronic devices which can be installed without disassembly or physical alteration of the devices concerned.

It is a further object of the invention to provide an improved means for locating lost or stolen items, this means being hidden from unauthorized users in order to reduce the risk of such means being disabled by the unauthorized user.

DELL EXHIBIT 1002
Page 174 of 659

It is a still further object of the invention to provide an improved means for locating lost or stolen items which actively resist attempts to disable the means by an unauthorized user.

It is a still further object of the invention to provide an improved means for inexpensively and reliably locating lost or stolen items.

This invention also overcomes disadvantages associated with the prior art that may interfere with the operating system or running applications. This is accomplished by disposing the means for initiating communication with a host system in the firmware such as on the ROM BIOS or the modem component of a client electronic device. This security system operates independently of the operating system running on the electronic device.

In addition, a feature whereby the security system transmits through the Internet is disclosed. This feature enables the security system to initiate a call to the host monitoring system even when the client is simultaneously running a different Internet application. This represents an advantage over the prior art including co-pending Continuation-in-Part Application (Serial No. 08/558,432), which is hereby incorporated by reference, which could not transmit while an application was using the modem since interference could alert the user to the presence of the security system. This security system operates independently of the operating system running on the electronic device.

SUMMARY OF THE INVENTION

This invention relates to a security apparatus and method for retrieving lost or stolen electronic devices such as portable computers, PCs (including stolen components such as CPU, hard drives, etc.), cablevision devices, personal digital

assistants (PDAs), cellular telephones, etc. This invention enables electronic devices to be surveyed or monitored by implanting thereon an intelligent agent with a pre-defined task set. This agent communicates with a preselected host monitoring system which is capable of multiple services including; tracing location, providing identifying indicia such as an electronic serial number (ESN), and electronically notifying the end user/owner of its location. The agent hides within the software/firmware/hardware of the electronic device, and operates without interfering with the regular operation of the device. According to one embodiment of the invention, the Agent is disposed on the ROM BIOS of the electronic device and the Agent takes control of the electronic device and its facilities during its boot-up. According to another embodiment of the invention, the Agent is disposed on the modem component of the electronic device and the Agent operates independently of the electronic device. Another embodiment of the Agent is on the processing unit (e.g., microprocessor) of the electronic device. Yet another embodiment of the Agent is a hardware implementation, such as hard-wired circuitry or a single integrated circuit. The Agent is further designed to evade detection and resist attempts to disable it by an unauthorized user.

The invention overcomes disadvantages associated with the prior art by yielding a security device for small computers, cellular telephones and the like which can be programmed as firmware onto the non-volatile memory (such as ROM BIOS, ROM, Flash ROM, EPROM, EEPROM or the like) of such devices. Accordingly, no physical alteration is necessary or apparent to a thief. The existence of the security device is well cloaked and thus it cannot be readily located or disabled even if the possibility of its existence is suspected. Apparatuses and methods according to the invention can be very cost effective,

requiring relatively inexpensive modifications to software or hardware and operation of relatively few monitoring devices.

According to one aspect of the invention there is provided an electronic device with an integral security system. The security system includes means for sending signals to a remote station at spaced apart intervals of time. The signals include identifying indicia for the electronic device. The means for sending signals includes a telecommunications interface connectable to a telecommunications system, and means for dialing a preselected telecommunications number. In an alternative embodiment, signals are sent through a global network interface. This can be accomplished via the standard public telecommunications system which may be linked to a global network service provider, or through a private network (LAN) link to the global network. The remote station includes a telecommunications receiver having the preselected telecommunications number. The remote station and the electronic device may also simultaneously be connected through the global network.

In one embodiment of the invention the electronic device is a computer, and the means for sending signals includes means for providing signals to the telecommunication interface to dial a preselected telecommunication number and send the identifying indicia. The telecommunication interface may be a modem. The means for providing signals may include security software installed as a firmware onto the non-volatile memory (such as ROM BIOS, ROM, Flash ROM, EPROM, EEPROM, or the like) of the computer, a software program, a micro-code program, a digital signal processor ("DSP") program or a built-in function of the operating system.

The security system may be recorded on the boot sector of a hard disk, on a hidden system file such as IO.SYS, MSDOS.SYS,

IBMBIO.COM or IBMDOS.COM, or alternatively on the ROM BIOS of the computer, or a combination of both. The security system functions without interfering with the operating system or any running applications. The security system is loaded into memory whenever the electronic device is powered on or reset. It is loaded before the operating system. Alternatively, the security system may be recorded on the Flash ROM of the modem component of the electronic device. The security system functions independently of the main processor of the electronic device. Consequently, the security system as provided in either the ROM BIOS or the modem Flash ROM is operating system independent.

The Agent may be implemented in the firmware or software of any electronic device, such as a computer. Alternatively, the Agent may be implemented in any component of a computer, as with an electronic component such as the DSP in a modem or the CPU in the computer. Furthermore, the functionality of the Agent may be implemented in the circuitry of any hardware device capable of establishing a communication link through sending and receiving packets of data.

There is provided according to another aspect of the invention a method for tracing lost or stolen electronic devices whereby a telecommunications interface is connectable to a telecommunications system at a first telecommunications station. The method includes providing the electronic device with means for sending signals to the telecommunications interface. The means is instructed by the agent to send first signals to the telecommunications interface that then calls a remote telecommunications station. These first signals contain the encoded identification (serial number) of the sending computer. Upon detecting an incoming signal, the remote computer determines the identification of the sending computer by decoding its serial number, and can retrieve the caller phone

number from the Telephone Company. The remote computer compares the serial number with a predefined listing of serial numbers of reported lost or stolen computers. The call will only be answered if the sending computer is on the predefined list. In an alternative embodiment, this call filtering feature can be removed and the remote computer will answer all incoming calls.

In an alternative embodiment, if the remote computer answers the incoming call then the means for sending signals automatically sends second signals to the telecommunications interface. The telecommunications interface then transmits identifying indicia for the device as well as any other pertinent information to the remote telecommunications station.

There is provided according to another aspect of the invention a method for tracing lost or stolen electronic articles through a global network such as the Internet. The client computer sends DNS queries that contain encoded identification information to a remote station through the Internet. The remote station receives the queries and decodes the encoded identification information in order to determine if the client computer matches an entry on a list of reported lost or stolen computers. If so, the host sends a predefined response to the client computer indicating that it should initiate a traceroute to provide the host with the Internet communication links connecting the client computer to the host. Additionally, when the client computer receives this predefined response from the host it immediately attempts to contact the host via the telecommunications system.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other objects and advantages will become apparent by reference to the following detailed description and accompanying drawings, in which:

FIG. 1 is a functional block diagram of a preferred embodiment of the electronic article surveillance system in accordance with the teachings of this invention.

FIG. 2 is a simplified illustration of the functional block diagram of FIG. 1 for the purpose of showing an illustrative embodiment of the present invention.

FIG. 3 is an illustrative embodiment in the form of a flowchart of the process by which the operating system and agent are able to start up and run simultaneously.

FIG. 4A is an illustrative embodiment in the form of a flowchart showing the Agent's work cycle according to an embodiment of the invention.

FIG. 4B is an illustrative embodiment in the form of a flowchart showing the routine for determining PCMCIA support in the electronic device.

FIG. 4C is an illustrative embodiment in the form of a flowchart showing the modem call routine initiated by the Agent.

FIG. 5 is an illustrative embodiment in the form of a flowchart showing the Agent startup loading sequence.

FIGS. 6A, 6C and 6D are illustrations of alternatives to loading of the Agent.

FIG. 7A is a schematic block diagram illustrating the alternate embodiment of Segmented Agent. FIG. 7B is a flow chart of the Segmented Agent process.

FIGS. 8A-F are block diagrams illustrating the alternate embodiment of Modem Agent.

FIG. 9 is an illustrative embodiment in the form of a flowchart of a process by which the host identification and filtering subsystem identifies and filters out unwanted calls from agents.

FIG. 10A is a schematic showing an illustrative embodiment of the encoding/decoding method whereby the monitoring service would have to subscribe to 60 telephone numbers.

FIG. 10B is a schematic showing an illustrative embodiment of the encoding/decoding method whereby the monitoring service would have to subscribe to 300 telephone numbers.

FIG. 11A is an illustrative embodiment in the form of a flowchart of a process by which the host telephone monitoring subsystem exchanges data with an agent.

FIG. 11B is an illustrative embodiment in the form of a flowchart of a process by which the host Internet monitoring subsystem exchanges data with an agent.

FIG. 11C is an illustration of a manner in which the client identification is encoded within the host name according to one aspect of the invention.

FIG. 12 is an illustrative embodiment in the form of a flowchart of the process by which the host notification subsystem, contained within the host computer, notifies end-users of the status of monitored devices.

FIGS. 13A and B are schematic diagrams illustrating the embodiment in which the Agent resides in the CPU.

FIG. 14 is an illustrative embodiment in the form of a flowchart showing the conventional method of booting up a personal computer with alternative loading points for the agent security system shown in broken lines.

FIG. 14A is an illustrative embodiment in the form of a flowchart showing a method for startup loading of an agent security system according to an embodiment of the invention wherein the operating system boot sector is loaded with the agent.

FIG. 14B is an illustrative embodiment in the form of a flowchart wherein the hidden system file IO.SYS or IBMBIO.COM is modified to be loaded with the agent.

FIG. 14C is an illustrative embodiment in the form of a flowchart wherein the partition boot sector is modified to be loaded with the agent.

FIG. 14D is an illustrative embodiment in the form of a flowchart wherein the agent security system is ROM BIOS based.

FIG. 14F, 14G are portions of an illustrative embodiment in the form of a flowchart showing the agents' work cycle according to an embodiment of the invention.

FIG. 14F1 is a portion of an illustrative embodiment in the form of a flowchart showing the agents' work cycle for the Internet application.

FIG. 14H is an isometric view, partly diagrammatic, of the physical structure of a computer disc.

FIG. 15 is a schematic showing an illustrative embodiment of the encoding/decoding method whereby the monitoring service would have to subscribe to 60 telephone numbers.

FIG. 15A is a schematic showing an illustrative embodiment of the encoding/decoding method whereby the monitoring service would have to subscribe to 300 telephone numbers.

FIG. 16 is a drawing showing some elements which may be installed in conjunction with a PC.

FIG. 17A is a drawing showing ID number that are associated with elements which may be installed in conjunction with a PC.

FIG. 17B is a high level flow diagram showing steps used by an agent tracking associated element ID numbers.

FIG. 18A is a high level diagram showing the elements and steps of creating and storing a validation key the first time.

FIG. 18B is a high level diagram showing the elements and steps of creating and checking a validation key.

FIG. 19 is a high level diagram showing the elements and steps of creating and checking a validation key against stored databases.

FIG. 20 is a high level diagram showing computrace agent elements associated with a birth certificate file.

FIG. 21 is a high level diagram showing an event loop of a secure protocol component.

FIG. 22 is a high level diagram showing basic protocol of the secure protocol component.

FIG. 23 is a high level diagram of the steps used by the secure protocol component.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

System Overview

Referring to FIG. 1, the preferred embodiment of the electronic article surveillance system is comprised of three main components: (1) client device A consisting of any one of the electronic devices shown which have been implanted with the agent; (2) A telecommunication link B such as a switched communications system, the Internet, radio tower, satellite and cable networks; and (3) The host monitoring system C which controls the communications between the client device A and the host monitoring system C.

Referring to FIG. 1, the client device can be a cablevision device A2, laptop computer A3, or other type of electronic device A4 including a cellular telephone or personal digital assistant (PDA). However, for illustrative purposes, the client device consists of a client computer A1 attached to modem M. The host monitoring system C sends and receives data packets from the client computer A1 over a suitable bi-directional transmission medium, such as a common telephone line L1. Telephone line L1 couples the client computer A1 to the host monitoring system C and the host computer 3 through Public Switched Telephone Network B1 (Telephone Company). The host computer 3 notifies the appropriate parties C3 (owner O, law enforcement agency, or monitoring company) of the status of the client device A via suitable communication means such as electronic mail N1, fax N2, telephone N3 or pager N4. Host monitoring system C also identifies and can filter incoming calls C1, and provide processing, auditing and communication functions C2.

In another embodiment of the invention cablevision device A2 is connected to cablevision network B2 via cable L2. This

cable L2 further connects cablevision network B2 to the host monitoring system C.

In another embodiment of the invention laptop computer A3 is connected to radio tower B3 via radio frequency (RF) transmissions L3. These RF transmissions are received by satellite dish S at the host monitoring system C.

In another embodiment of the invention electronic device A4 is connected to satellite B4 via microwave signal L4. Microwave signal L4 further connects satellite B4 to satellite dish S at the host monitoring system C.

In yet another embodiment of the invention client computer A1 is connected to private network (such as a LAN) B7 which is connected to a global network such as the Internet B5 via leased line L5. The connection between client computer A1 and private network B7 can be provided through wireless connection L8. Leased lines L5 and L7 can, according to one embodiment of the invention, transmit data to and from client computer A1 digitally. Host computer 3 is also connected to the Internet B5. In an alternative embodiment of this global network or Internet application, client computer A1 can alternatively, or simultaneously, be coupled to the Internet B5 through modem M which connects client computer A1 to telephone line L1. Telephone line L1 connects to Public Switch Telephone Network (PSTN) B1 which provides access to Internet provider B6 (such as AOL, Netcom, etc.) via telephone line L6. Internet provider B6 provides access to Internet B5 via leased line L7. Alternatively, client computer A1 may be linked directly to Internet provider B6 via wireless communication link L9. Although this aspect of the invention is described in the context of the Internet, it will be understood by one of ordinary skill in the art that the application of this invention to any currently existing of future global network is

contemplated herein. Further, although the Internet aspect of this invention is described and illustrated with respect to client computer A1 it should be understood that the Internet application is readily applicable to the other described devices (including laptop computers, cablevision networks, cellular telephones, personal digital assistants, and other electronic devices).

Referring to FIG. 2, the host monitoring system C has two monitoring subsystems: telephone monitoring subsystem 9x and Internet monitoring subsystem 9y. Telephone monitoring subsystem 9x monitors information transmitted via telephone line 1 from client computer 10 which has an agent installed thereon. Internet monitoring subsystem 9y monitors information transmitted via the Internet 9j from client computers 10 which have agents installed thereon.

Telephone monitoring subsystem 9x includes voice board 2, host computer 3a, hard disk controller 4, hard disk 5, CRT 6, keyboard 7, and printer 8. Host computer 3a is coupled to a suitable display device, such as CRT 6, keyboard 7, and printer 8. The keyboard 7 permits the operator to interact with the host monitoring system C. For example, the operator may use keyboard 7 to enter commands to print out a log file of the clients that have called into the system. The host computer 3a illustratively takes the form of an IBM personal computer. The source codes for the host monitoring system C, in Visual C++ by Microsoft, are disclosed in copending Application Serial Nos. 08/826,098 and 08/558,432 and are incorporated herein by reference.

Telephone line 1 is connected to the host computer 3a by a voice board 2 which is adapted to receive and recognize the audible tones of both caller ID and dialed numbers transmitted via the telephone line 1. Client computer 10 is connected to

modem 9 via serial ports 9b. Host computer 3a is connected to voice board 2 via data bus 2a. The modem 9 and voice board 2 are connected to telephone line 1 which is routed through Public Switched Telephone Network (PSTN) 9c in accordance with a conventional telephone system. Client computer 10 and modem 9 form a first telecommunication station, while computer 3 and voice board 2 form a second, or remote telecommunications system. The host monitoring system C sends and receives data packets from client computer 10.

Ring signals are received on phone line 1 as an input to voice board 2. In an illustrative embodiment of the invention, voice board 2 may take the form of the DID/120, DTI/211, and D/12X voice boards manufactured by Dialogic Corporation. The voice board 2 is operative to recognize the ring signal. Then it receives the caller ID and dialed numbers and converts them into corresponding digital signals. As explained in greater detail below, in one embodiment of the invention, the dialed numbers provide in encoded form the unique serial number of the client computer. Host computer 3a decodes the encoded serial number for comparison against a list of reported lost and stolen computers stored in hard disk 5.

In an illustrative embodiment of the invention, the hard disk controller 4 may comprise memory control boards manufactured by Seagate Tech under the designation Hard Disk Controller. The hard disk controller 4 is particularly suitable to control the illustrative embodiment of the hard disk memory 5 manufactured by Seagate Tech under their designation ST-251.

Similarly, the Internet monitoring subsystem 9y is comprised of a host computer 3b, hard disk controller 9e, hard disk 9f, CRT 9g, keyboard 9h, and printer 9i. The host computer 3b is coupled to a suitable display device such as CRT monitor 9g, keyboard 9h, or printer 9i.

Leased line 9k connects host computer 3b to the Internet 9j. Client computer 10 is connected to modem 9 via serial port 9b. Modem 9 and host computer 3b may be connected to the Internet 9j by an Internet provider 9o which uses a communication link such as Serial Line Interface Protocol (SLIP), or Point to Point Protocol (PPP). Alternatively, or simultaneously, client computer 10 may be connected to the Internet 9j through private network (LAN) 9p having gateway to the Internet or the equivalent. In alternative embodiment, client computer 10 may be linked to Internet provider 9o and private network 9p via wireless links L9 and L8 respectively. For illustrative purposes, the communication link is a SLIP link. The Internet monitoring subsystem 9y sends and receives data packets from client computer 10 over the Internet 9j.

Domain Name Service (DNS) queries from the agent that are transmitted through the Internet 9j are received as input to the host computer 3b. Host computer 3b extracts the host name from the DNS query, and then extracts and decodes the agent identification (serial number) from this host name. Host Internet monitoring computer 3b uses the decoded agent identification for comparison against a list of reported lost and stolen computers stored in hard disk 9f. The Internet and DNS queries are discussed in more detail below.

According to one embodiment of the invention, the unique identification associated with each electronic device can be an Electronic Serial Number (ESN). These ESN codes can comprise a string of alphanumeric characters that can be encrypted and encoded. The ESN can be generated randomly by a central delegating body to assure that each electronic device has an ESN that is unique. The ESN can be permanently associated with an agent security system to enable the unique identification of the electronic device in which the agent is installed.

The agent is a software program such as a terminated stay resident program, VXD (Virtual Device driver program), application program (such as Windows service or Windows NT service), or a file filter program. The Agent is installed on hardware, software, or firmware. Some alternative methods of installation are described in co-pending U.S. Application Serial No. 08/558,432 which is hereby incorporated by reference. Once the Agent is installed it will report its identity and its location to the host after specified periods of time have elapsed, and upon the occurrence of certain predeterminedconditions. This is further illustrated in co-pending U.S. Application Serial No. 08/558,432.

Referring now to Fig. 2, once the Agent is installed and running it will periodically (every four hours) report its identity and location on the Internet 9j to the Internet monitoring subsystem 9y. The Agent can also concurrently report its identity and location to the telephone monitoring subsystem 9x through PSTN 9c after specified periods have elapsed, and uponthe occurrence of certain pre-determined conditions.

Internet and DNS Queries

The Internet is a collection of networks linked together by IP routers and high-speed digital links. Computers which have access to one of these networks can run Internet applications to send and retrieve digitally recorded files such as audio and video files. Some of the popular Internet applications are Netscape (used to surf the web), Eudora (for e-mail), Telnet (for logging on to another computer, ping (Internet utility for checking the status of a particular machine). These Internet applications can be run simultaneously. Thus, a computer can be running client programs such as Eudora and Netscape and at the

same time operate as an FTP Server (File Transfer) for other clients that want to transfer files. The applications share the same communications links to the Internet and computer resources (CPU and memory). Thus, multiple applications can simultaneously run without interfering with each other. There is, however, a resultant diminishing effect on performance. The agent of the instant invention would have virtually no effect on the performance of other applications since it transmits such a small data packet.

Each computer linked to the Internet has a unique Internet host name/IP address. Computer networks comprising one or more of these computers are also given names to form a hierarchical naming structure. For instance, the web site for IBM is "www.ibm.com." The prefix "www" is the name of the computer (server) which is attached to the ibm.com network. Addresses could be coded using numbers, but this would make administration of the Internet extremely difficult. Instead, a method providing for the mapping of Internet host names to network addresses was implemented. This mapping system is the Domain Name System (DNS). It is a distributed, hierarchical administrative system. At the top of the hierarchy is the root domain containing the top-level domains (com, edu, net, ca, us, etc.). At the bottom end is a domain name such as cs.berkeley.edu. which corresponds to the computer science department of the University of California at Berkeley. Each domain has more than one authoritative server that can map its Internet host name to its IP (numerical) address.

If a user wants to access the site at www.psmith.cs.berkeley.edu from the address pliving.absolute.com, the user would first input www.psmith.cs.berkeley.edu. into his web browser. The web browser would then send a DNS query to the absolute.com

authoritative server to determine if the desired address had been recently resolved (DNS resolutions are cached to enhance the performance of the DNS system). If the absolute.com DNS server cannot resolve this address, then the next DNS server up the chain is checked (the DNS server at the "com" level). If that higher level server also cannot resolve the address, then the root server directs the process down the chain to the top-level "edu" DNS server. If the "edu" DNS server cannot resolve the address, then the DNS server at berkeley.edu is contacted. Ultimately, a DNS server is found that can determine the appropriate IP address based on the Internet host name. The IP address is provided to the web browser to enable communication with www.psmith.cs.berkeley.edu.

Once the desired IP address has been determined, packets of data can be sent across the Internet through IP routers. These IP routers can read the numerical addresses and determine where to send each packet. Each IP router has a unique IP address. Typically, several IP routers need to be contacted to link a user with his desired Internet site. As explained in more detail below, the traceroute routine provides a listing of all IP routers used to enable communication between a client and host.

Functions of the Agent

The Agent may be implemented in the firmware or software of any electronic device, such as a computer. Alternatively, the Agent may be implemented in any component of a computer, as with an electronic component such as the DSP in a modem or the CPU in the computer. Furthermore, the functionality of the Agent may be implemented in the circuitry of any hardware device capable

of establishing a communication link through sending and/or receiving packets of data.

One of the important functions of the agent is to contact the host monitoring system C to report the identity, location, and other information relating to its associated client computer 10. The agent has to determine the appropriate time for it to call the host monitoring system C. The agent can contact the host monitoring system C through the PSTN 9c connecting to the telephone monitoring subsystem 9x, or through the Internet 9j which connects the Internet monitoring subsystem 9y. Thus, the agent can communicate with a host monitoring system C using either the Internet or the PSTN techniques. Alternatively, the agent may rely concurrently on both techniques.

FIG. 3 is a flow chart of the agent work cycle. This work cycle describes the method by which the Agent is loaded when the client computer 10 is initially turned on or reset, and the manner in which the operating system and the agent run concurrently. In this illustrative embodiment, the Agent is embedded in software. Once the client computer 10 is powered on 11, it performs a power on self-test (POST) 12. The POST tests the system hardware, initializes some of the devices for operation, and loads the master boot record (MBR) 13. Since the MBR was installed with an Agent subloader, the subloader is loaded into memory 14 and executed. The subloader's first task is to load the Agent into memory 15 (which is discussed in detail below in reference to FIG. 5.) Then the subloader loads the operating system (OS) into memory 16 and returns control to the operating system. Now both the operating system 17 and the Agent 18 are running simultaneously.

a. PSTN

In the PSTN application, once the Agent is running 18, it will determine the appropriate time to call the host 19. The time period in which the Agent is waiting for the appropriate time to call the host is the "active" period. The Agent will only call the host when a pre-defined time period has elapsed, or when a pre-determined event has occurred which triggers the client to contact the host. Every one-eighteenth of second the Agent compares the current date and time with the date and time that the Agent is due to call the host. If the Agent determines that it is time to call the host it will transfer to "alert" mode.

In alert mode the Agent will attempt to call the host eighteen times per second until it is successful. Once in alert mode, the Agent does a thorough search within the computer to find free (not currently being used by any running application) communication equipment 20. In an illustrative embodiment, the communication equipment comprises a modem 9. It is contemplated herein that different communication mechanisms (i.e., modem, satellite link, RF link, etc.) can be provided at several of the communication ports. In such a scenario, the Agent would poll the communication ports (corresponding to the different communication mechanisms) to find free communication equipment. If the Agent fails to find any free equipment, then the Agent will abort its attempt to call the host and repeat the cycle 18 within one-eighteenth of a second. However if the Agent locates free communication equipment, it will call the host 21. Upon receiving a call from the client computer 10, the host examines the Agent identity, which according to the preferred embodiment is the serial number of the client computer, and determines if a connection should be established 22. The host establishes a connection when the serial number of the computer contacting the host matches an entry on a list of reported lost or stolen computers. In an alternative embodiment, this call-filtering

feature is eliminated and the host system establishes a connection whenever there is an incoming call. The list of reported lost or stolen computers is maintained within the host monitoring system C. If the host does not accept the call then the Agent will not call back until the next appropriate time (after predetermined time period has elapsed) 18. If the host accepts the call, then the Agent will send the host its encoded identity (such as its ESN), location (caller ID), any relevant serial numbers of computer components, such as CPU, hard drive, BIOS and any other desktop management interface (DMI) and any other pertinent information such as local date and time 23. The Agent then checks if the host has any data or commands for the client 24. If the host has no data or commands to be sent, then the Agent will terminate the call and repeat the cycle 18. Otherwise, the host will send the data or commands 25 before it terminates the call, and returns to "active" mode 18. This work cycle is described in much greater detail below with reference to FIGS. 14F, 14F1 and 14G.

In the Internet application, which can run alone or concurrently with the PSTN application, the Agent initiates a call to the host at relatively short predetermined intervals. According to the preferred embodiment, in its "active" mode the Agent calls the host every four hours 18a. The Agent uses the current time and the unique Agent identification to encode an Internet host name 18b. The Agent then forms a DNS request using the encoded Internet host name 18c. The Agent sends this DNS request to the host through the Internet 18d. If the agent's attempt to send the DNS request to the Internet times out 18h after a predetermined time period has elapsed, the Agent will sleep for one minute and then repeat the cycle from step 18b. If the call fails due to another error (such as the

absence of Winsock facilities which enable communication with the Internet, and/or the failure of the computer to be configured for TCP/IP communication) 18e then the Agent will repeat the cycle four hours later 18a. In this way, the Agent inherently checks for the existence of an Internet connection.

After sending its DNS request, the Agent waits for a response. Upon receiving a valid response from the host 18e, the IP address is extracted from the response and compared against a reference IP address 18f. In this illustrative embodiment of the invention the reference IP address is "204.174.10.1". If the IP address equals "204.174.10.1" then the agent's mode is changed from "active" to "alert" on the Internet side 18g. The host will send this reference IP address only when it has determined that the Agent identification matches one of the entries on a list of reported lost or stolen computers stored at the host. If the IP address extracted from the host response does not equal "204.174.10.1" then the Agent remains in active mode and does not call the host for another four hours.

As will be explained in more detail below, when the Agent goes into "alert" mode in the Internet application, the Agent initiates a traceroute routine which provides the host with the Internet communication links that were used to connect the client computer to the host. These Internet communication links will assist the host system in tracking the client computer. The IP address of the source of the DNS query is sent to the host within the DNS query. However, if the source of the query is transmitted through a "proxy" server, then the IP address of the client computer (which may not be unique since it may not have been assigned by the InterNIC) will likely be insufficient to track the location of the client computer. In such a scenario, it is necessary to determine the addresses of other IP

routers that were accessed to enable communication between the client and the host. These addresses and the times that they were accessed are compared with internal logs of the proxy server that record its clients' Internet access history. In this way, the client can be uniquely identified and located. Additionally, the transfer of the Internet application into "alert" mode is a condition that triggers the transfer of the PSTN application to "alert" mode.

The system remains transparent to an unauthorized user via implementation of well-known deflection methods. Attempts to read or write to the location where the Agent has been installed are deflected in order to prevent discovery of the agent. When read attempts are made to the Agent location the system generates meaningless bytes of data to be returned to the user. When write attempts are made to the location where the Agent is installed, the client computer accepts the input data and informs the user that the write has been successful. However, the data is not really stored, and thus the Agent is preserved. The Agent, in order to remain hidden to the user, will not interfere with any running applications unless designed to interfere.

Detailed Operation of Agent Work Cycle

Referring to FIG. 5, the Agent startup and loading sequence is described. The computer 10 is powered on and the loading sequence begins 700. As is well known in the art, the machine's start-up ROM procedure 701 in the computer 10 begins when the power is turned on. This process supervises the booting up and loading of the operating system of the computer. It performs the power-on self-test (POST) 702, in fact POST is carried out on every reset of the system, including the time when the power

is first turned on. This test has two purposes: it performs a quick test 703 of the basic elements of the system; and it initializes the major hardware components for use. POST tests all of the ROMs on the system board by performing a checksum. This test adds together all of the bytes in the ROM module. As is does the addition, it discards any carry from the 8-bit result. If the final result is zero, the ROM passes the test. The initialization is done immediately after POST, it checks for new equipment and extensions to ROM 704. If it finds any 706, it momentarily turns control over to the ROM extensions so that they can initialize themselves. By design, the ROM Agent is a ROM extension, therefore its initialization routine will receive control 707 from the computer during the machine's start-up ROM procedure.

Once activated the Agent takes control of the whole computer 708. If it determines that it should call the Host computer, it follows the processes described in reference to FIG. 4A, 4B and 4C. Basically, it finds a free communication port, establishes a communication link to the Host, sends its identity then relinquishes control back to the machine's start-up ROM procedure. After POST ended 713, the machine's start-up ROM procedure loads the operating system from disk 714, and passes control to it 715.

Referring to FIG.4A, a flow chart is provided which describes one embodiment of the Agent work cycle in accordance with this invention. The Agent looks for communications ports to be used. There are two types of communications ports: the old by popular communications ports are called COM; and the new PCMCIA ports calledPCMCIA. Since COM is the more popular than PCMCIA, the Agent first looks for COM communications ports 322-338, if no COM communications ports are found then it will look

for PCMCIA ports 338-350. To look for COM communications ports, the Agent checks all COM port addresses using COM port address table 333 to see if they exist 335. The first one encountered will be dynamically hooked 336 into by swapping the appropriate interrupt handler and unmasking the appropriate interrupt request line. If an error occurs, the next port will be checked 338,334 until either a valid COM port is found or the COM port address table has been exhausted 338. If the COM communication port responds properly, then attempt to check if a modem is currently connected to this COM communications port via issue of the Hayes compatible AT command 339. if the modem does not exist, then the next port will be checked 338. If the modem exists it will respond with an "OK" to the AT command 341.

If no COM ports are found or if no modems are connected to COM communications ports and if BIOS supports PCMCIA modem 340, the Agent attempts to locate PCMCIA communications ports 340-350. The Agent searches for PCMCIA communications ports and PCMCIA modems in steps 342-350 in a fashion similar to the way it searches for COM communications ports 322-338. If no PCMCIA support is enabled 340 or no PCMCIA ports are found, the Agent will stop 358.

After a functional communications port and a modem are found regardless of their type the Agent will attempt to initialize the modem by sending it modem initialization strings 351-353 using strings from a table of initialization strings. If the modem does not respond with an "OK" 355, this indicates that the initialization attempt failed 356. If the initialization attempt failed, then the next set of strings in the table will be tried 354, and so on until a valid set of initialization strings is found, or the modem initialization string table is exhausted 356 at which point, the Agent will stop 358.

DELL EXHIBIT 1002
Page 198 of 659

During the system boot process, when the Agent stops at 358, it relinquishes control back to the machine's start-up ROM procedure (see step 715 in FIG. 5).

FIG. 4B describes in detail how the Agent detects whether PCMCIA support is enabled. It does this by checking to see if the computer is using a PCI BIOS 387, and the Cirrus PD6729 PCI Controller chip 389. If these features and chip set are detected, the Agent checks for port conflict 390 and wake up the Cirrus PCI Controller 391. The Agent makes an I365_IDENT call to PCMCIA Controller to identify the chip further 392. Such I365_IDENT call is also made to the PCMCIA Controller even if the PCI BIOS and Cirrus PCI Controller are not present. The PCMCIA Controller chip is then initialized 393, if the chip is initialized successfully then PCMCIA support is enabled 395, otherwise PCMCIA support is not enabled 388. Once a valid and available communications port has been found, and it has been verified that a functional modem is associated with that port, the system will attempt to dial out to the remote host 357 (see also 370 in FIG. 4C).

Referring to FIG. 4C, the Modem Call routine 370 is illustrated. A dial string table 372 is used 371 to attempt the call since a PBX or switchboard etc. may need to be exited via a dialing prefix. If successful 373-374, the CONNECT result code (numeric or letters) from the modem will be received by the client 374. The Agent also decrements the offset in the dial string table so that the next time the machine is powered on or reset, the current dial string will be used. The host will send a signal ("Query") to the client requesting its serial number. If the client does not receive the "Query" signal 379 it will abort 384, reset the communication port and modem 385, and repeat the cycle 334, 343. If the client receives the "Query" signal, then the serial number is sent 380. At this point,

telecommunications have been established and the agent-host transaction begins. If the transaction succeeds, the resultant state will be "active", otherwise it will be "alert". If a "NO DIALTONE" or "BUSY" event occurs 375-376, the offset in the Dial String Table will be incremented 378 so that the next dial string will be attempted the next time the machine is powered on or reset.

The Agent to remote host transaction involves the sending of the computer serial number 380 via the telephone company or carrier service. The "Caller ID" is implicitly received by the remote host (typically during the initial telecommunications event "RING"). Upon the occurrence of the event "CONNECT", the host sends the client a vendor specified message called "QUERY" 379 which in effect tells the client to send its serial number 380. This involves the host acknowledging that it has received 381 and processed 383 the serial number thereby validating it. The client will attempt this call a pre-defined number of times 382 before it gives up (disconnects, cleanups, unhooks port 384, resets communication port and modem 385, repeats the cycle 300). At this point, the modem disconnects 384, and any other cleanup necessary occurs (such as changing the date of the last call to the present). Finally, the resultant state will be reset to "active" and the Agent will remove all traces of it in memory to avoid being detected by unauthorized users. The Agent then stops 386. During system start-up, when the Agent stops, the machine's start-up ROM procedure continues to scan for the next ROM extension (see step 712 in FIG. 5.)

If the computer that called in was not reported stolen, no further action with regard to the computer system that called in will be taken. If, however, the serial number transmitted to the remote Host matches one of the serial numbers on a currently valid list of stolen computers, further processing will occur to

facilitate the recovery of the missing equipment. Such processing includes, but is not limited to, placing either an automatic or manual call to the local authorities in the vicinity of the missing equipment or the owner of such equipment.

Instead of making a modem call via the PSTN, the BIOS Agent may be configured to communicate with the host monitoring server via the internet in a similar fashion as explained in reference to FIG. 3.

Referring to FIG. 3G, a dial string table 140 is used 139 to attempt the call since a PBX or switchboard may need to be exited using a dialing prefix. The dial string is sent 141, and if successful, the CONNECT result code (numeric or letters) from the remote host server will be received by the client 143. The host will send a signal ("Query") to the client requesting its serial number. If the client does not receive the query signal 148 it will abort 149 and repeat the cycle 117. If the client receives the "Query" signal, then the serial number is sent to the host 151. At this point, telecommunications have been established and the client-server transaction begins. If the transaction succeeds, the resultant state will be "active", otherwise the state of the PSTN application will still be in "alert" mode. If, for some reason, a "NO DIALTONE" event happens 144, a delay will occur 147 and the next dial string 141 will be attempted again. If the line is "BUSY" 145, then a redial attempt 146 will occur using the same dial string for a predefined number of attempts or until a telecommunications connection is made, whichever occurs first. If there is no connection made pursuant to the sending of the dial string and if no dial tone or busy signal is received, then the call attempt is aborted 142.

The client to remote host server transaction involves the sending of the computer serial number 151 via the telephone company or carrier service. The "Caller ID" is implicitly received by the remote server (typically during the initial telecommunications event known as "RING"). Upon the telecommunications event called "CONNECT", the remote host server sends the agent security system client a vendor specific message called "QUERY" 148 which in effect tells the client to send the serial number. This step is particularly significant in an alternative embodiment of the invention wherein the serial number is not sent via the dialed numbers. The step of sending this serial number 151 requires the server to acknowledge that it has received 152 and processed 154 the serial number (validating it). If the appropriate acknowledgment is not received, the client computer will attempt to send its serial number a predefined number of times 153 before it gives up (whereby it disconnects, cleans up, unhooks port 127, 155 and returns to "alert" mode 156). Once the server has acknowledged that it has received and processed the serial number and any other information sent by the client, the modem disconnects 160. Any other cleanup necessary (such as changing the date of the last call to the present) will also be done here 160. Finally, the resultant state will be reset to active 161.

If the serial number of the computer that called in does not match with any of the reported lost or stolen computers, no further action will be taken. If, however, the serial number transmitted to the remote host server matches one of the serial numbers on a current list of lost or stolen computers, further processing will occur to facilitate the recovery of the missing equipment. Such processing includes, but is not limited to, automatically or manually placing a call to the local authorities in the vicinity of the missing equipment, or the owner of such equipment.

Instead of making a modem call via the PSTN, the BIOS Agent may be configured to communicate with the host-monitoring server via the Internet in a similar fashion as explained in reference to FIG. 2.

Operation of Agent Work Cycle Using a Global Network

Referring now to Fig. 14F1, a flow chart is provided which describes in detail the background process operations relating to the Internet application. The background process wakes up every four hours 200. It uses the current date and time together with the agent identification (serial number) to encode an Internet host name 205. This encoded host name is used in forming a DNS query 206 to be sent to the host Internet monitoring subsystem 9y. After sending this DNS query to the host Internet monitoring subsystem 9y through the Internet 207, the agent waits for a response 208. If an error is found 208a due to a missing DLL or poor TCP/IP configuration, or an error other than a timeout, then the agent will wait four hours and repeat the cycle 200. If no response is received after a predetermined time period has elapsed, the agent will sleep for one minute 209 and then send another DNS query 205. Upon receiving a valid response from the host Internet monitoring subsystem 9y, the Internet Protocol (IP) address is extracted 210. If this IP address equals "204.174.10.1" 211 then the background process sets the agent's mode to alert 212. If the IP address does not equal "204.174.10.1" 211, then the agent remains in active mode and does not attempt to send another DNS query to the host for four hours 200.

Once the agent is in alert mode it initiates a traceroute 213 to provide the host with the Internet communication links which connect the client computer to the host. The transfer of

the Internet application to alert mode also triggers the transfer of the PSTN application to alert mode. Once the PSTN is in alert mode, the agent attempts to call the host telephone monitoring subsystem 9x to report its status (identification, location, and other information) through the PSTN eighteen times per second until it is successful.

The following is a discussion of how the traceroute routine operates within the Internet to provide the Internet links which connect the client computer to the host. The Internet is a collection of local area networks joined by IP routers. These IP routers read the numerical destination address of the IP packet sent by each computer linked to the Internet and decrease the Time to Live (TTL) field (used to age a packet) of the packet before sending it to the next appropriate router. However, if the TTL field is zero, the router will return the packet to the source computer with a fail error code.

A traceroute is performed by doing multiple pings from the computer 10 to the host Internet monitoring subsystem 9y. The TTL field is incremented from one for each ping. The first ping is sent with a TTL value of one. It will fail at the first router and the first router address will be determined since the IP packet which will indicate the address of the first router will be returned to the source (client) computer. The second ping will then be sent with a TTL value of two. If this call fails then the second router address will be determined. This process is continued until the ping succeeds. By saving each router address, a trail of routers linking the client computer with host Internet monitoring subsystem 9y is created. This route, representing the sequence of Internet communication links between the computer and the host, is then transmitted to the host Internet monitoring subsystem 9y which saves this information on disk.

The client computer then performs an arp to resolve the mac address which is transmitted to the server. This information can be used to help track the computer as a mac address is a unique number stored in Ethernet LAN cards. It is possible for an ip address to change, but the mac address is constant for the life of the Ethernet LAN card.

First, the "owner" of the source IP address (corresponding to a certain router (LAN) used) will be determined. This is accomplished by presenting the linking information (complete linking information between the client computer and the host is provided pursuant to the traceroute) to the appropriate Internet governing body, such as InterNIC, which is responsible for delegating IP addresses. According to the preferred embodiment, this query can be performed by sending a telnet command to the InterNIC including the address that needs to be queried.

Once the owner of an IP address is determined by querying the InterNIC, the retrieval process can continue. The owner, which may be an independent service provider (such as AOL, Netcom, etc.), is contacted and the date/stamps saved by the Internet monitoring subsystem 9y are compared with the ISP's server logs which are used for billing. These logs generally contain extensive details relating to the owner, time, and date that a particular IP address was used. These logs may be stored in TACACS or RADIUS databases that are created from Cisco or Livingston terminals respectively. Thus, the location from which the client computer called the host through the Internet may be determined.

If the DNS query fails, or the returned address is 204.174.10.1, or the traceroute fails the client attempts to establish a web session with the absolute web server. It first tries to establish the session directly, then it tries any available web proxy server.

If it cannot establish a web session, it tries to establish an ftp session. The client first tries to establish the ftp session directly, then it tries any available ftp proxy server.

Once a web session or ftp session has been successfully established, the sessions are used as secure, encrypted transport sessions. These sessions allow the secure transmission of dos commands and data files.

The dos commands are executed on the client with the results returned and displayed on the server. This facility would allow an authorized user to search for files on the client, upload those files from the client to the server, and irreversibly erase the files from the client computer.

Referring to FIGS. 14F and 14G, the following is a detailed description of the agent work cycle with respect to the PSTN application. Once the system is powered on 117 a timer interrupt will occur 18.2 times per second. Every eighteen timer interrupts, the complementary metal-oxide semiconductor (CMOS) real-time clock will be accessed, and the time and date will be stored for comparison with the previous real-time clock access. If the date and/or time changes towards the future, no action will be taken to track the time displacement. In this way the agent determines whether it is time to call the host 118. Thus if the current date has advanced far enough into the future (past the date and time to call the host), the agent security system will change its mode of operation from active to alert whereby calls will be regularly attempted (eighteen times per second) until a call is made and a transaction with the host server has been completed. If the system time has been backdated, a modal change from active to alert will occur. This feature safeguards against a thief disabling the agent by backdating the client so that the agent does not call the host for a long period of time.

The communications ports are checked 119-125 (via a port address table 120) to see if they exist. If the first one encountered is not in use 123, it will be dynamically hooked 126 into by swapping the appropriate interrupt handler and unmasking the appropriate interrupt request line. If an error occurs, or if a port is in use, the next port will be checked 124 until either a valid port is found or the port address table has been exhausted 125. If the port address table is exhausted then the agent waits X seconds before trying to find an unused port again. Appropriate cleanup routines restore "swapped" ports to their initial settings.

If the communications port responds properly and a port is actually hooked into 126, the system will attempt to connect to a modem via issue of the Hayes compatible AT command 128. If the modem does not exist, that port is unhooked 127, and the next port is checked 124. If the modem does exist and if it responds with an "OK" 129 to the AT command, the system will attempt to initialize the modem by sending it a modem initialization string 130, 132 (from a table of initialization strings 131). If the modem does not respond with an "OK" 134, this indicates that the initialization attempt failed and the next string in the table is tried 136. This process continues until a valid initialization string is found 134, or the modem initialization string table is exhausted 136 (at which point, the routine will delay for some seconds then try again from the start by checking for the next available port 121).

Once a valid and available communications port has been found, and it has been verified that a functional modem is associated with that port, the system will attempt to dial out to the remote host server 137, 138.

Installing and Loading the Agent

The agent is installed during a typical boot up sequence to the operating system of a computer. FIG. 14 shows a boot-up process for a typical personal computer. It should be understood that this invention is applicable to other types of computers and electronic devices presently available or as marketed in the future with suitable modifications. The aspect of the invention described below is the process of installing the security software onto a portable computer. The method of installation is crucial because the software must remain undetectable once installed. Furthermore, the software should be as difficult as possible to erase. In summary, the invention achieves these objects by installing the software in such a manner that it remains hidden to the operating system, such as MS-DOS.

Four alternative ways of installing the agent security system during the disk boot are illustrated in FIG. 14A-14D respectively. A conventional boot up method is described in detail in Appendix I. The system can also be installed with MS.SYS or IBMDOS.COM, but these are more difficult and less preferred than the three alternatives set out below. The loading program TENDER (further described in the Appendix) can be used to install the agent by one or more of these alternative installation methods. Thus, the agent may be installed in a variety of locations whereby second and third agents can provide back up support for the primary agent. The four locations where the agent can be installed on the client device are as follows:

1. The operating system boot sector- See FIG. 14A.

2. A hidden system file such as IO.SYS for MS-DOS or IBMBIO.COM for PC-DOS- See FIG. 14B.

3. The partition boot sector- See FIG. 14C.

4. The ROM BIOS- See FIG. 14D

Referring to FIG. 14A, the agent loading sequence is described for loading the agent on the operating system boot sector. The computer 10 is powered on and the loading sequence begins 64. As is well known in the art, the computer 10 performs an initial testing routine to assure that all components are working properly 65. Illustratively, the program incorporated is the IBM-PC compatible Power-On Self Test (POST) routine. The partition boot sector is loaded 66. Next the operating system boot sector with the installed agent is loaded 67. In an effort to maintain the transparency of the agent, the CPU registers (corresponding to the current state of the computer) are saved 68. Before the agent is installed there is a check for a Remote Procedure Load (RPL) signature 69. If the signature is present this indicates that the agent is already in memory and will not be loaded again. However, if there is no RPL signature then preparation is made to load the agent. First, space is reserved for the agent at the ceiling of conventional memory 70. Next, Interprocess Communication Interrupt (2Fh) is hooked 71, which enables communication with other programs. Interrupt Eah, which is the disc input/output handler, is hooked 72. The old timer interrupt is saved, and new hook timer interrupt is put into place 73. Now the CPU registers are restored 74 in order to maintain the transparency of the system. The original operating system boot sector is loaded 75. The original operating system had been moved to accommodate the agent installation. Finally, the operating system is loaded 76 and running 77 again.

Referring now to Fig. 14B, the agent loading sequence is described 78-91 for loading the agent on a hidden system file such as IO.SYS for MS-DOS or IBMBIO.COM for PC-DOS. The sequence is analogous to that disclosed above for the operating system boot sector. However, instead of loading the agent with the operating system boot sector, the agent is loaded with the operating system file 82 (load modified IO.SYS or IBMBIO.COM).

Referring to FIG. 14C, the agent loading sequence is described 92-104 for loading the agent on the partition boot sector. The sequence is analogous to that disclosed above for the operating system boot sector. However, instead of loading the agent with the operating system boot sector, the agent is loaded with the operating system partition boot sector 94.

Referring to FIG. 6A, the Agent is implanted in the boot sector of the computer's hard-disk 721. The Agent is loaded into memory when the computer is turned on or reset 722. Once active, the Agent executes in memory 723 until the computer is powered down or reset.

Referring to FIG. 14D, the agent loading sequence 105-116 is described for loading the agent via ROM BIOS. The sequence is analogous to that disclosed above for the operating boot sector. However, the Agent is loaded from the ROM after the CPU registers are saved 107. At that time the ROM can take control of the system and load the agent. Once the CPU registers are restored 113, the ROM can no longer load the agent.

As is well known in the art, the computer 10 is performs an initial testing routine to assure that all components are working properly 65. Illustratively, the program incorporated is the IBM-PC compatible Power-On Self Test ("POST") routine. Next, in an effort to maintain the transparency of the Agent, the CPU registers (corresponding to the current state of the

computer) are saved 107. Before the Agent is installed there is a check for a Remote Procedure Load ("RPL") signature 108. If the signature is present, this indicates that the Agent is already in memory and will not be loaded again. However, if there is no RPL signature, then preparation is made to load the Agent. First, space is reserved for the Agent at the ceiling of conventional memory 109. Next, Interprocess Communication Interrupt (2Fh)is hooked 110 which enables communication with other programs. Interrupt 13h, which is the disc input/output handler, is hooked 111. The old timer interrupt is saved, and new hook timer interrupt is put into place 112. Now the CPU registers are restored 113 in order to maintain the transparency of the system. The original operating system boot sector is loaded 114. The original operating system had been moved to accommodate the agent installation. Finally, the operating system is loaded 115 and running again 116.

Another configuration the BIOS Agent is shown in FIG. 6C. the Agent is implanted into the computer's BIOS 731 and/or bootstrap BIOS. When the computer is turned on or reset, the Agent loads itself into memory and checks for an image of itself on the computer's hard-disk 732. If an image of the Agent is found, that image is refreshed 733 and run from the disk 734. If an image is not found, one is created on the disk 735. The newly created image is then loaded into memory and run from the disk 734.

Turning to the operating system independent methods, referring to FIG. 6E, the Agent is implanted into the computer's BIOS 741 and runs directly from the BIOS 742. As more fully discussed below, variations of the BIOS Agent may include implanting the Agent in a DSP of a modem, a CPU of the electronic device, a hard wired circuitry or an integrated circuit in the electronic device.

All of the above BIOS Agents may be configured to communicate with the host monitoring server via modem call and/or internet.

Variations on Loading the BIOS Agent

Four alternative ways of installing the Agent security system during the disk boot were disclosed in co-pending U.S. Application Serial No. 08/558,432 which is hereby incorporated by reference. In one of the alternative methods of installation the Agent was disposed on the ROM BIOS using hook interrupts and saving and restoring CPU registers. That method required these brute force techniques to enable the Agent to be compatible with certain operating systems. Operating system independent Agents are further disclosed herein.

Segmented Agent

Referring to FIG. 7A, an alternate embodiment of the operating system independent BIOS Agent is described in which the Agent 751 is segmented into two components. The Secure Protocol Component (SPC) is implanted into the computer's BIOS 752. The SPC handles device tracking function only 753. Additional functions, such as asset and configuration management, are handled by a High Level Component (HLC) that resides on the computer's hard-disk 754 and run from the disk 755.

Referring to FIG. 7B, the embodiment of FIG. 7B is described in greater detail. The SPC 757, upon recognizing machine events and at specified intervals, checks to see whether the Operating System is installed and active on the hard-disk 758. Events that can be recognized include Power Management events and Plug-and-Play queries such as the ACPI (Advanced

Configuration & Power Interface) adopted by Microsoft and other developers or SMI (System Management Interface) adopted by Intel and others. Power Management events are generated from the hard-disk powering down, the CPU switching speeds, or the display switching on or off. Plug-and-Play queries are received from the Operating System when it is identifying devices installed in the machine and loading drivers to control those devices. If the SPC is able to communicate with the Operating System, it determines if it is time to contact the Server 760. It does this by checking a "counter" which is reset to a certain value during bootup and then decremented with each check that is performed. Any time the counter reaches 0 (zero), the SPC contacts the Server 761. If the SPC is unable to establish a communication link with the Operating System, it assumes that a problem exists with the system and forces the counter to 0 (zero) 759. The SPC then immediately establishes a link to the Server 761 by any of the means discussed before regardless of the amount of time that has elapsed since the last connection.

Once a communication link has been established between the SPC and the Server 762, the Server asks the SPC to identify itself 763. The SPC responds with the ID of the device that is being tracked 764. The Server then sends a request to the SPC 765 asking that it perform one or more tasks at a specified future time (such as contacting the Server again). At the appropriate time, the SPC responds to any such request 766. All communications between the Agent and the Server will incorporate data encryption 767 to provide an additional layer of security and prevent the sophisticated and user from intercepting or transmitting messages in an attempt to interfere with device tracking. The Server will determine the location of the tracked device with whatever means are available through the particular communication service being utilized. For instance, if a link were established over standard phone lines, Caller ID/ANI could

be used to fix the location, or if a link were establish over Internet, the ID address can be used to fix the location.

The capabilities of the software installed on the hard disk would be based upon the needs of the customer and might include advanced asset management or system administration functions. The hard disk-based components of the Agent would perform in a method similar to that of the SPC, contacting the Server at specified intervals and transmitting data back and forth as necessary to complete its scheduled tasks 769.

Alternatively, the SPC may be implemented in the CPU of the computer 10, the DSP of the modem, or in the form integrated circuits or hard wired circuits, as more fully addressed below.

The segmented Agent may be configured to communicate with the host monitoring server via modem call and/or internet.

Modem Agent

Referring to FIG. 8A, according to another embodiment of the invention, instead of installing the ROM BIOS of the computer, the Agent is installed into the Flash ROM (or EPROM) 811 or DSP 812 of the computer modem, either on a plug-in card or built-in on the motherboard (810) of the computer. The Agent can be imbedded into the modem Flash ROM (or EPROM 811) or DSP 812 by an installation utility that runs on the computer, or it can be embedded into the modem Flash ROM or DSP by the manufacturer. The Modem Agent can communicate with the Host Monitoring System through the PSTN 813 at scheduled times without the involvement of the PC processor. Thus, the Modem Agent is independent of the software running on the computer including the operating system.

The Modem Agent enables a monitored computer to communicate to the monitoring server even if a new disk drive is installed. This provides a much more secure method of tracing the location of stolen computers where modifications are made to the computers before they are used. In the case where computers are stripped for parts, the Modem Agent will still be able to be located. Integration of the Modem Agent onto the motherboard of the computer will not allow the Modem Agent to become separated from the motherboard, protecting the most important component of the computer.

A. Modem Hardware Architecture

The hardware architecture consists of a programmable modem either in a plug-in card 820 or a module 830 integrated onto the motherboard 831 of the monitored computer as shown in FIG. 8B and FIG. 8C respectively. Plug-in card based modems 820 are usually programmable but can be removed from the monitored computer. This prevents the modems from tracking the main portion of the computer. Modem modules 830 integrated directly onto the motherboard can not be removed from the main portion of the computer. The modem module 830 is coupled to the CPU 832 and RAM 833.

The modem module 830 or plug-in card 820 will contain a modem chip set 824, 834 that provides the modem communication (encoding and modulation) and modem controller functions. Depending on the manufacture the chip set, it may contain a single or multiple DSPs and possibly a microcontroller. The DSP will usually provide the communication software for encoding and modulation. The microcontroller will usually provide the modem controller software but some chips set provide two DSPs for both functions. Along with the chip set the modem will contain RAM

825, 835, a flash programmable EPROM 826, 836, A/D and D/A converters 827, 837 as well as a POTS interface 828, 838.

The RAM is used by the modem chip set as its main memory. The flash programmable EPROM is used to store the modem software. A/D and D/A converters with the POTS interface allow the chip set to send/receive signals over the analog PSTN phone lines.

While the Modem Agent is described below in connection with communications with the host monitoring server via modem call, the Modem Agent may be configured with the additional and/or alternate function of communicating with the host monitoring server via internet.

B. Modem Agent Software Architecture

The Modem Agent resides on either a software upgradable ISA of PCI modem card or a memory mapped/ISA mapped modem module integrated on the mother board. These modems usually consist of two software entities, the controller software 841 and the communications software 842 as shown in FIG. 8D. The controller software 841 contains the software that controls the interface between the PC 845 and the communications software 842 as well as the POTS interface 844. It allows application software to communicate with and control the actions and parameters of the communication software 842.

The communication software 842 contains the modem communication functionality that provides the encoding and modulation schemes employed during communications. The communication software usually runs on a DSP while the controller software usually runs on a separate microcontroller. However, some modems use a single processor to provide both

functions. The communications software is usually not modifiable and is proprietary to the manufacture of the modem chip set.

A third software entity, the Modem Agent 843, must be added to the modem software. The Modem Agent will reside on the processor that contains the Modem controller or the Flash EPROM or ROM. The Modem Agent will receive extended AT commands from the Agent Configuration Utility 846. These extended AT commands will be proprietary to the host monitoring service and will each require a password. The Modem Agent will also be able to communicate with the host monitoring server directly. This capability will be provided by the call management function within the Modem Agent. (See FIG. 8E and discussions below.)

The Modem Agent 843 will run in parallel to the modem controller 841 such that no modifications to the manufacturer's software in the modem controller will be required. The modem controller will respond to the extended AT commands with "ERROR". However, the Modem Agent will qualify the error response with an extension response to indicate that the command was recognized and executed correctly if the syntax of the command and the password are correct. This will allow the standard modem controller code to function as is and still allow the Modem Agent to respond to commands.

Referring to FIG.8E, the Modem Agent 843 consists of three main program components: the command interface module 801, the command function module 802, and the call management function module 803. The command interface module 801 will handle all communications with the PC interface, in parallel with the modem controller. This will allow the command module to communicate with PC applications. Its functions will include receiving/transmitting of controller characters from/to the PC as well as AT command identification. The command interface

module 801 supports extended AT modem commands that enable control and configuration of the Modem Agent. Theextended AT modem commands include but are not limited to: set ESN, set dial strings, enable monitoring, disable monitoring, report status, initiate monitoring call, and set local time. All of the extended commands are password protected to prevent unauthorized access and detection of the Modem Agent.

The commands function module 802 implements the functionality of the extended AT commands as well as functions required to communicate to the monitoring server. This could include call initialization, call scheduling, ESN identification, status monitoring, mode management, etc.

The call management function module 803 will provide the interface to the monitoring server. It will allow the command module to communicate with the monitoring server. Its functions will include receiving/transmitting of data from/to the monitoring server and controlling the modem communication inferface. The call management function module 803 contains the Secure Protocol Component (SPC) of the Segment Agent as described before.

C. Modem Agent Functions

The Modem Agent provides two sets of functions. Firstly, to communicate with the PC's CPU, a set of extended AT commands are required. Secondly, to communicate with the host monitoring server, a set of functions are required.

1. Extended AT Commands

The Modem Agent supports extended AT commands to:

a. set ESN

This command allows a configuration application to modify the ESN number that the Modem Agent uses when connecting to the host monitoring server. This command is used to configure new Modem Agents as well as change the ESN when a new number has been assigned to it.

b. set dial strings

This command allows a configuration application to modify the number dialed when contacting the host monitoring server. This command is used to configure new Modem Agents with the correct dial-up phone number for the host monitoring server as well as modify it if a change is required.

c. enable monitoring

This command allows a configuration application to enable the monitoring service of the Modem Agent. This command is used to re-enable monitoring if the service has previously been disabled.

d. disable monitoring

This command allows a configuration application to disable the monitoring service of the Modem Agent. This command is used when the owner of the monitored PC wishes to terminate the electronic device trace service. The command will turn off the

Modem Agent functions and AT commands with the exception of the enable monitoring command.

e. report status

This command allows a configuration application to report the status of the Modem Agent.

f. force contact with Monitoring Server

This command allows an application to force the Modem Agent to contact the host monitoring server. This command can be used, for example, to test the Modem Agent configuration.

g. set local time

This command allows a configuration application to set the current time on the Modem Agent. This is to allow the Modem Agent to synchronize scheduled calling times to local time.

h. set Alert Mode interval

This command allows the interval of the alert mode (as described before) to be set.

All commands are password protected. The Modem Agent is shipped with a default configuration. The password accompanying each command will be calculated from the argument of the command. This will make the AT commands more difficult to

defeat and will not allow the application communicating with the Modem Agent to become out of sync with its password. The calling application must take care to not send AT commands while the modem is being used by another application.

2. Modem to Server Functions

For the Modem Agent to communicate with the host monitoring server, a set of functions are required to:

a. contact and communicate with monitoring server

When monitoring is enabled, the Modem Agent calls the host monitoring server's phone. The Modem Agent sends its ESN to the host monitoring server. The host monitoring server tells the Modem Agent when to call again. The Modem Agent calls back at the scheduled time. A state diagram of the contact and communication mechanism is shown in Figure 8F.

b. schedule communications with monitoring server

The Modem Agent is not able to schedule contact times on its own because it does not have access to a real-time clock. However, the Modem Agent is capable of measuring the passage of time. Thus, there is a need to initialize the current date and time in the Modem Agent upon power-up of the modem. This function can be provided by the HLC in a segmented Agent configuration described before, for example. If the modem Agent does not receive from the HLC the current date and time within a predetermined interval after power-up, then the Modem Agent will enter alert mode and initiate contact with the host monitoring

Server. When the Modem Agent contacts the host monitoring server, it will verify the time last set by the Agent Configuration Utility.

c. prevent modem contention

The Modem Agent does not interfere with the use of the modem by PC applications. Before calling the host monitoring server, the Modem Agent ensures that the modem is not currently in use. If a PC application starts to use the modem, as indicated by the receipt of AT commands by the modem, then the Modem Agent immediately drops any active call and immediately relinquishes control of the modem to the PC.

d. active alert mode

The Modem Agent will enter alert mode when it has not received communications with the Agent Configuration Utility of configuration application within X minutes. The Modem Agent will then immediately attempt to contact the monitoring server and will continue to contact it every Y minutes until communications from the Agent Configuration Utility are received (set absolute time AT command). This mode is to prevent thieves from removing the hard disk or reformatting the hard disk to defeat the Agent tracing service.

CPU Agent

The Agent may be implemented in a CPU using an existing technology in many current microprocessors which allows patching of the microcode. The microcode is the architectural layer of

the CPU which translates an external macrocode algorithm stored in volatile or non-volatile memory into a microprocessor's internal execution codes. Referring to FIG. 13A. the microcode patch 90 is formatted and encrypted according to each specific chip manufacturer's specifications. It is uploaded from the BIOS 91 to a microcode patch area 93 and/or microcode storage 94 in the CPU 92, after reset, during the POST initialization of the computer. The microcode patch 90 can implement all the functions of the conventional algorithmic Agent. Referring also to FIG. 13B, the Agent may take a similar form as the BIOS Agent or the SPC of Segmented Agent described before. The SPC in the microcode patch initiates communication with the modem 95 asynchronously of the normal code stream (i.e., of the operating system or application program 96) via the logic unit and decoder 97 of the CPU 92.

Examples of microprocessors which allows for microcode patching are the Pentium Pro and Pentium II processors developed by Intel Corporation. Of course it is also possible to implement the Agent in microcode or in logic circuitry inside the CPU during the manufacturing process in addition to the patching facility or exclusive of the patching facility of the CPU.

The CPU Agent may be configured to communicate with the host monitoring server via modem call and/or internet.

Hardware Agent

The Agent may be implemented in hard wired circuitry or a single integrated circuit using existing technology which takes an engineer's logic specification and translates into the data which is used to program, build, or design the hardware device or circuit. The hardware device or circuit would then execute

according to the engineer's logic specification and perform the functions of the Agent by establishing a communications link and sending and receiving data packets in order to establish both the identification and location of the electronic device within which the hardware device or circuit is included, thereby simulating the algorithmic function of the Agent.

Host Identification and Filtering System

The Host Identification and Filtering System identifies and filters out unwanted calls from agents. FIG. 9is a flow diagram of the host identification and filtering program executed by host computer 3. Once the security program is executed 26, the voice board waits 27 for the ring signal on the telephone line 1. When a ring signal is detected 28, the voice board 2 acknowledges the incoming call by sending a signal to the telephone company 9B via telephone line 1 requesting that the caller ID and the dialed numbers be sent to it. The voice board then waits until these numbers are received 29, 30.

Once the caller ID and the dialed numbers have been received, they are saved to the hard disk 31, 32. The security program then compares the dialed numbers 33, which provide an encoded version of the serial number of the client computer 10 (coding scheme explained in detail below), against a list of serial numbers stored on the hard disk 4. If no match is found, the program lets the phone ring until the client computer 10 hangs up the telephone line 34. In the preferred embodiment, the client computer is programmed to hang up after 30 seconds of unanswered ringing. However, if a match is found, the security program routes the call to an appropriate receiving line connected to a modem 35, which answers the call. In an alternative embodiment, the host 3 answer all calls and the

DELL EXHIBIT 1002
Page 224 of 659

serial number of the client computer 10 is provided in a separate subsequent call from the client computer 10.

Encoding of the client computer serial number

Referring to FIG. 10A in one embodiment of the invention, the serial number of client computer 10 is encoded within the dialed numbers it sends to the host 3. In the preferred encoding methodology, the client computer transmits its six digit serial number 170 to the host via a series of six complete dialed phone numbers 172. The first eight dialed digits after the first "1" are meaningless. The ninth dialed digit "N" 175, indicates which digit position within the serial number that the tenth dialed number corresponds to. The tenth dialed digit "D" provides the Nth digit of the serial number. The host computer 3 receives the six complete dialed phone numbers 172 and decodes them 173 by looking at only the ninth and tenth dialed digits. The client computer serial number 174 is thus reproduced.

For example, in the sequence "800-996-5511", the only relevant digits are the "11" portion. The first "1" indicates that the digit immediate to its right (1) is the first digit in the serial number. Similarly, in the sequence "800-996-5526", the "2" indicates that the number immediate to its right (6) is the second number in the serial number. The client computer, in total, dials six numbers 172 in order to convey its six-digit serial number to the host.

In order to accommodate this method of serial number coding, the host monitoring system needs to subscribe to sixty different phone numbers. All sixty numbers should have the same first eight digits, and only vary from one another with respect to the last two digits. The ninth digit need only vary from "1"

through "6" corresponding to the six digits within a serial code. However, the last digit must vary from "0" to "9".

Referring to FIG. 10B, the encoding methodology can alternatively be modified such that the client computer need only call the host three times to convey its serial number 180. According to this coding method, two digits of the serial number 186 would be transmitted in each call. Thus, the eighth dialed digit 185 would vary from "1" to "3", corresponding to the three packets of two digits 186 that make up the serial number 180. The ninth and tenth dialed digits 186 would vary from "0" through "9". However, this would require the operator of the monitoring system to subscribe to three hundred different phone numbers.

Host Processing, Auditing and Communication Subsystem

The host processing, auditing and communication subsystem receives and transmits information to and from clients. FIG. 11A is a flow diagram of the host communication program executed by host computer 3. After the host computer 3 is powered on 36, communication equipment is instructed to wait 37 for the telecommunication begin signal from the client computer 10. The telecommunication equipment acknowledges the begin signal by initiating a session to communicate with the client computer 38 and preparing the host to receive data packets from the client 39. The program first establishes that the client computer is sending data packets and that it has received all of the packets 40, 41. Next, the program determines if the client has any data or commands to be sent to the host 42. If not, the session is terminated 43, and the cycle is repeated 37. When all data packets have been received, the program permits the host to send data packets to the client computer. The program prepares to

send data packets 44, and then establishes that there are more data packets to be sent 45 before sending each packet 46. Once all data packets have been sent, the program terminates the session 43, hangs up the phone, and prepares to repeat the entire cycle 37. Host-side source codes are disclosed in the copending patent application serial nos. 08/826,098 and 08/558,432 which had been incorporated by reference here.

Referring to FIG. 11B, the host processing, auditing and communication subsystem for the Internet application receives and transmits information to and from clients over the Internet. FIG. 11B is a flow diagram of the host communication program executed by host computer 3 in connection with the Internet application. After the host computer is powered on 36a, TCP/IP support is loaded and the computer waits for a DNS query from the client computer 36b. The host name is then extracted from the DNS query 36c. Next, the DNS request is decoded to determine the client computer identification 36d. A check is made to determine whether the computer has been stolen 36e. This is accomplished by comparing the identification number of the client computer with a list of reported lost or stolen computers which is stored by the host computer. If it has been stolen a suitable message 36f is returned to the client computer 10. In the preferred embodiment, the message is provided by setting the IP address of the next transmission to the client computer to "204.174.10.1" 36f. If the client computer is not stolen, an alternate message is returned 36g. In the preferred embodiment this is achieved by setting the IP address to "207.174.10.16" 36g. The host uses either of these two IP addresses to form a response to the DNS query received from the client computer 36h. The host then sends its response to the client computer 36i. The host also records the transaction on the hard disk. The host then prepares to repeat the entire cycle 36b.

Referring to FIG. 11C, the manner in which client identification is encoded is illustrated. FIG. 11C shows the various components of a host name which is used to form a DNS request. The host name, according to one embodiment of the invention, is a string of characters including the date and time 37, encoded client identification 38, and domain name 39. The encoded client identification 38 is extracted from the host name for decoding at the host Internet subsystem 9y.

Host Notification Subsystem

The host notification subsystem notifies the end-users regarding the status of their electronic devices. In FIG. 1, various methods of notification such as; electronic mail N1, fax N2, paging N4, and telephone call N3, are depicted. FIG. 12 is a flow diagram of the host notification program executed by host computer 3. The host notification program determines whether there are any pending notification instructions or commands 48. If there are pending notifications, the information is retrieved 49. The program then determines the preferred preselected notification method 50, and formulates the message to be dispatched 51 according to the preselected notification method. This message is dispatched to the end-user 52. After dispatching the message, the program repeats the entire cycle 47. Host-side source codes are disclosed in the copending patent application serial nos. 08/826,098 and 08/558,432 which had been incorporated by reference herein.

Variations and Alternatives

The above description relates to the agent security system installed and operating in a conventional PC with an Intel 80X86

microprocessor or equivalent and with a conventional MS-DOS or PC-DOS operating system. It will be recognized that the system can be modified to fit other types of computers including, for example, those sold under the trademark Macintosh. The system can easily be modified to suit other types of operating systems or computers as they develop.

The above system is also intended to be added to existing computers without physical alteration. Another approach is to modify the ROM of such computers to contain the agent security system as shown in FIG. 14D. The agent security system also may be incorporated into the ROM of portable computers, cellular telephones or other such items when they are manufactured. FIG. 14D above describes the loading of the system from such a modified ROM.

One embodiment of the invention uses a modem connected or built-in to a computer. In the future it is likely that telephone systems will be digitized, thus obviating the need for a modem. The scope of this invention contemplates such digitized systems.

The system could also be included in the ROM of a cellular telephone. In this case, the program would hide the outgoing calls from the user by silencing audio signals and maintaining a normal screen display. It is also conceivable that portable computers can be supplied with integral cellular telephones modified in this manner or with some other telecommunication device.

The main telecommunication criteria for this agent security system is that the outgoing transmission (wire, radio signal or otherwise) be received by a switching mechanism, and contain information that causes the switching mechanism to forward the

information received to a remote station. Presently, this information is a telephone number and/or a DNS query. But other indicia of the remote station may be substituted in alternative switchable communications systems without departing from the scope of this invention.

Covering Peripherals and Software

Referring now to Fig 16, modern electronic devices, such as personal computer 400, are associated with a large number of valuable assets in the form of internal components such as processor 402 and option card 404, attached peripherals such as printer 406, keyboard 408, mouse 410 and modem 412, and installed software programs such as installed program 414.

The security function of the agent discussed above may be extended to encompass identifying, listing, reporting, locating and recovering these associated assets. This method and apparatus could also be used to reliably track and manage the type of assets being deployed in an organization's work force. This method can immediately report the variance should any unauthorized component change take place.

This security apparatus and method utilizes a hidden, tamper-proof agent 416 installed on an electronic device such as computer 400 for initiating communications and locating electronic devices as previously disclosed herein. The agent is also capable of determining the identifying indicia, such as a unique serial number, of a component or peripheral.

Referring now to Fig. 17A, each computer, peripheral and component such as computer 400, CPU 402, option card 404, printer 406, keyboard 408, mouse 410 modem 412, and software program 414, and agent 416 or other associated peripheral or

component are assigned an identifying indicia, such as unique serial numbers 401, 403, 405, 407, 409, 411, 413, 415 and 417 respectively. The serial number of each component comes from the manufacturer or is embedded at the time of assembly or installation of the component, peripheral or software.

Referring now to Fig. 17B, at step 420, agent 416 within an electronic device such as computer 400 periodically gathers the serial numbers 401, 403, 405, 407, 409, 411, 413, 415 and 417 of computer 400 and each of the components and software 402, 404, 406, 408, 410, 412, 414 and 416 respectively. On a regular basis, or in the event of a variance between a stored string of previously recorded serial numbers, at step 422 agent 416 transmits its electronic serial number 417 plus the string of discovered serial numbers as serial string 424 to the server . The server stores serial string 424 or a validation key 428 derived from serial string 424 in a database.

The component validation key is comprised of the agent's ESN and all the serial numbers of the associated components. One method is to string the ESN and serial numbers end-to-end. This method is illustrated in Fig. 17B.

After formulating validation key 428, agent 416 sends validation key 428 to server 430. The identity and the location of agent 416 is recorded, as previously disclosed, and validation key 428 is archived on storage device 432. All further communications with agent 416 cause server 430 to check subsequently transmitted validation key 429 for variances against the original archived validation key 428. Server 430 may also check validation key 428 against records of stolen components or software. Any discrepancies may be queued for appropriate action.

When new components and software are added to an existing configuration, validation key 428 will change to reflect the configuration modifications. Each modification so detected, will cause a variance in validation key 428. These variances will be checked against stored information 434 at server 430 and validated. The validation process will include checks against records 435-439 of stolen components and software, such as record 439 of duplicated identification numbers (as commonly occurs in component and software piracy), and records 440 authenticating proper final assembly by manufacturers. This validation process in illustrated in Fig. 19.

Manufacturers experience losses of components and software before final assembly of the electronic unit. Since this method and apparatus identifies and locates individual components and software, the information collected may be used to initiate recovery of specific components and software as well as the complete unit. If the electronic device, such as a PC, is misappropriated before final assembly, some of the components may not yet have been imprinted with a unique number. The absence of this number may also be an indicator of an invalid or illegal configuration.

The Agent can also be used to regularly upload the system, software & hardware configuration information of the Personal Computer. The agent is capable of reading a hidden file termed the "PC's Birth Certificate".

Birth Certificate" Repository & Reader

PC "Birth Certificate" 450 refers to a small data file 451 which contains certain static and dynamic information pertaining to a specific PC such as PC 456 or portable 458 (serial number, asset

tag number, invoice information, etc.). The creation, content, and format of the Birth Certificate 450 is configurable.

The agent may provide a method for encrypting and storing Birth Certificate 450 in a protected area 460 of PC hard-disk 462.

The agent retrieves the Birth Certificate using a Reader program which serves as a secure key. Only personnel in possession of a "master" Reader 452, or customers who have licensed a "private" Reader 454 will be able to access Birth Certificate information. The Reader may reside on a floppy disk such as disk 452 or 454.

Remote Computer Monitoring Software

Agent 464 silently calls into monitoring center 472 on a periodic (programmable) basis. Call and other PC asset management activity is logged, and reported to customers on-demand via the web-based Online Monitoring Service 468. The online monitoring service database 470 may include the following:

· Call-in phone number (retrieval option includes: name and address),

· Birth Certificate information such as file 451,

· Dynamic System information files such as file 476 (NetCensus, Asset Insight, etc.)

· Customer-created information files such as file 474

The above data will be collected, aggregated per customer, and sent to a 3rd party data center on a regular basis. Stand-alone systems such as system 476 may be installed within the data center, or on-site at customer locations.

CompuTrace is designed as a system to track the physical location of computers. The CompuTrace Agent such as agent A of Fig.1 is installed on a remote computer A1 to be monitored and through the use of (i) the public switched telephone network B1, (ii) the Internet B5, and (iii) local area networks B7, the CompuTrace server 3 maintains a database of records on computer A1's location and movements.

Tracking information is collected during periodic telephone calls to the CompuTrace server 3; wherein server 3 identifies the unique agent A and obtains the phone number from which that call has been made.

Once installed, the operation of the remote CompuTrace software is invisible to the user, and calls are made without the user's explicit awareness.

Overview of the CompuTrace BIOS Agent.

The core function of the CompuTrace Agent such as agent A, is to initiate independent transactions with a monitoring server 3 at regular intervals. This function has been adapted to work under an SMM environment. This subset of agent functionality is described as the Secure Protocol Component 752 (SPC) shown in Fig. 7A.

SMM is triggered by a System Management Interrupt (SMI) event. These SMI events are triggered by hardware and are serviced in

DELL EXHIBIT 1002
Page 234 of 659

Operating System (OS) independent memory space. This feature of SMM enhances the security of the SPC by effectively hiding the SPC from applications executing under the control of the OS.

The technical challenge is to successfully establish a link with the monitoring server and reliably send and receive packets of data from the SMM environment, which (because it executes outside of OS control) is restricted in both the frequency and latency of SMI events.

The Server Interface

In order to understand the role of the SPC, it is necessary to describe its interface with the monitoring server. The subset of transactions described below are the minimum required to perform the security function of a CompuTrace Agent.

A CompuTrace SPC transaction consists of the following steps:

· Step 652, The SPC initiates communication link 654 to the CompuTrace Server,

· The SPC and Server connect,

· The SPC reports the remote computer's time/date and the CompuTrace ID number,

· The Server logs this data and determines the status of the remote computer,

· The Server sends a series of commands to the SPC,

· The Telephone call is terminated.

Server to SPC commands supported by the SPC are as follows:

· Set next call date

Notifies the SPC of the date and time at which to perform the next call-out. This function is executed as a standard part of every call-out transaction.

· Set callout phone number

Notifies the SPC of a new phone number to which it should direct its call-outs. The SPC will direct all subsequent call-outs to this phone number until otherwise instructed.

· Disable CompuTrace

The SPC is disabled and will not call out within the natural lifetime of the unit. May be implemented as a sub-function of "Set next call date."

The Event Loop of the SPC:

The SPC is constructed as a timed event-driven state machine. A simplified diagram of event loop 602 is illustrated in Fig. 21.

At the top center of the diagram, Trigger 600 is shown to drive the timing of events to the state machine of the SPC. Trigger 600 is activated at regular frequencies, but the exact frequency of the Triggers is relatively unimportant to the successful operation of the SPC.

As illustrated, the sources of the Trigger are Slow 604 (in the range of 0.25 seconds to 15 minutes) and Fast 606 (in the range of 0.25 seconds to 3 seconds). Sources Slow 604 and Fast 606 are determined by the current execution state 608 of the SPC.

In the initial execution state the Trigger source is Slow 604, the execution state 608 is false, and Time Out state 610 is calculated to determine if Time to Call 612 should be evaluated (exceeding Next Call Out Date). If it is Time to Call, execution state 608 of the SPC is changed to Start Call 614. Start Call state 614 sets the execution state 608 true and all Active execution states use Fast 606 source. Fast 606 source drives the evaluation of all communication states as well as some additional housekeeping states.

While execution state 608 is true, the Time Out state 611 is evaluated at the rate of Fast 606. If there is no Time Out, execution state 616 will Execute and be evaluated at 618 to determine if the SPC should Advance to Next state 620. The execution state of the SPC will remain unchanged until each state is evaluated successfully or a Time Out occurs. In the event that a Time Out occurs, the state will Retry 619 as appropriate or assume an Error state 621. [Note that there are

some special communications driven error states not shown on this simplified diagram.]

Upon the successful completion of all execution states 608, execution state 608 is reset to false and Slow 604 Trigger again drives the state machine to evaluate the Time to Call condition.

Communications in the SPC:

The communications in the SPC are not interrupt driven in the conventional sense. Driving communications with UART interrupts would conflict with the requirements of SMM. The communications and the communication protocol are driven by the Fast Trigger source explained above. Remember that the Fast Trigger source can be varied in the range of 0.25 seconds to 3 seconds as required to improve the latency of SMM.

The Basic Protocol of the SPC is illustrated in Fig. 22. This figure applies to the execution of the communication state subset of all Active states of the SPC.

Transaction 630 begins at Compare UART state 632. The status of the UART is compared and evaluated to determine if activity has occurred outside of the execution environment of the SPC. In this simplified drawing of contention handling, if No Activity is detected, communications continue at step 638, otherwise, if DTR 634 has been reset, the communications will Abort at step 636. If DTR 634 is still active, the call will Hang-up at step 640.

Transaction packets 631 with the monitoring server 633 are designed to fit within FIFO 635 of a UART 637. This enables a polling method of communications in which the XMIT FIFO of the UART is filled with 16 bytes, or RECEIVER 639 is read for 16 bytes at each Fast 606 Trigger as appropriate.

If in a XMIT state 638, the SPC will Build the Packet 642, calculate the CRC 644, and then fill the FIFO of the UART with up to 16 bytes 646. The SPC returns to the OS and waits for the next Fast 606 Trigger. Packet data 631 sits in FIFO 635 of UART 637 awaiting transmission across the link.

If in a RECEIVE state 648, the SPC will Get the FIFO data for up to 16 bytes 650, check the CRC 652, and Decode the Packet 654. The receive FIFO of the UART may be empty, contain some of the packet bytes, or all of the packet bytes. The SPC did not need to respond to a UART interrupt and returns to the OS to wait until the next Fast Trigger to complete the transaction.

Resources for the SPC:

The actual size of the SPC can only be estimated until implemented in a specific BIOS, but the protocol and housekeeping code fit in about 2K. Extra code will be required to provide the Slow and Fast Triggers and to manipulate configuration data.

In the initial implementation, the triggers are generated by the legacy USB timer, which is shared by the legacy USB code. If the legacy USB support is not enabled, the timer can be controlled directly or shared with another function. This code requirement is fairly small since it is implemented by sharing existing functions for manipulating the chipset.

The housekeeping code does not need to reside entirely in post boot space. Some 20 bytes of persistent configuration needs to be stored and can reside in CMOS, the ESCD device, or both. This data can be stored in semi-persistent data space from within the SPC, such as CMOS, and then transferred to more persistent storage, such as the flash device, during the next boot cycle.

The interface code for a software driver needs to be implemented and will use the standard software SMI mechanisms.

This additional code should take no more than 2K compressed, for a total of no more than 4K of flash real estate. The dynamic requirements are around 2K of SMM space in the current implementation, but the SMM handler can vary the location of the SPC code. Some key parts of the SPC, especially the writeable data segment, must remain in SMM space. Currently this data segment is only about 48 bytes but may need to grow to around 100 bytes if required. If the state machine can also be contained in SMM space, the security of the SPC is enhanced.

The SPC Drivers

The SPC can be supplemented by software drivers:

Since the SPC is a subset of the existing product, the full functionality of CompuTrace will be provided by operating system dependent drivers. The CompuTrace Agent drivers have been developed for DOS, Win 31, Win 95, and Win NT.

These drivers will be enhanced to detect and communicate with the SPC. The API for communicating with the SPC will closely parallel the communications interface with the Server. The drivers will deposit transactions for the SPC to process when activated at a later time. By designing the API in this fashion, the resource requirements of the SPC will be minimized.

An illustration of the relationship between the software drivers and the SPC is contained in Fig. 23. This figure shows how the SPC is a security backup for the drivers and is usually disabled by transactions with software drivers. If the software drivers have not communicated recently with the SPC, the SPC will automatically complete the transaction with the monitoring server.

OEM configurations of the SPC:

We have identified four potential OEM configurations which embed the SPC.

DELL EXHIBIT 1002
Page 241 of 659

· The SPC is disabled

Provided for future use by the full CompuTrace driver suite.

· The SPC operates independently

Provided for protecting the unit from the point of manufacture, through the channel, then disabled when identified as a legitimate sale.

· The SPC is bundled with the full CompuTrace driver suite.

Provided as a value-added service for end-users direct from the point of manufacture.

· The SPC operates independently and is bundled with the full CompuTrace driver suite.

A combination of channel protection and value-added protection for the end-user.

This application contemplates sending and receiving signals from a client computer to a host system through a global network system. The Internet has been described in this application as merely one application of the invention. It is contemplated that this invention can and will be applied to other global network systems. Thus, the specific disclosure addressed to the Internet should not be construed as a limitation as to the scope of the invention, but rather should be considered to be merely one embodiment of the invention.

It will be understood by someone skilled in the art that many of the details described above are by way of example only and are not intended to limit the scope of the invention which is to be interpreted with reference to the claims which follow.

We Claim:

1. A method for tracing an electronic device characterized by:

providing an Agent(416) within the electronic device (400), the Agent configured to transmit identifying indicia (428) for the electronic device and/or its device components (402, 404, 406, 408, 410, 412, 414) to a host system (472) at a predetermined time without further intervention by the electronic device or user upon activation;

activating the Agent;

at the predetermined time, the Agent establishing a communication link (B) between the electronic device and the host system and transmitting the identifying indicia to the host system without intervention by the electronic device or user;

enabling the host system to determine the location of the electronic device based on tracing of the communication link.

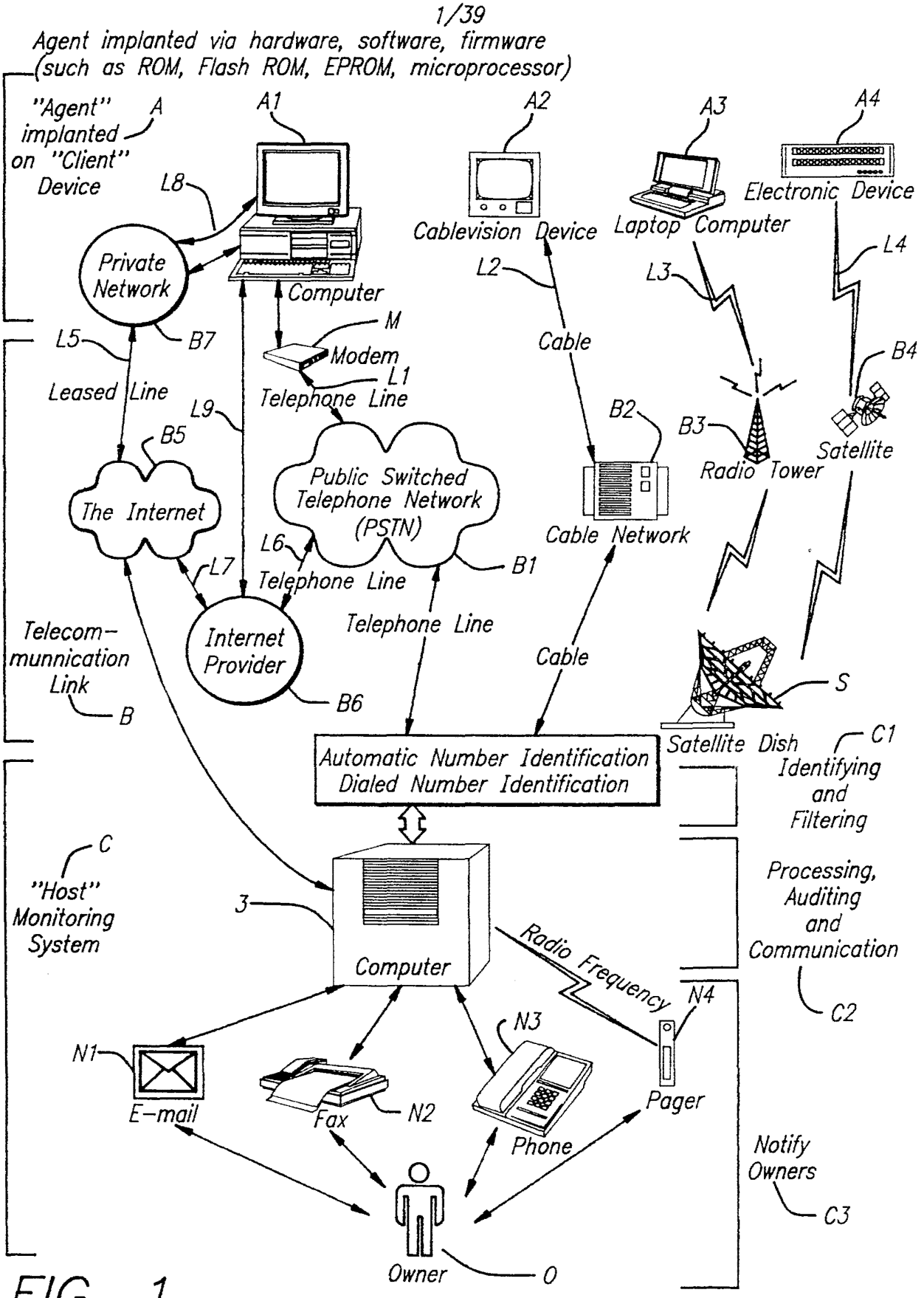

Agent implanted via hardware, software, firmware (such as ROM, Flash ROM, EPROM, microprocessor)
"Agent" implanted on "Client" Device
A
A1
A2
A3
A4
L8
Private Network
Computer
Cablevision Device
Laptop Computer
Electronic Device
L2
L3
L4
M
Modem
L1
Telephone Line
Cable
B4
L5
B7
Leased Line
L9
B5
B2
B3
Satellite
Radio Tower
The Internet
Public Switched Telephone Network (PSTN)
Cable Network
L6
L7
B1
Telephone Line
Telephone Line
Internet Provider
B6
Telecom-munnication Link
B
Cable
S
Satellite Dish
C1
Automatic Number Identification
Dialed Number Identification
Identifying and Filtering
C
"Host" Monitoring System
3
Computer
Radio Frequency
Processing, Auditing and Communication
C2
N4
N3
N1
E-mail
Fax
N2
Phone
Pager
Notify Owners
C3
Owner
O

FIG. 1

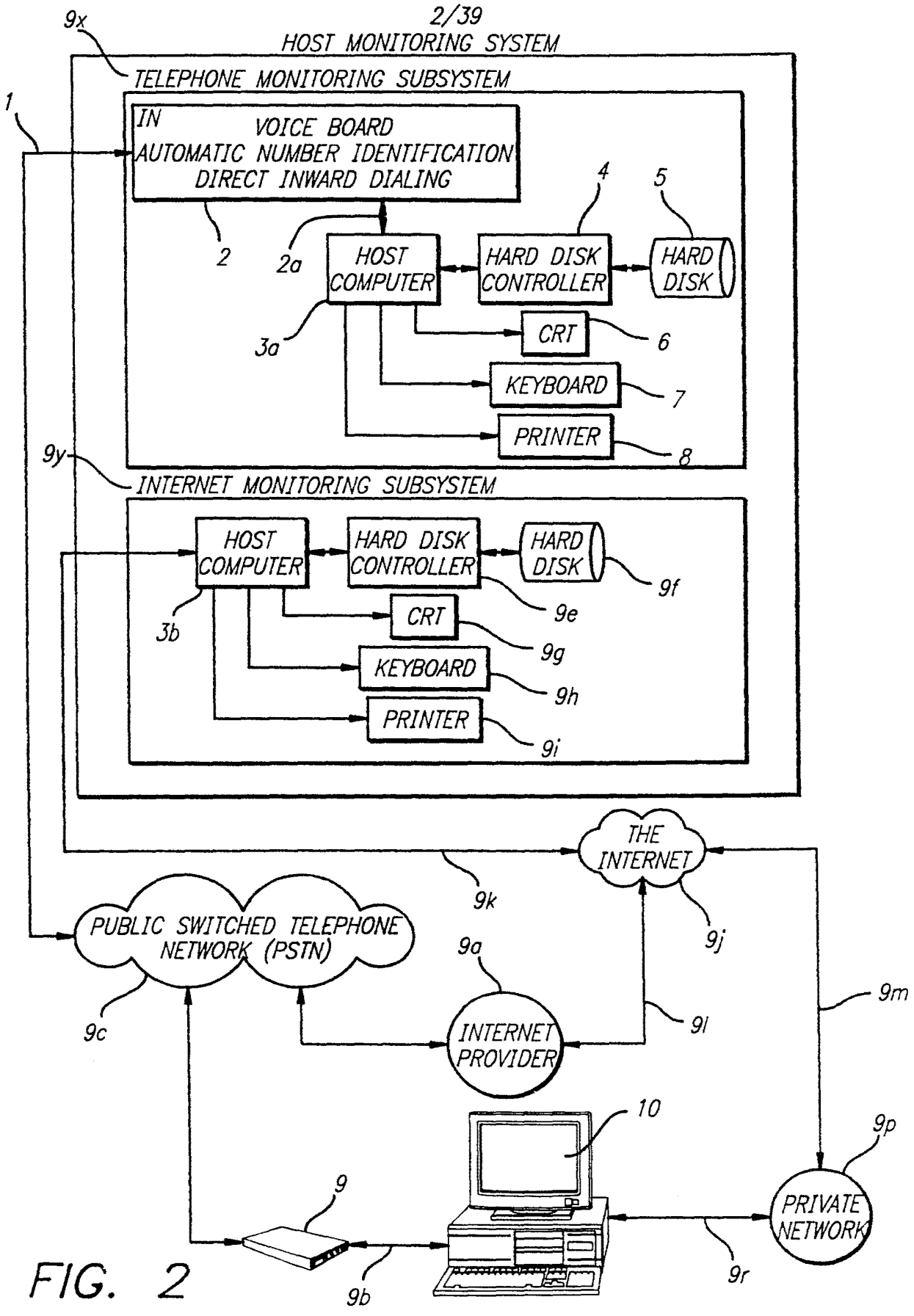


FIG. 2

DELL EXHIBIT 1002
Page 245 of 659

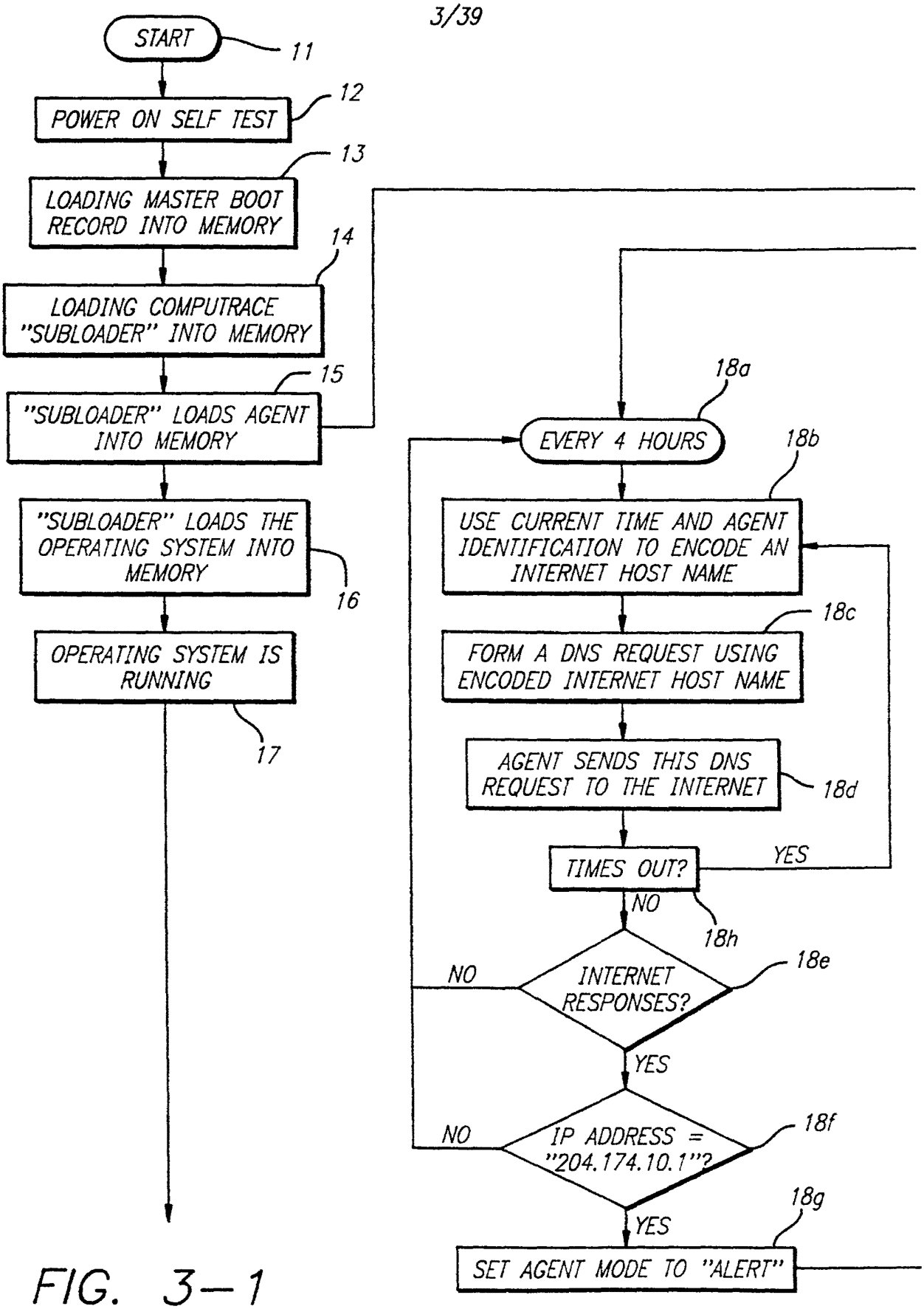


FIG. 3-1

DELL EXHIBIT 1002
Page 246 of 659

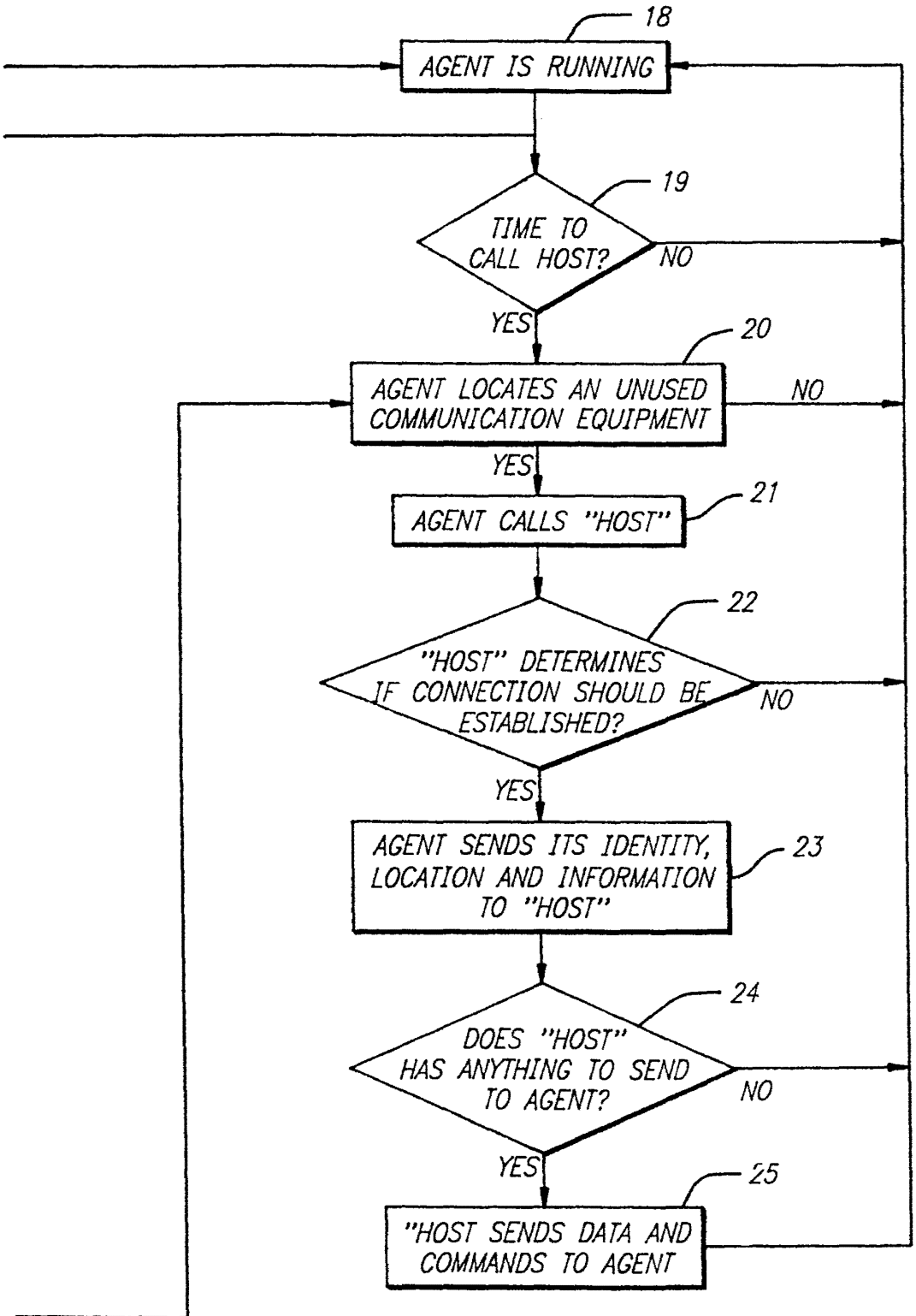

18
AGENT IS RUNNING
19
TIME TO CALL HOST?
NO
YES
20
AGENT LOCATES AN UNUSED COMMUNICATION EQUIPMENT
NO
YES
21
AGENT CALLS "HOST"
22
"HOST" DETERMINES IF CONNECTION SHOULD BE ESTABLISHED?
NO
YES
AGENT SENDS ITS IDENTITY, LOCATION AND INFORMATION TO "HOST"
23
24
DOES "HOST" HAS ANYTHING TO SEND TO AGENT?
NO
YES
25
"HOST SENDS DATA AND COMMANDS TO AGENT

FIG. 3-2

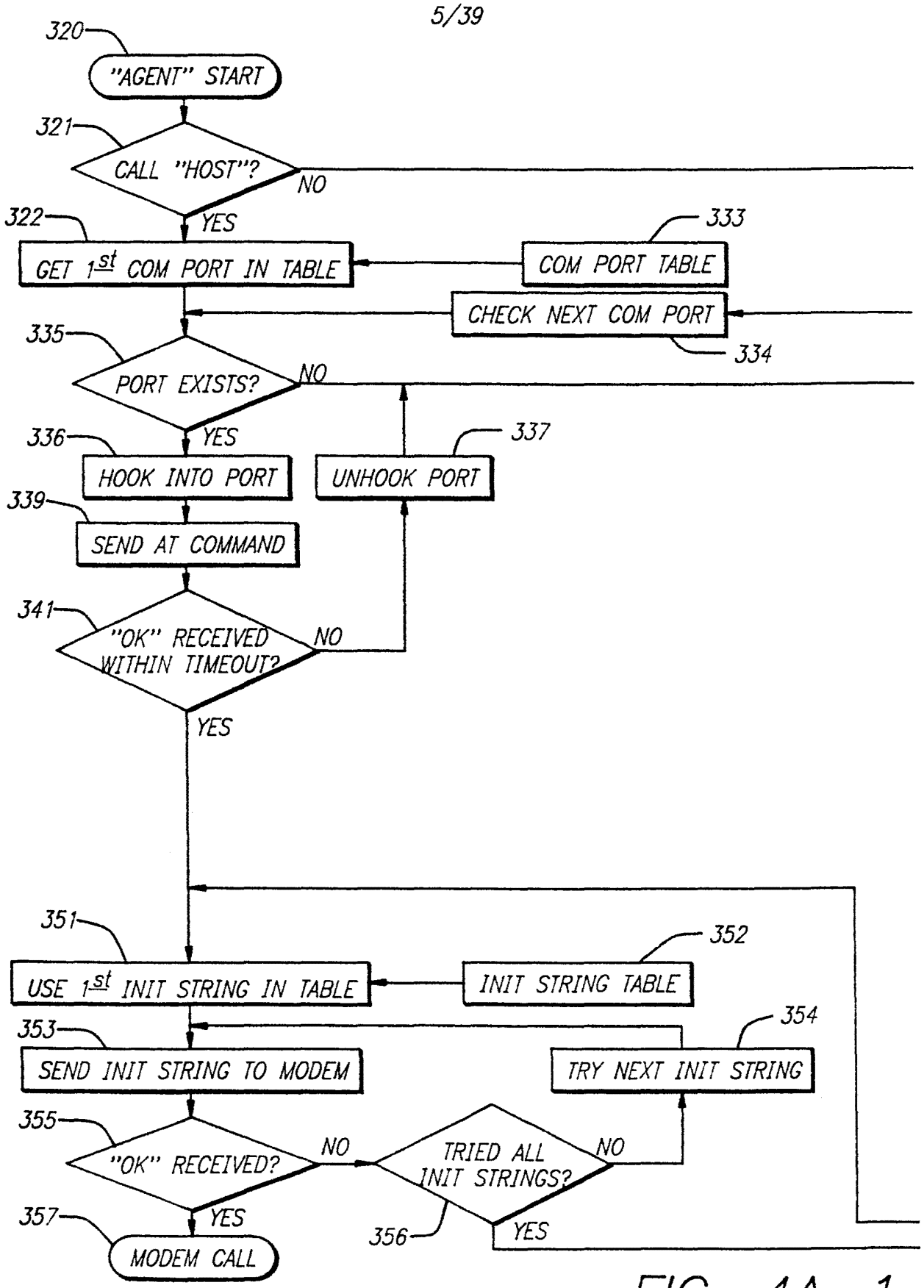
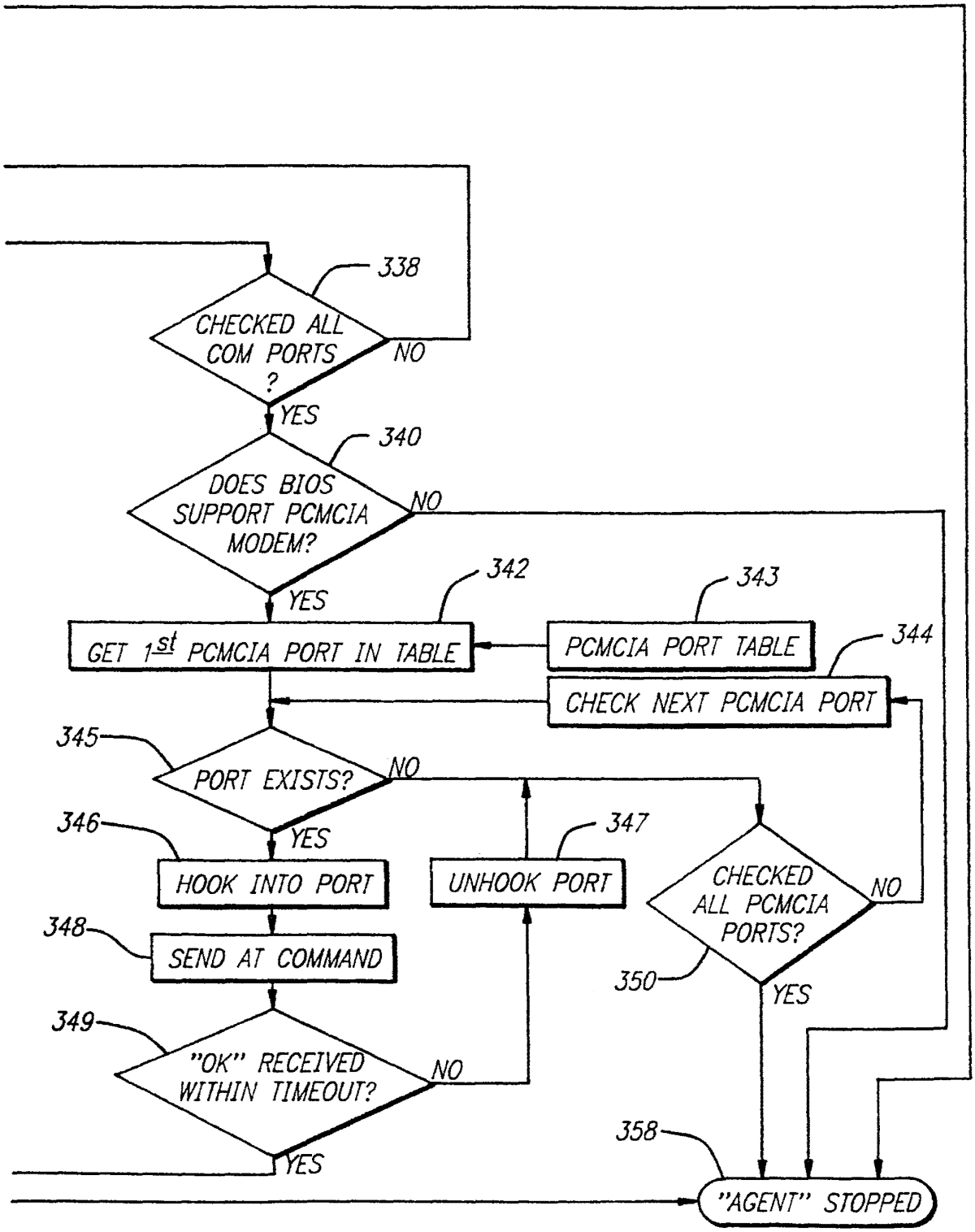


FIG. 4A—1

DELL EXHIBIT 1002
Page 248 of 659

FIG. 4A-2


338
CHECKED ALL COM PORTS ?
NO
YES
340
DOES BIOS SUPPORT PCMCIA MODEM?
NO
YES
342
343
GET 1st PCMCIA PORT IN TABLE
PCMCIA PORT TABLE
344
CHECK NEXT PCMCIA PORT
345
PORT EXISTS?
NO
YES
346
347
HOOK INTO PORT
UNHOOK PORT
CHECKED ALL PCMCIA PORTS?
NO
348
SEND AT COMMAND
350
YES
349
"OK" RECEIVED WITHIN TIMEOUT?
NO
YES
358
"AGENT" STOPPED

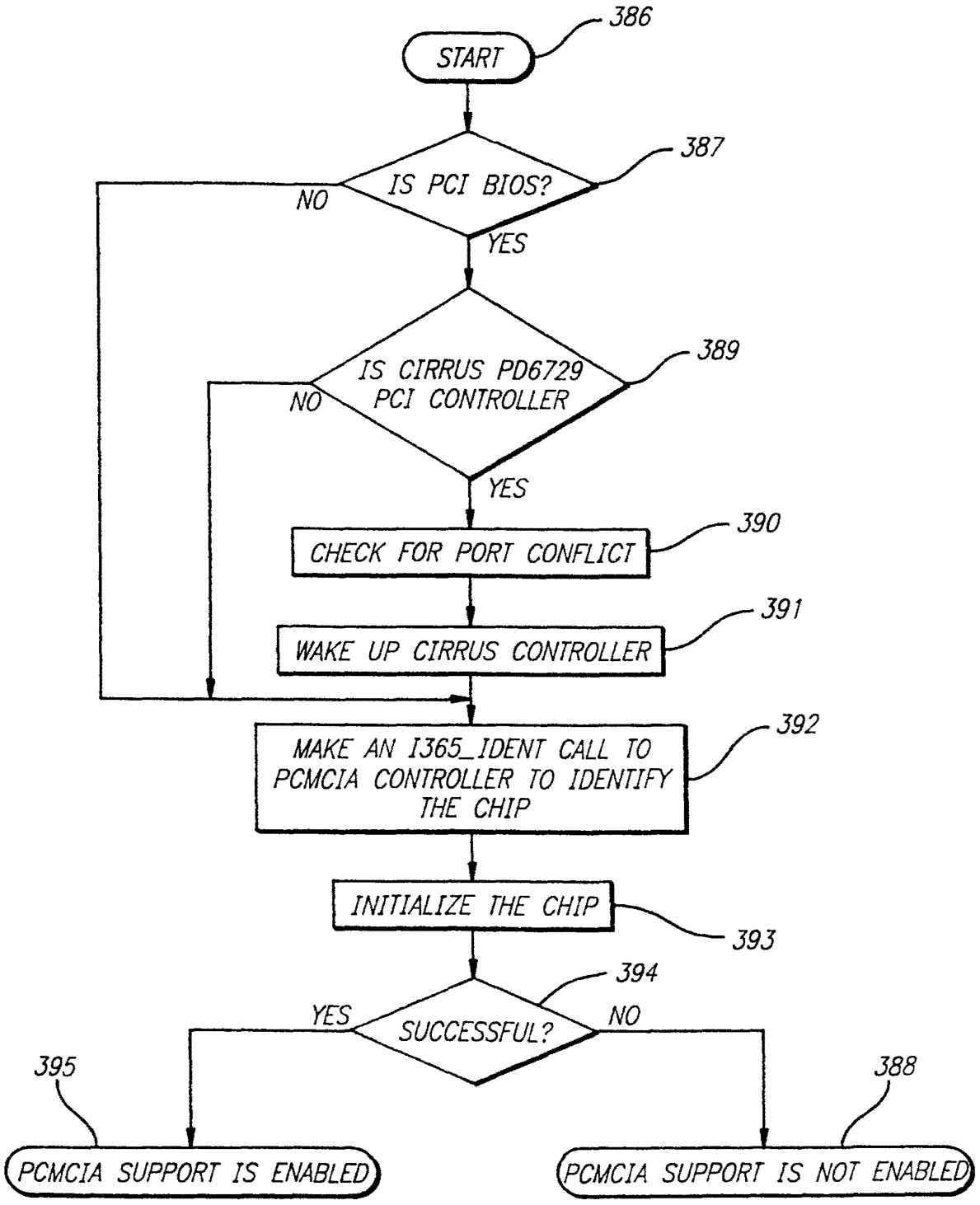


FIG. 4B

DELL EXHIBIT 1002
Page 250 of 659

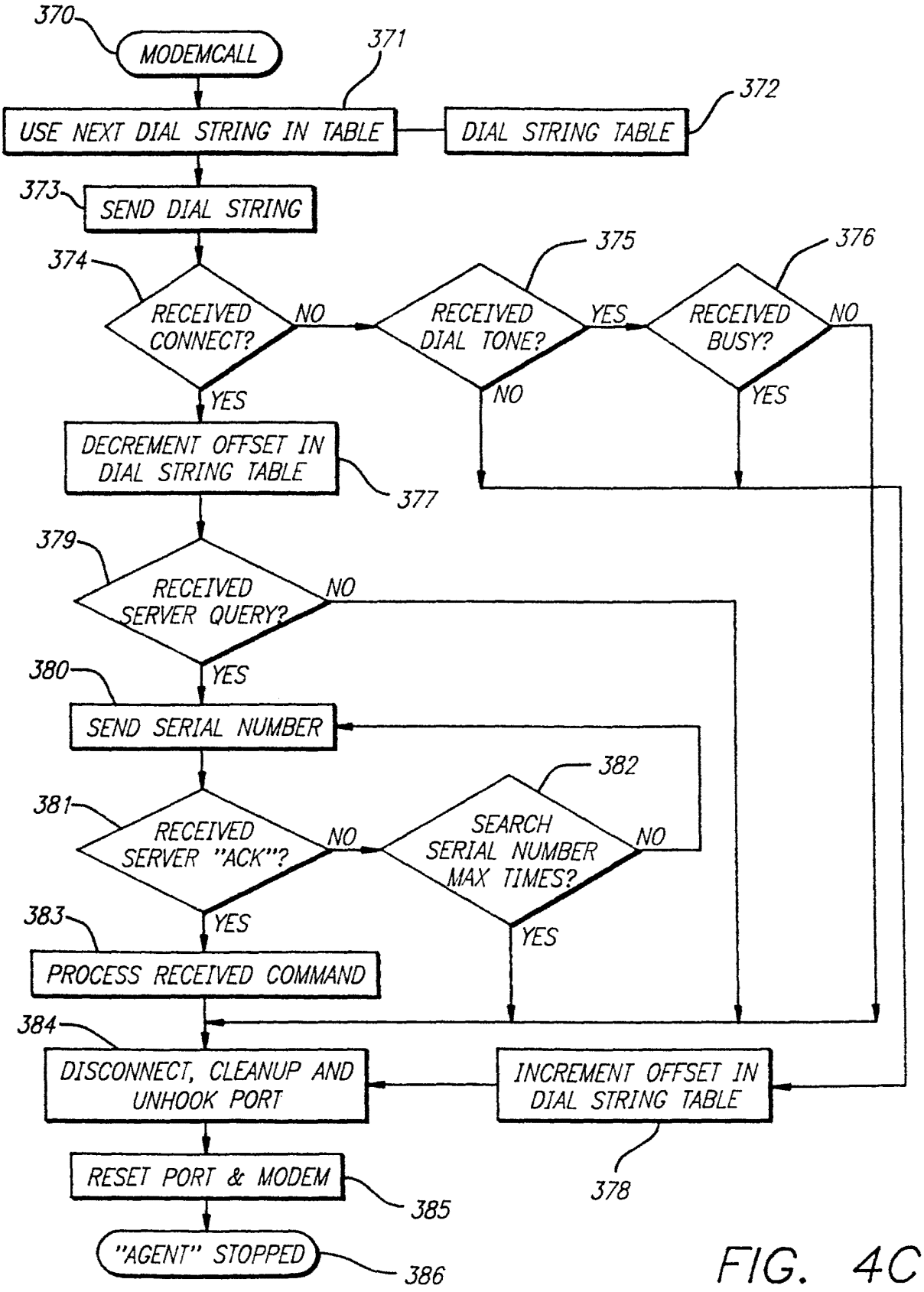

370
MODEMCALL
371
USE NEXT DIAL STRING IN TABLE
372
DIAL STRING TABLE
373
SEND DIAL STRING
374
RECEIVED CONNECT?
NO
375
RECEIVED DIAL TONE?
YES
376
RECEIVED BUSY?
NO
YES
NO
YES
DECREMENT OFFSET IN DIAL STRING TABLE
377
379
RECEIVED SERVER QUERY?
NO
YES
380
SEND SERIAL NUMBER
382
381
RECEIVED SERVER "ACK"?
NO
SEARCH SERIAL NUMBER MAX TIMES?
NO
YES
YES
383
PROCESS RECEIVED COMMAND
384
DISCONNECT, CLEANUP AND UNHOOK PORT
INCREMENT OFFSET IN DIAL STRING TABLE
378
RESET PORT & MODEM
385
"AGENT" STOPPED
386

FIG. 4C

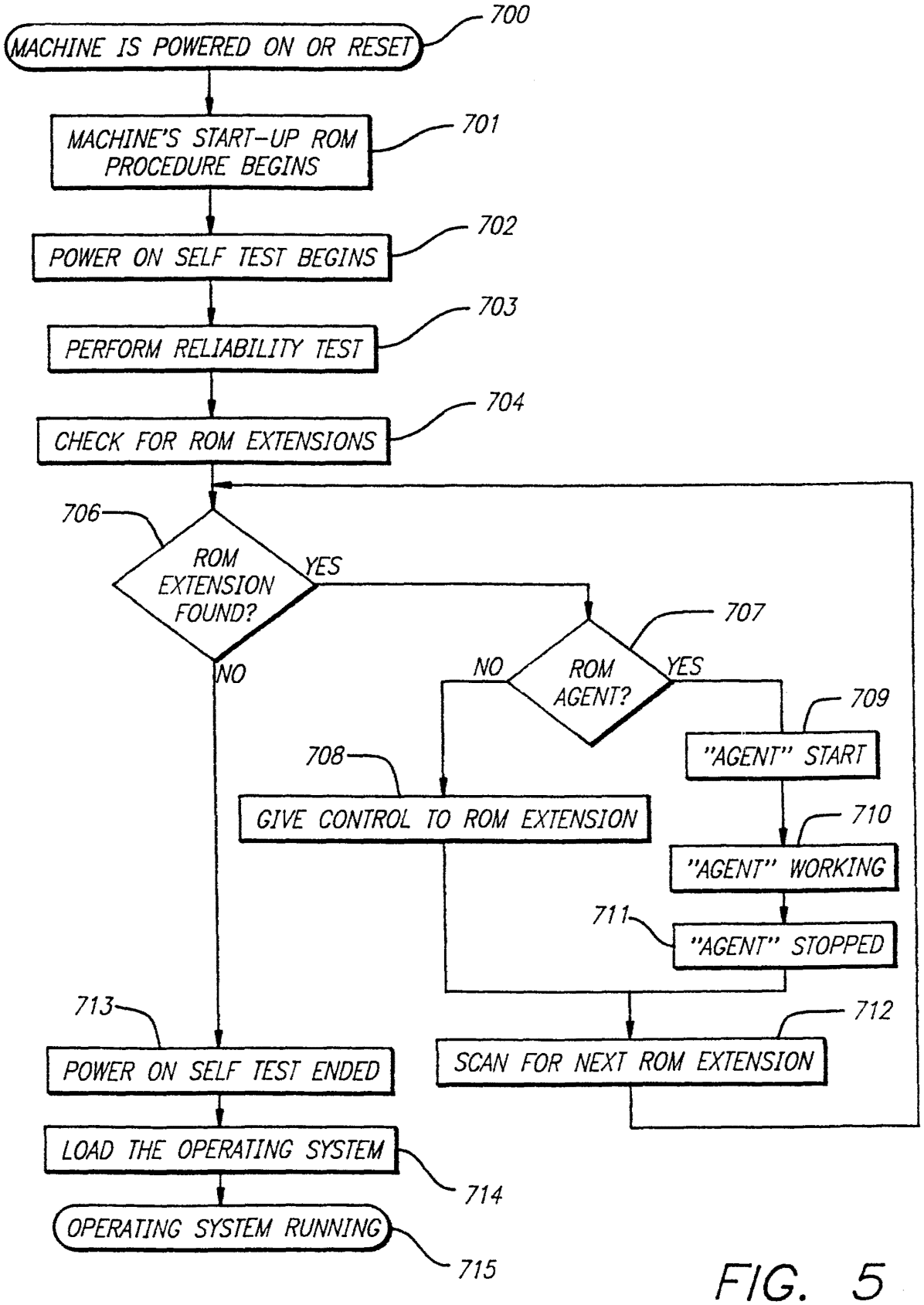


FIG. 5

DELL EXHIBIT 1002
Page 252 of 659

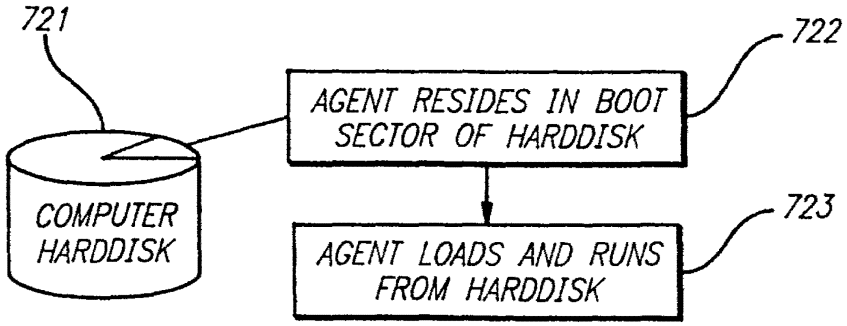


FIG. 6A

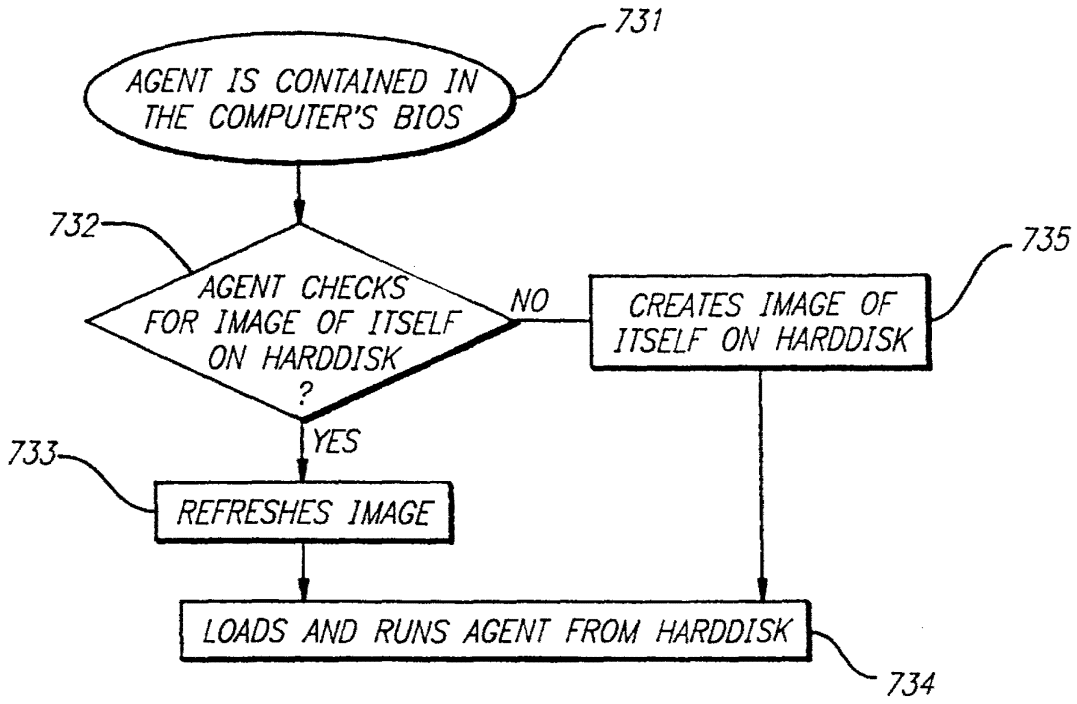


FIG. 6C

DELL EXHIBIT 1002
Page 253 of 659

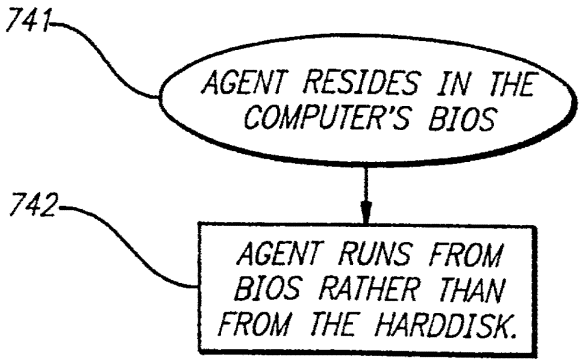


FIG. 6D

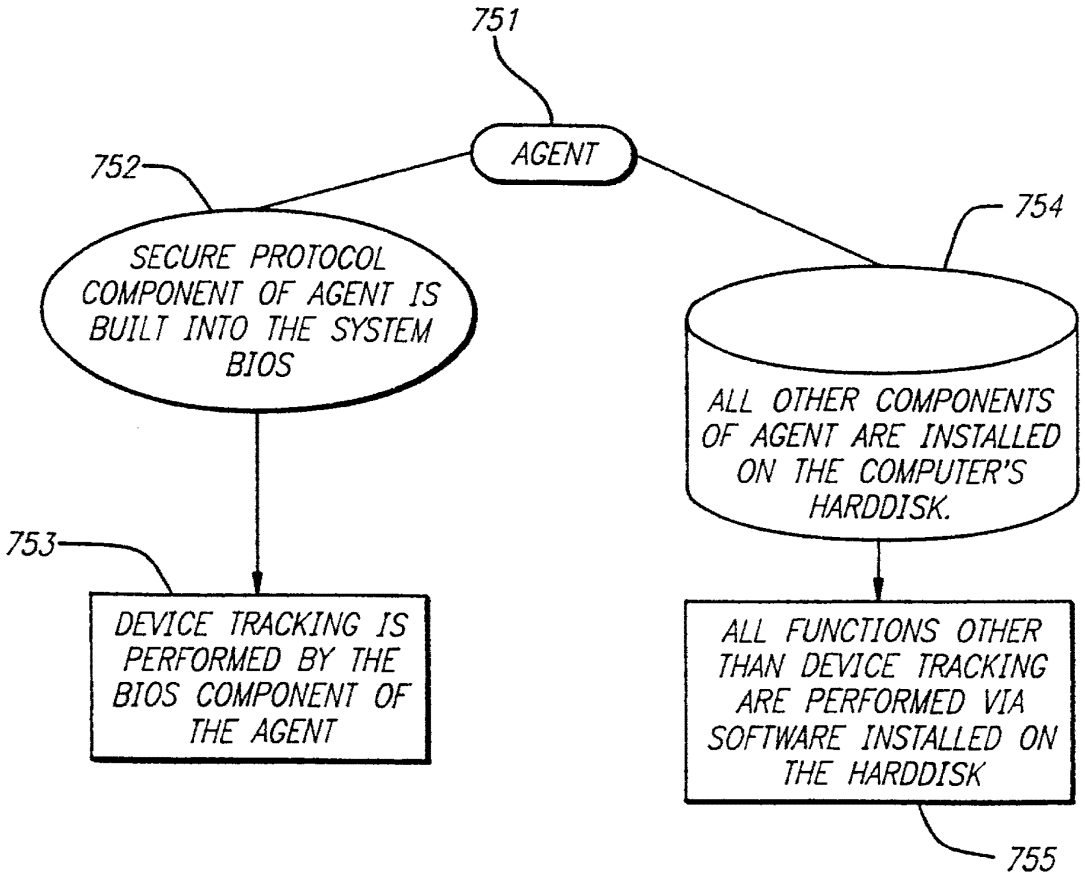


FIG. 7A

DELL EXHIBIT 1002
Page 254 of 659

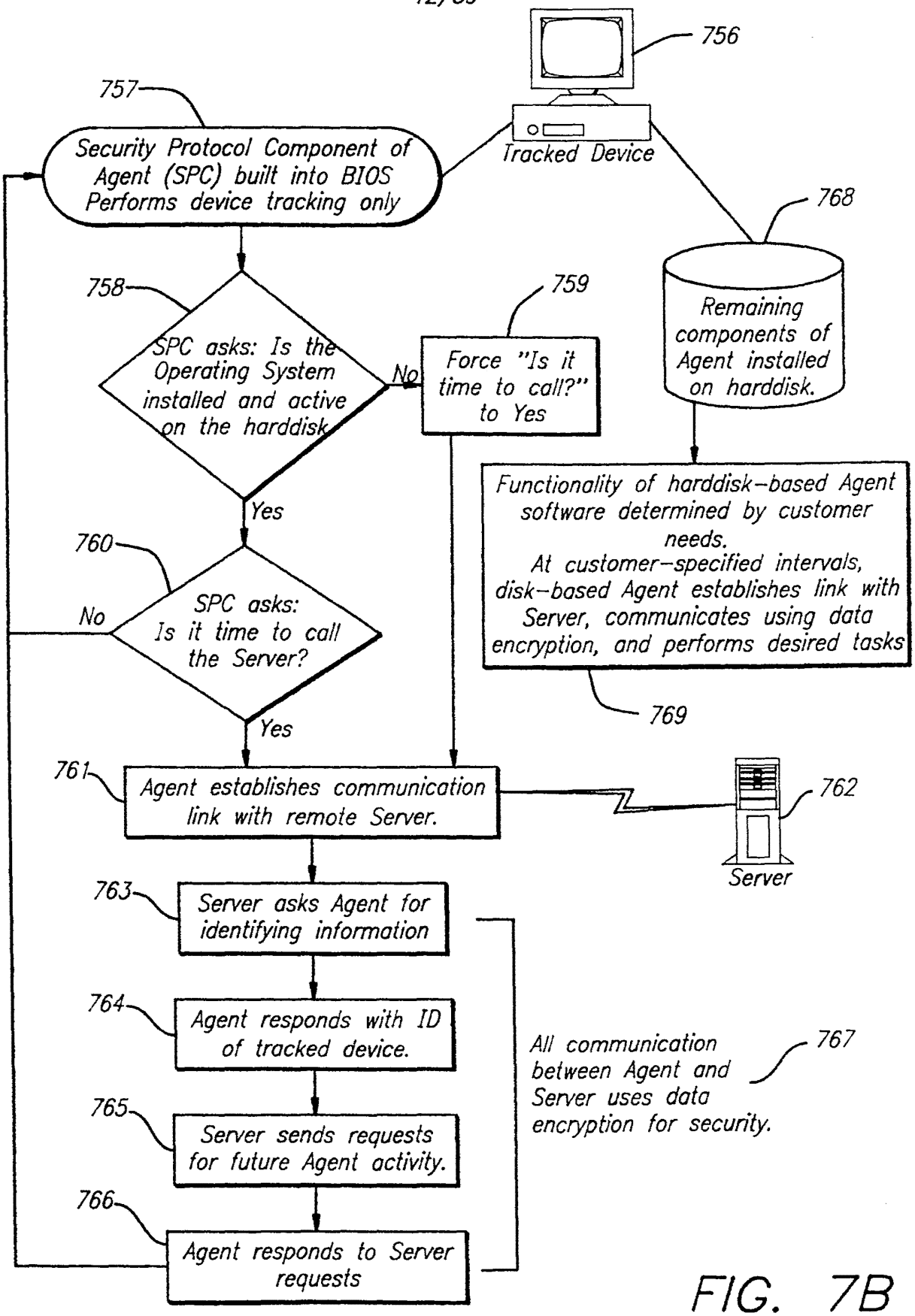


FIG. 7B

DELL EXHIBIT 1002
Page 255 of 659

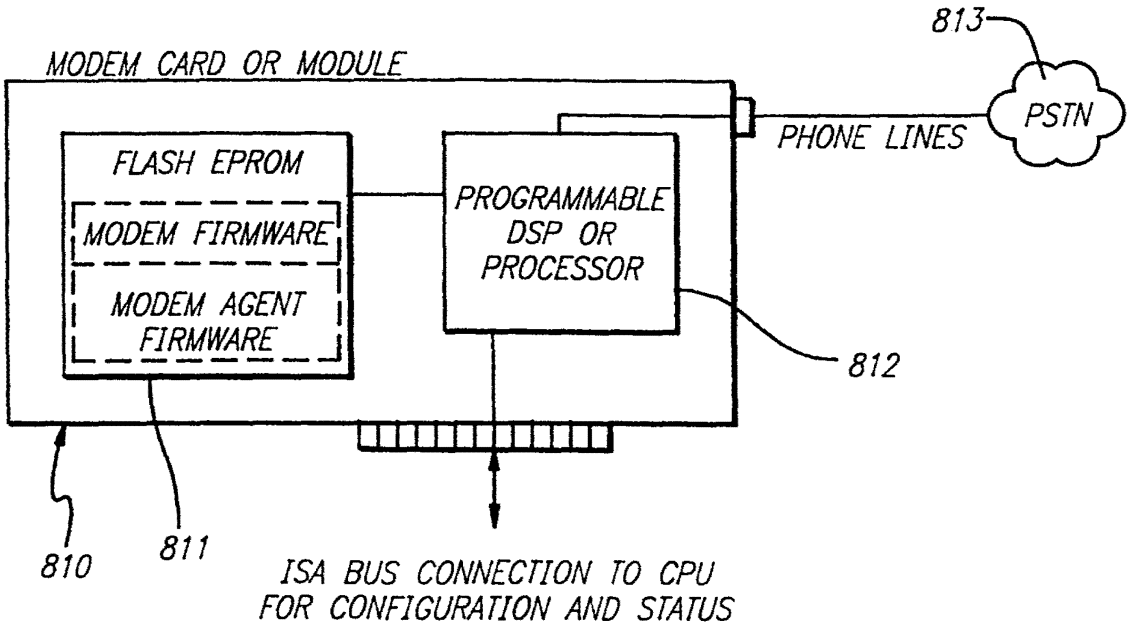

813
MODEM CARD OR MODULE
PSTN
PHONE LINES
FLASH EPROM
MODEM FIRMWARE
MODEM AGENT FIRMWARE
PROGRAMMABLE DSP OR PROCESSOR
812
810
811
ISA BUS CONNECTION TO CPU FOR CONFIGURATION AND STATUS

FIG. 8A

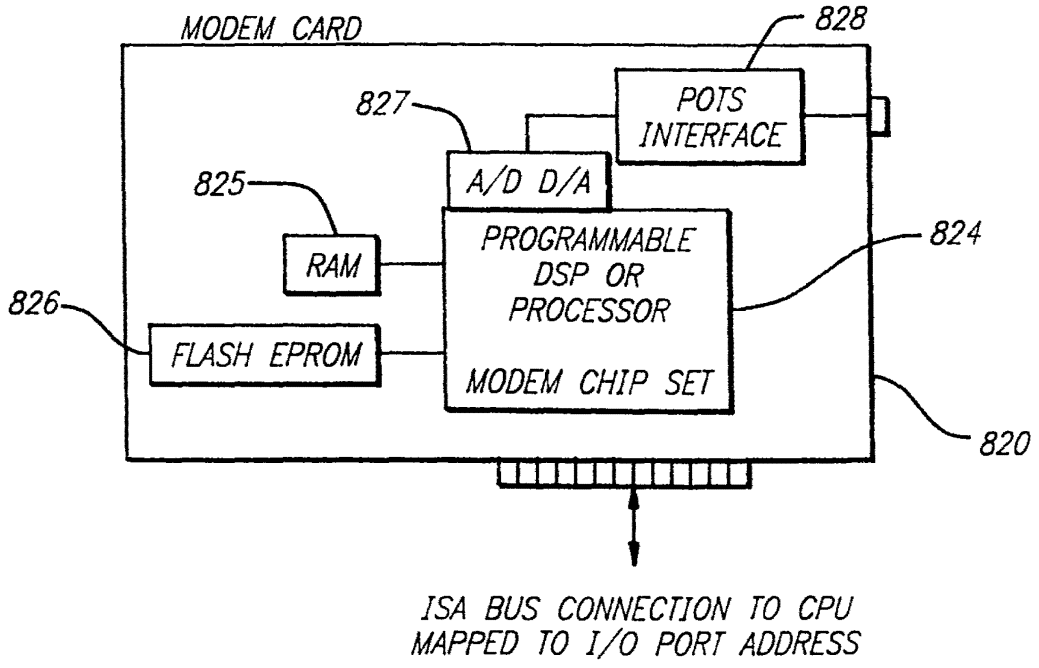

MODEM CARD
828
POTS INTERFACE
827
A/D D/A
825
RAM
PROGRAMMABLE DSP OR PROCESSOR
824
826
FLASH EPROM
MODEM CHIP SET
820
ISA BUS CONNECTION TO CPU MAPPED TO I/O PORT ADDRESS

FIG. 8B

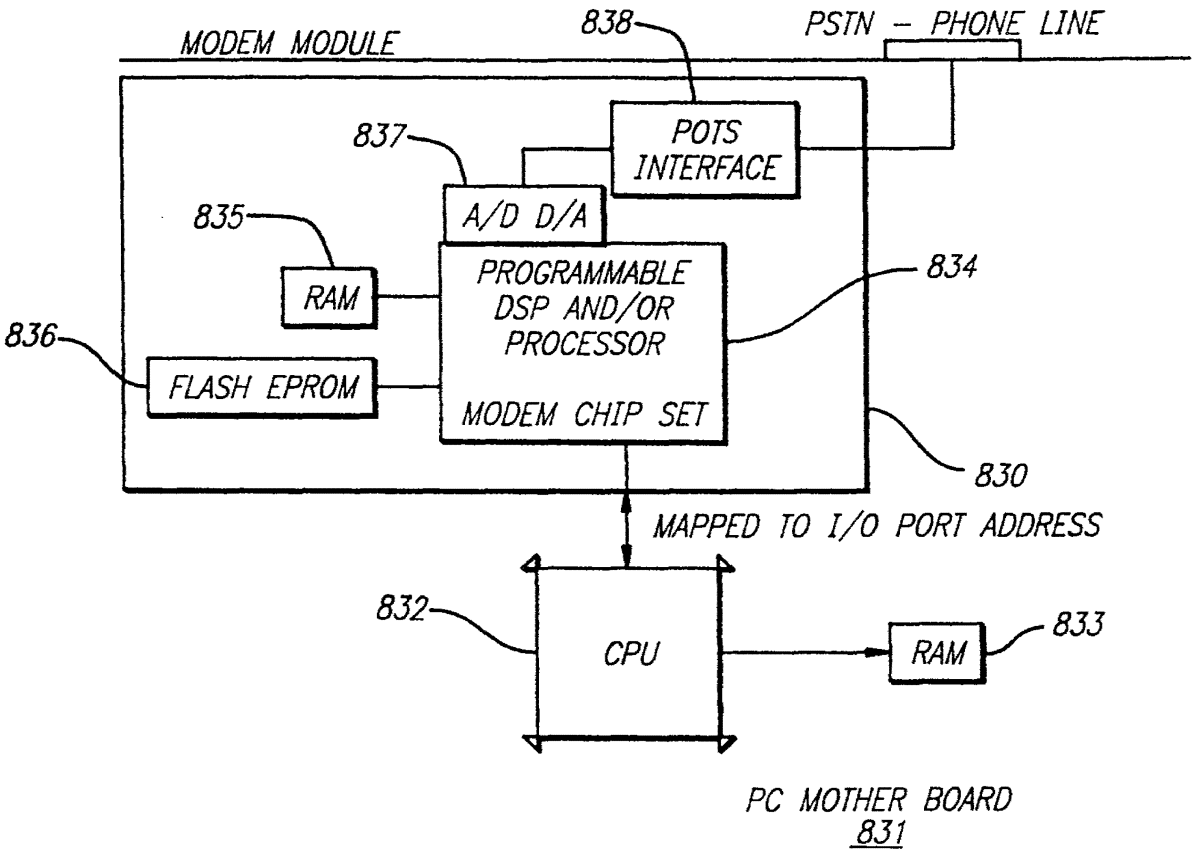

MODEM MODULE
838
PSTN – PHONE LINE
837
POTS INTERFACE
A/D D/A
835
RAM
PROGRAMMABLE DSP AND/OR PROCESSOR
834
836
FLASH EPROM
MODEM CHIP SET
830
MAPPED TO I/O PORT ADDRESS
832
CPU
RAM
833
PC MOTHER BOARD
831

FIG. 8C

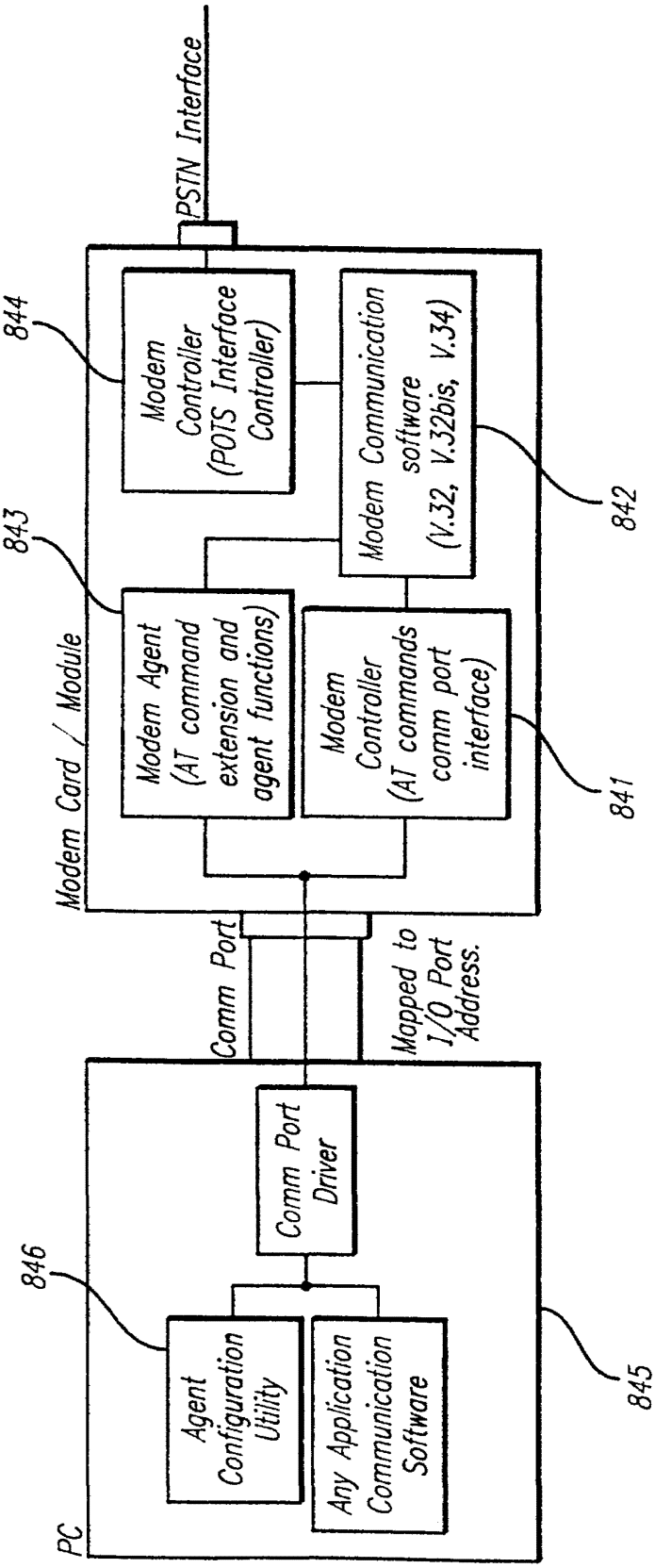


FIG. 8D

DELL EXHIBIT 1002
Page 258 of 659

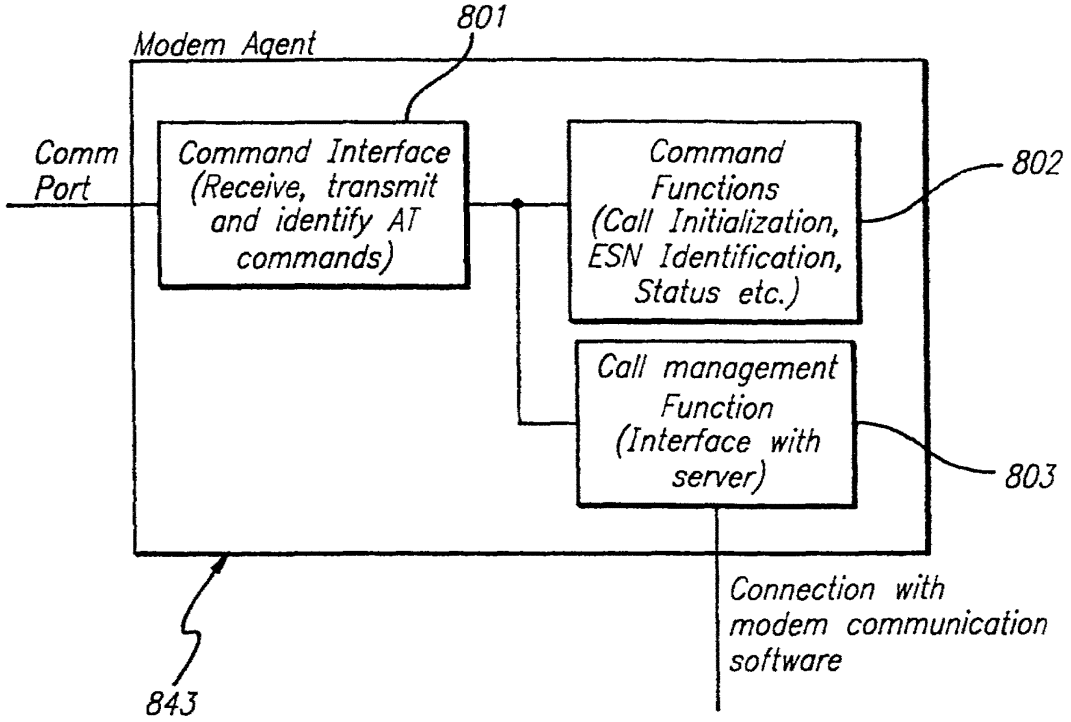


FIG. 8E

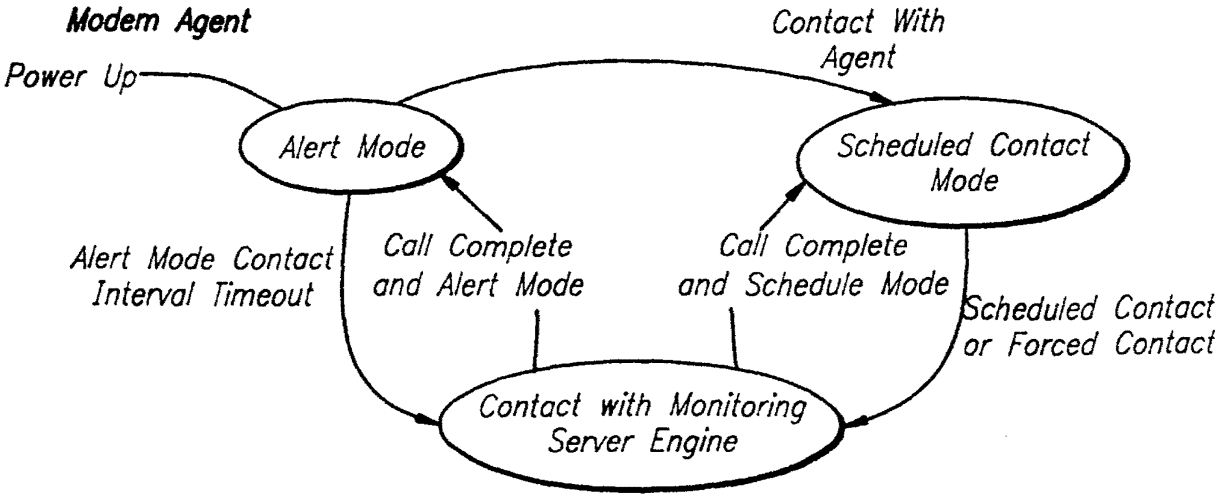


FIG. 8F

DELL EXHIBIT 1002
Page 259 of 659

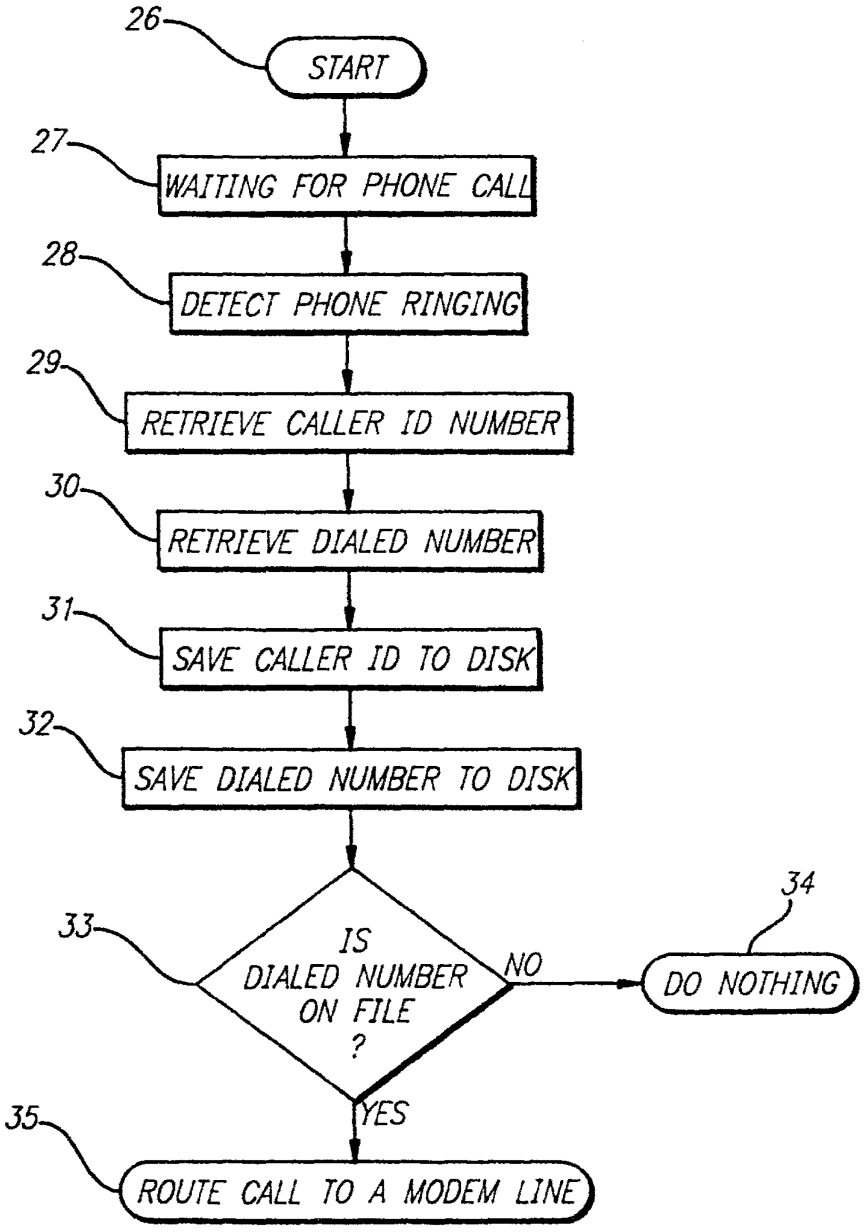

26
START
27
WAITING FOR PHONE CALL
28
DETECT PHONE RINGING
29
RETRIEVE CALLER ID NUMBER
30
RETRIEVE DIALED NUMBER
31
SAVE CALLER ID TO DISK
32
SAVE DIALED NUMBER TO DISK
33
IS DIALED NUMBER ON FILE ?
NO
34
DO NOTHING
YES
35
ROUTE CALL TO A MODEM LINE

FIG. 9

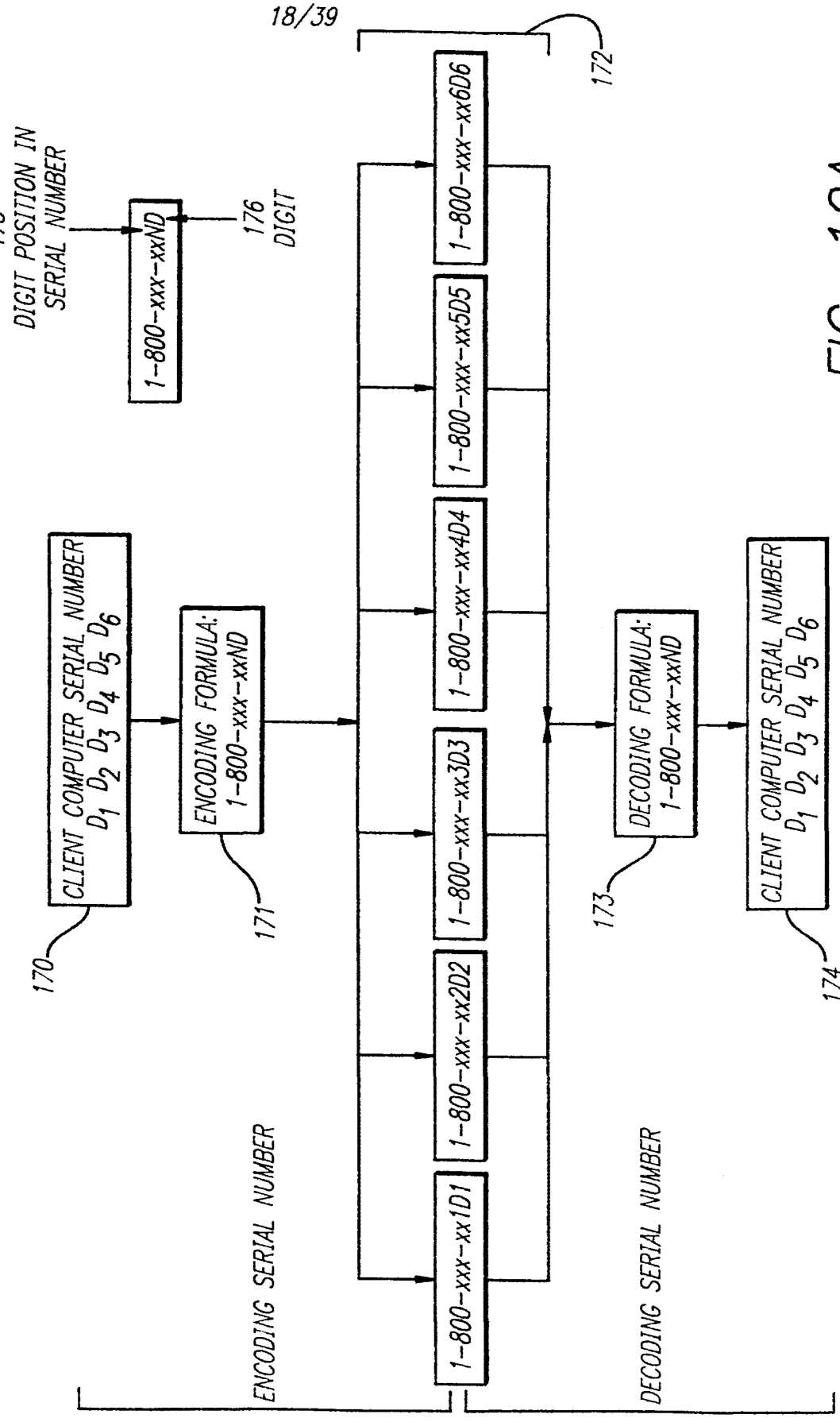


FIG. 10A

DELL EXHIBIT 1002
Page 261 of 659

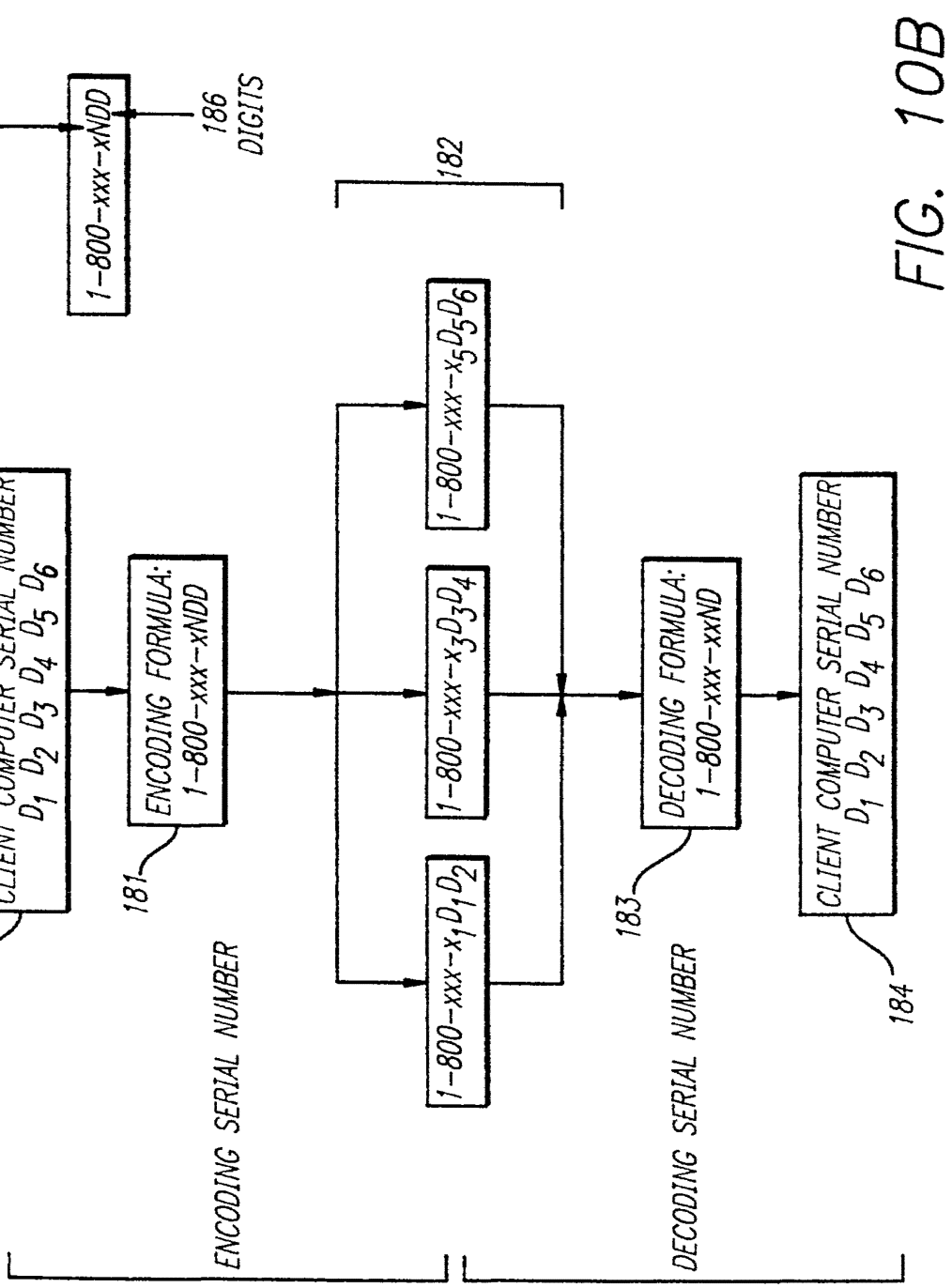

185
DIGIT POSITION IN SERIAL NUMBER
1-800-xxx-xNDD
186
DIGITS
182
CLIENT COMPUTER SERIAL NUMBER
D_1 D_2 D_3 D_4 D_5 D_6
180
ENCODING FORMULA:
1-800-xxx-xNDD
181
1-800-xxx-$x_1D_1D_2$
1-800-xxx-$x_3D_3D_4$
1-800-xxx-$x_5D_5D_6$
ENCODING SERIAL NUMBER
DECODING FORMULA:
1-800-xxx-xxND
183
CLIENT COMPUTER SERIAL NUMBER
D_1 D_2 D_3 D_4 D_5 D_6
184
DECODING SERIAL NUMBER

FIG. 10B

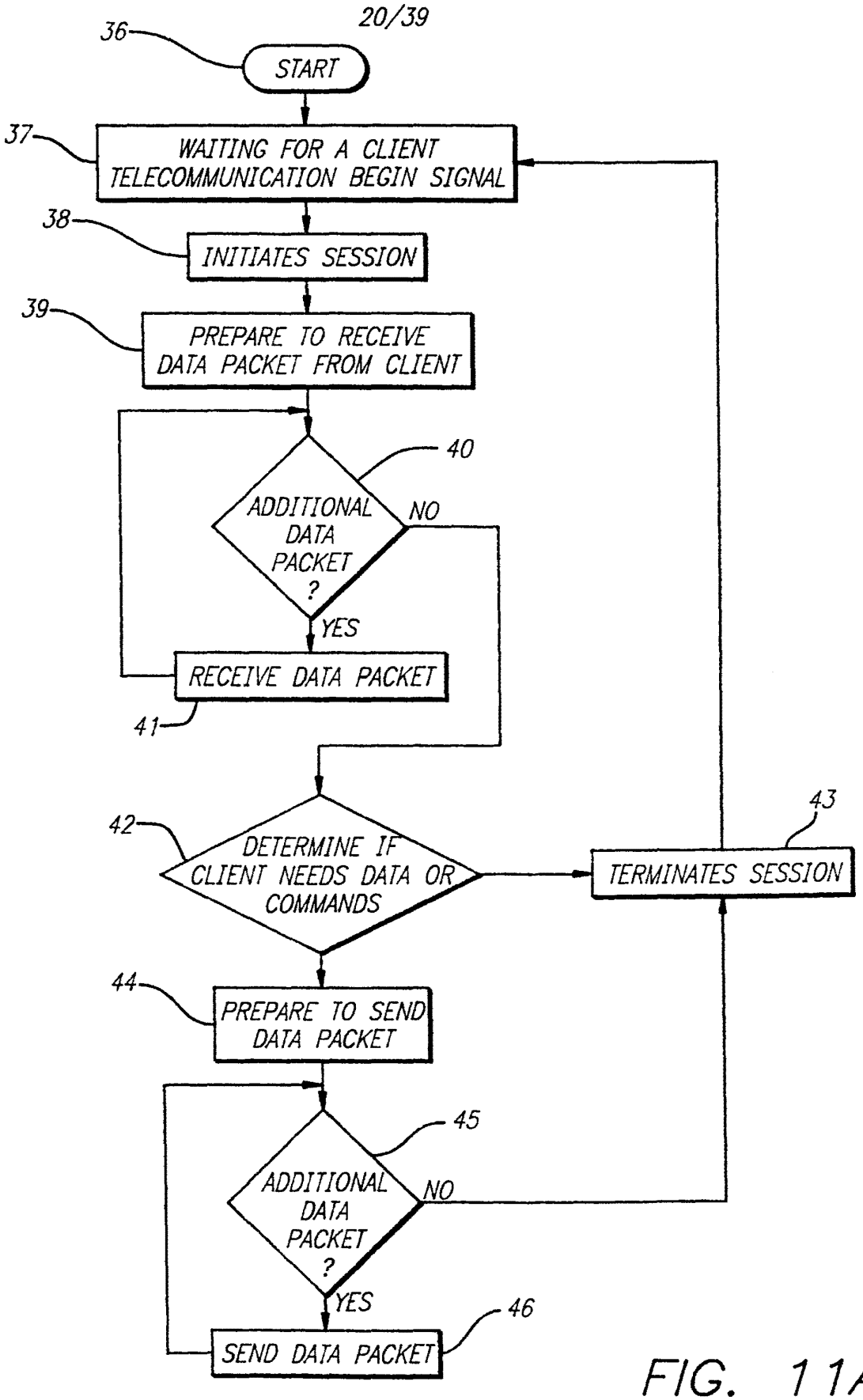


FIG. 11A

DELL EXHIBIT 1002
Page 263 of 659

FIG. 11B

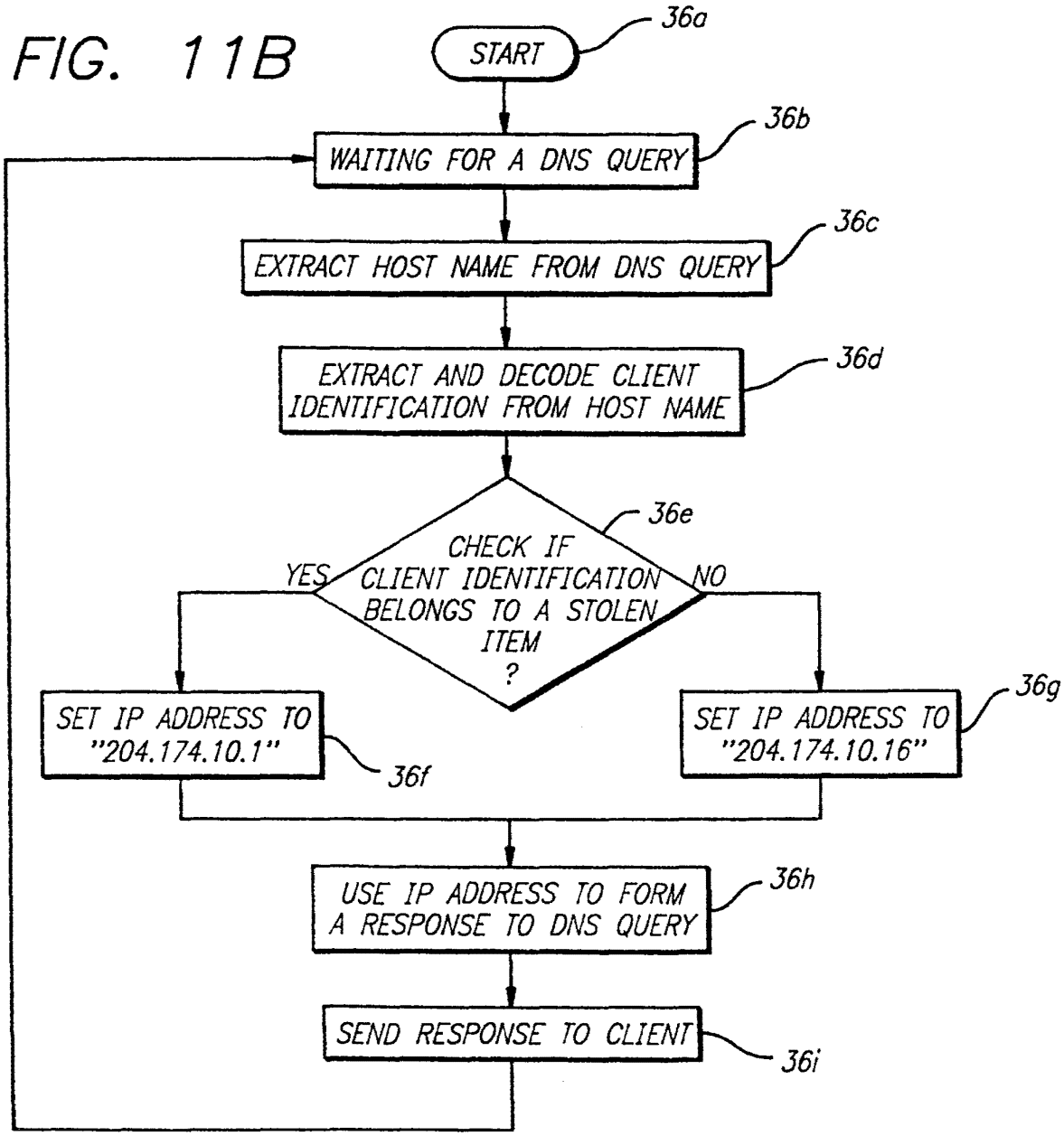
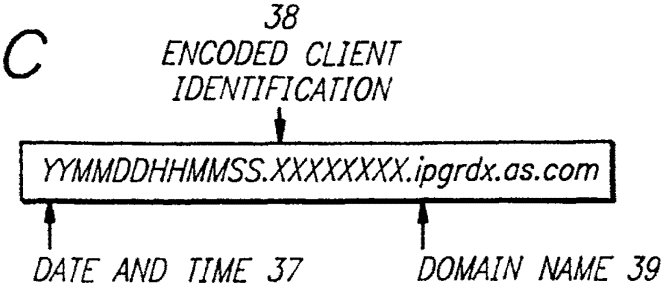


FIG. 11C



DELL EXHIBIT 1002
Page 264 of 659

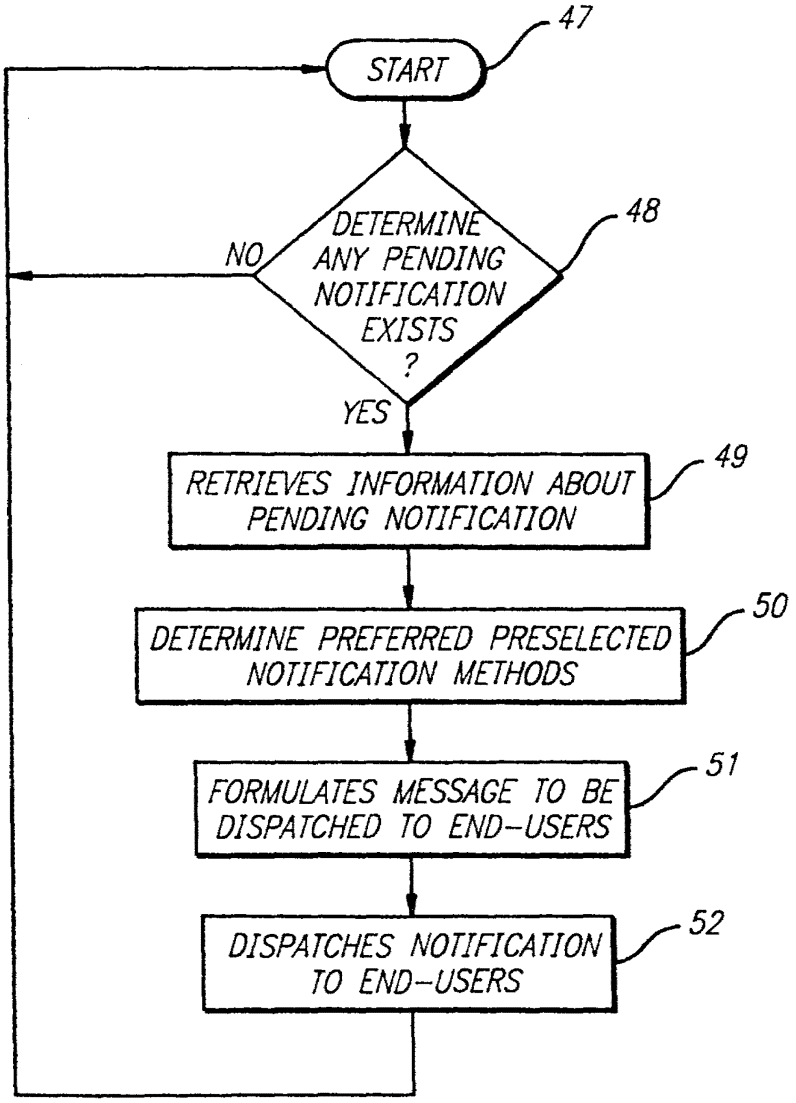

47
START
48
DETERMINE ANY PENDING NOTIFICATION EXISTS ?
NO
YES
49
RETRIEVES INFORMATION ABOUT PENDING NOTIFICATION
50
DETERMINE PREFERRED PRESELECTED NOTIFICATION METHODS
51
FORMULATES MESSAGE TO BE DISPATCHED TO END-USERS
52
DISPATCHES NOTIFICATION TO END-USERS

FIG. 12

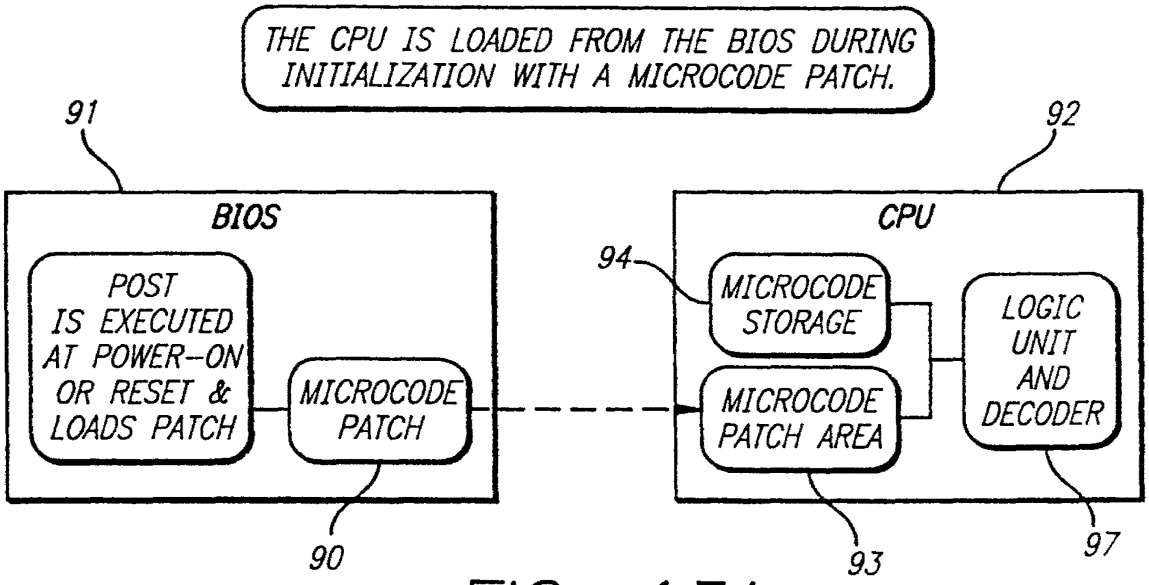


FIG. 13A

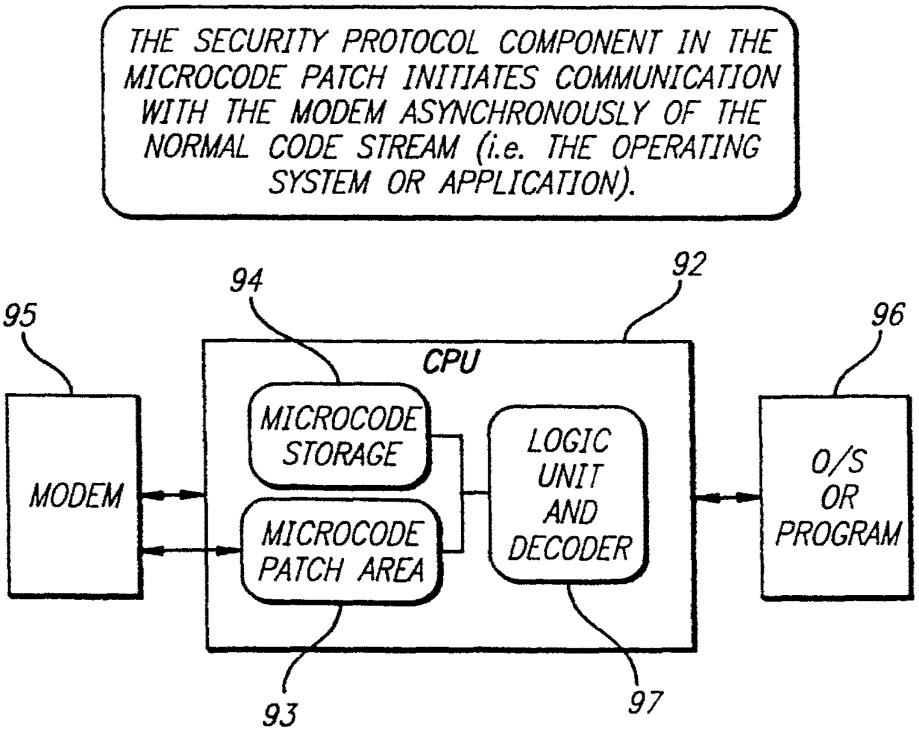


FIG. 13B

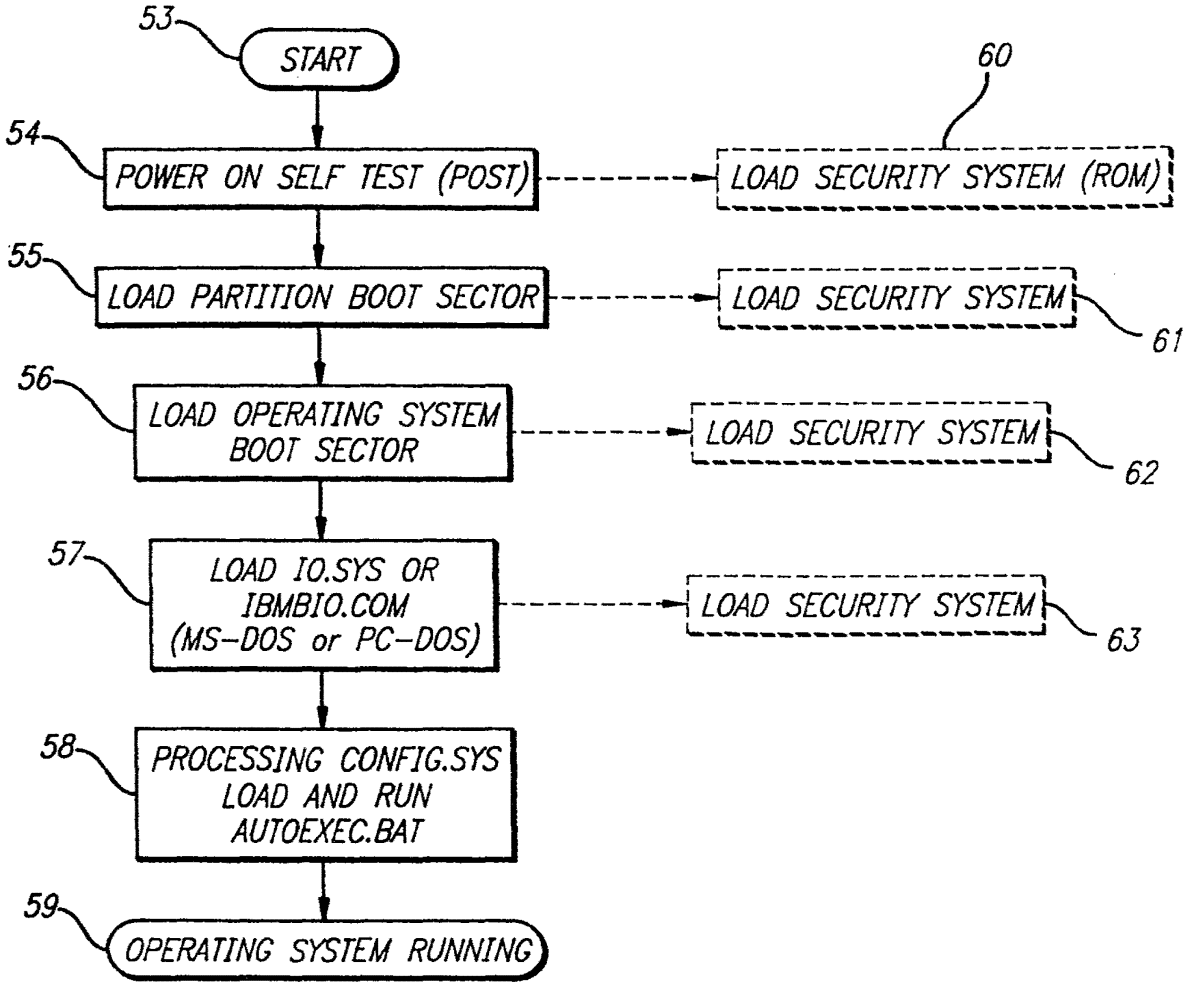


FIG. 14

DELL EXHIBIT 1002
Page 267 of 659

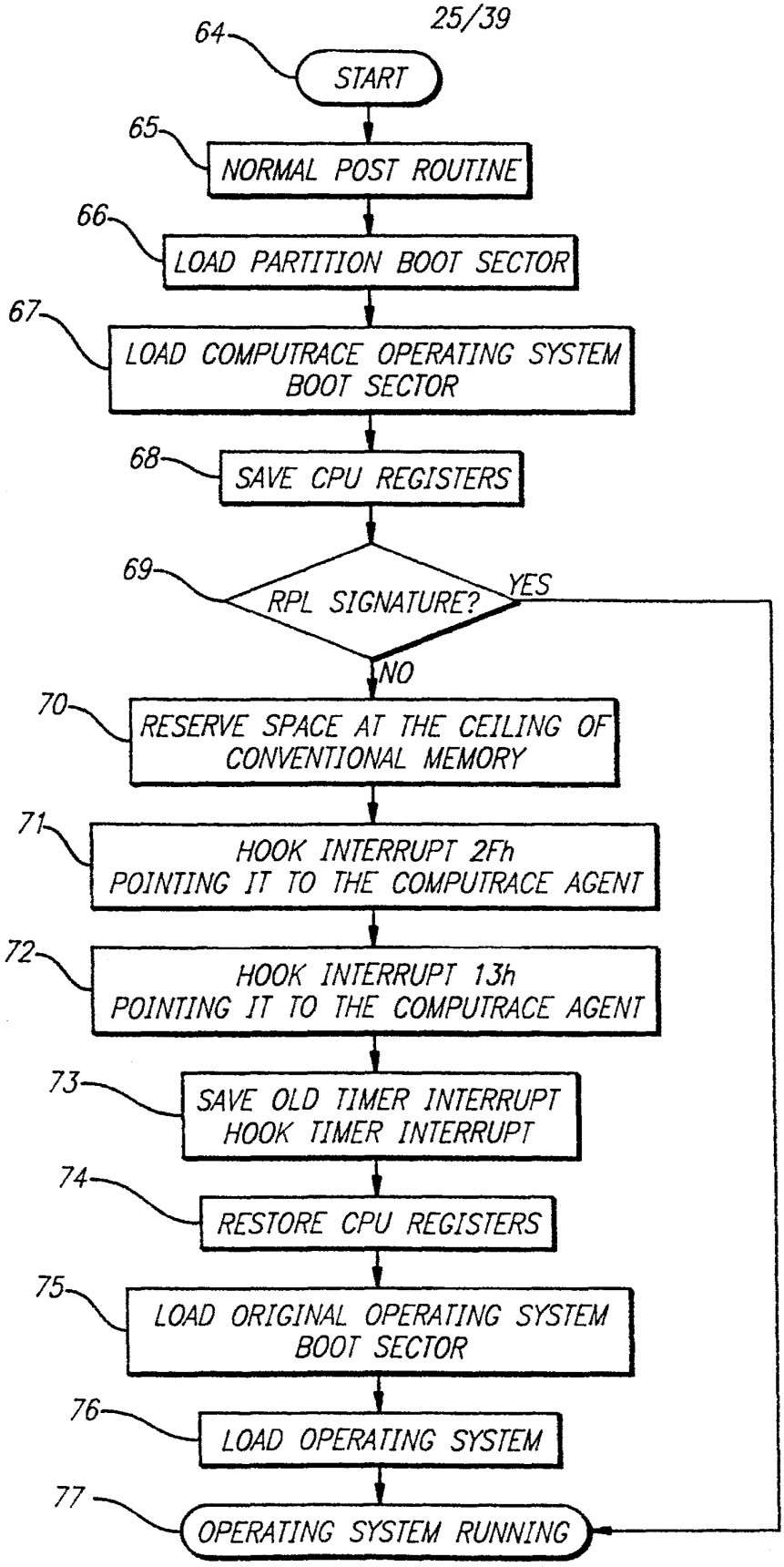


FIG. 14A

DELL EXHIBIT 1002
Page 268 of 659

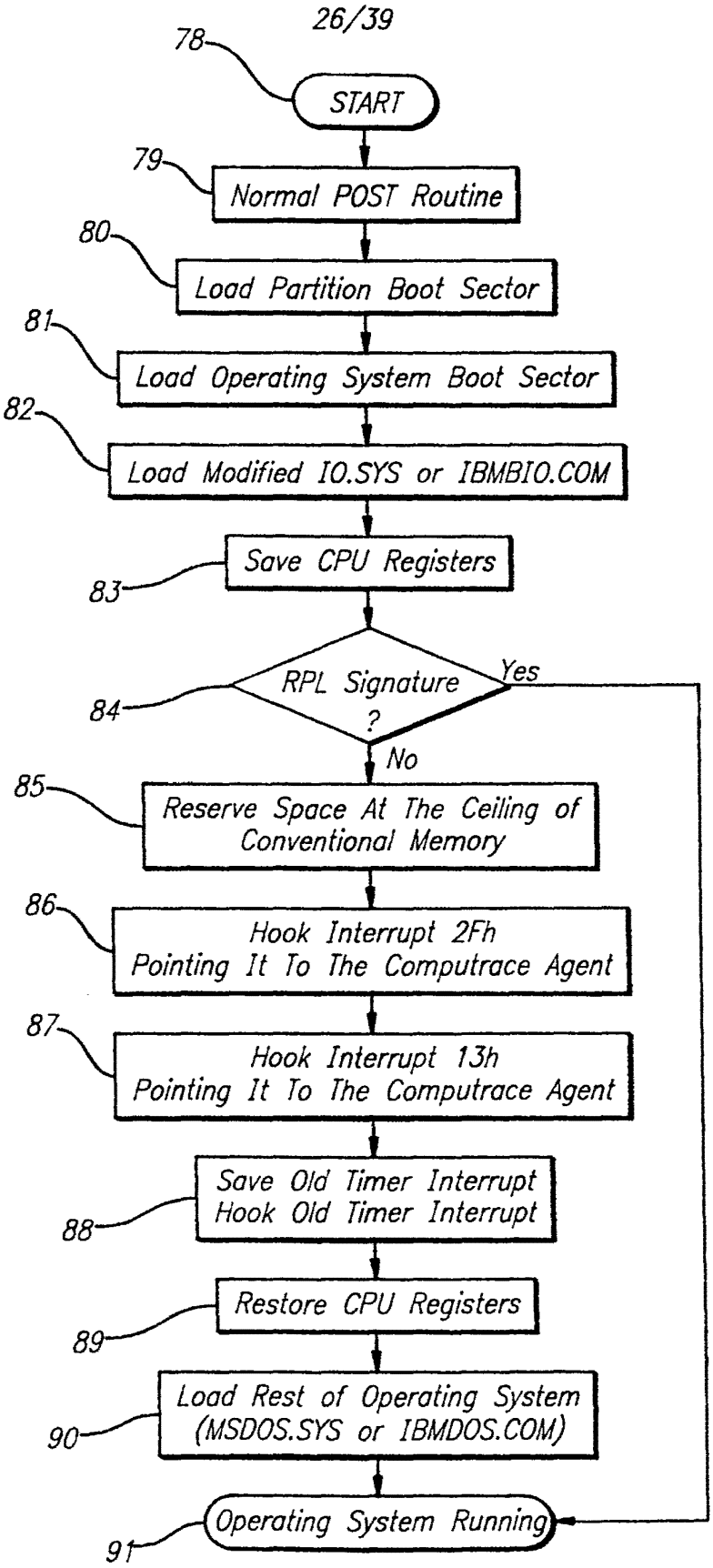


FIG. 14B

DELL EXHIBIT 1002
Page 269 of 659

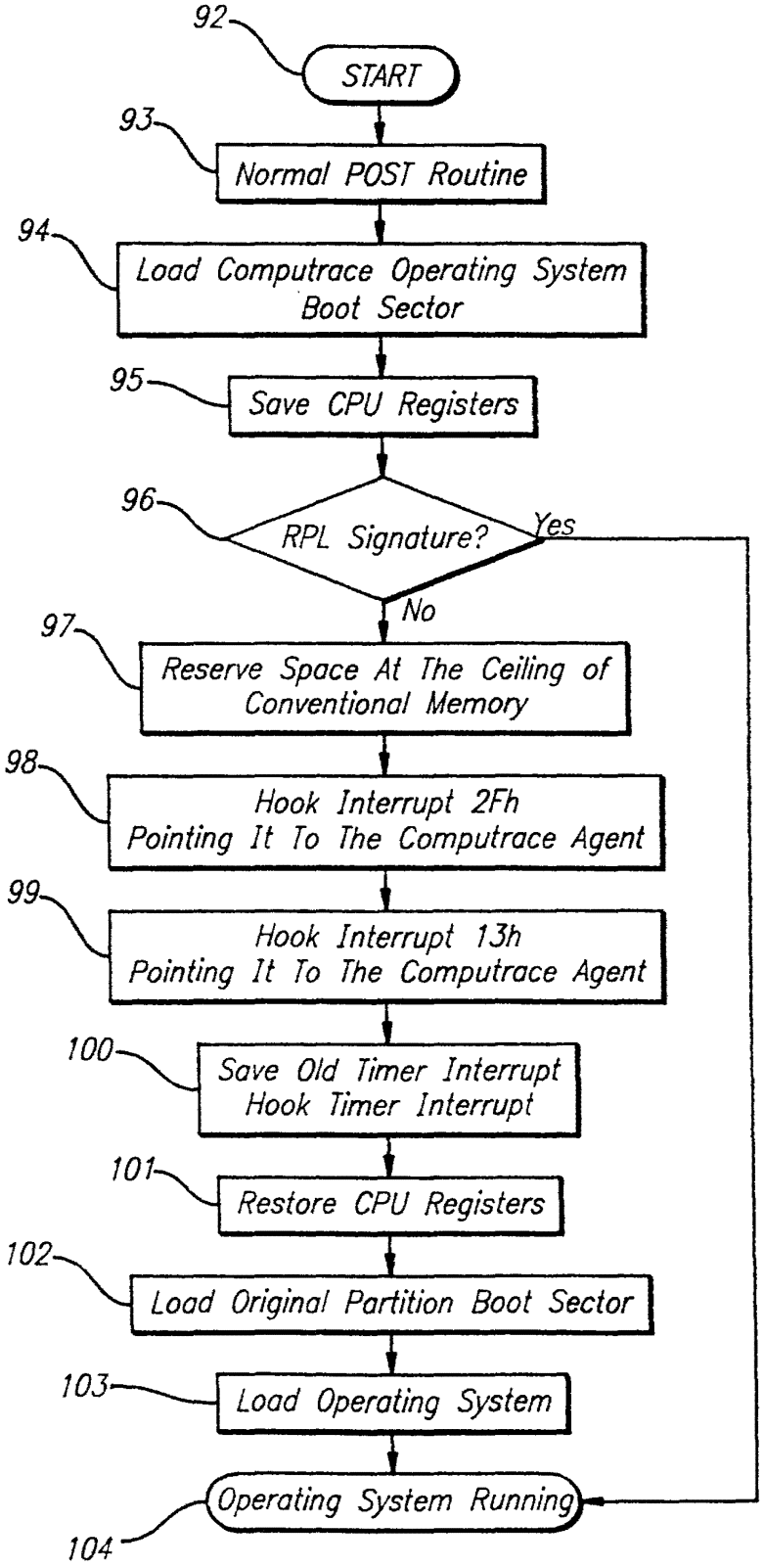

92
START
93
Normal POST Routine
94
Load Computrace Operating System Boot Sector
95
Save CPU Registers
96
RPL Signature?
Yes
No
97
Reserve Space At The Ceiling of Conventional Memory
98
Hook Interrupt 2Fh Pointing It To The Computrace Agent
99
Hook Interrupt 13h Pointing It To The Computrace Agent
100
Save Old Timer Interrupt Hook Timer Interrupt
101
Restore CPU Registers
102
Load Original Partition Boot Sector
103
Load Operating System
Operating System Running
104

FIG. 14C

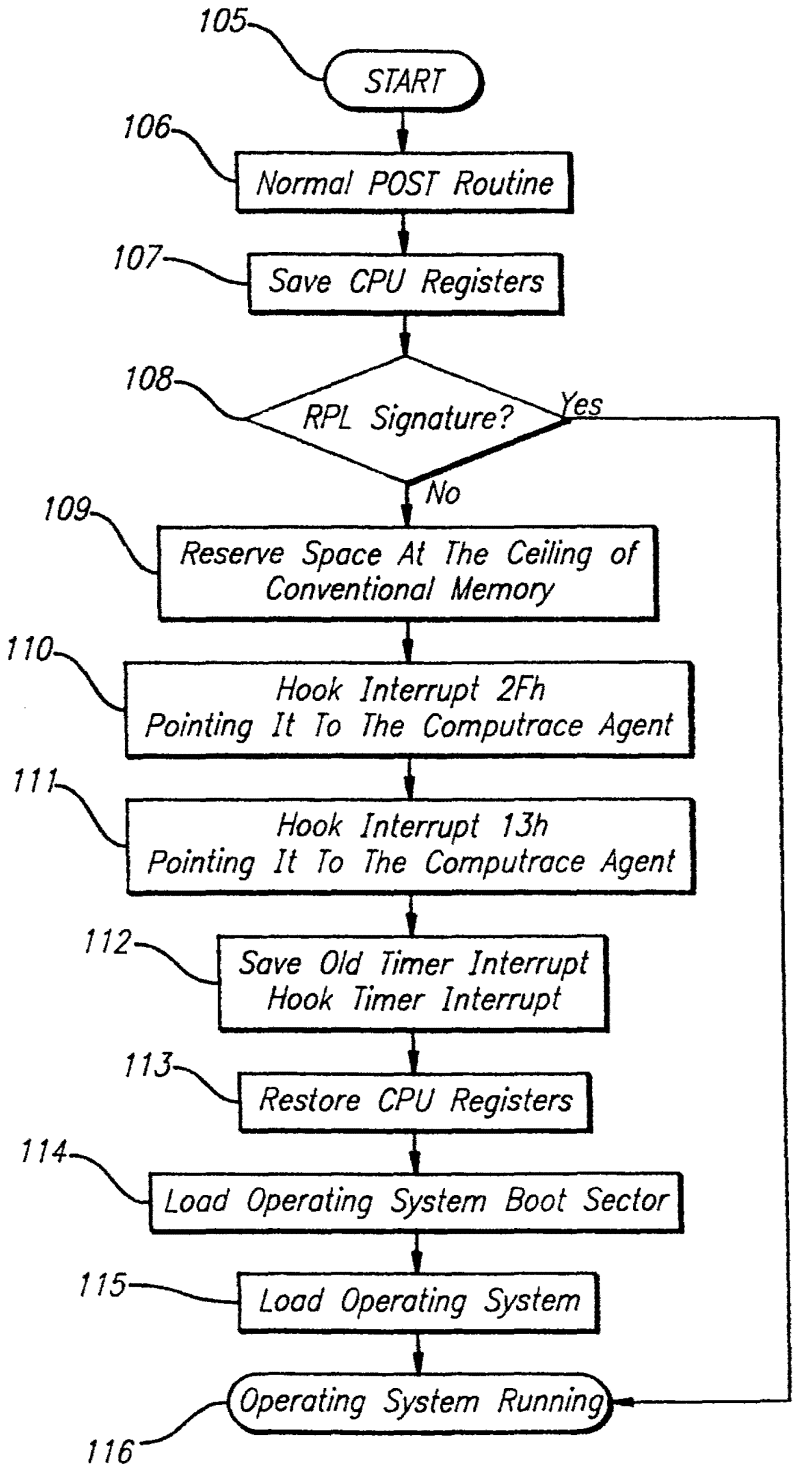

105
START
106
Normal POST Routine
107
Save CPU Registers
108
RPL Signature?
Yes
No
109
Reserve Space At The Ceiling of Conventional Memory
110
Hook Interrupt 2Fh Pointing It To The Computrace Agent
111
Hook Interrupt 13h Pointing It To The Computrace Agent
112
Save Old Timer Interrupt Hook Timer Interrupt
113
Restore CPU Registers
114
Load Operating System Boot Sector
115
Load Operating System
Operating System Running
116

FIG. 14D

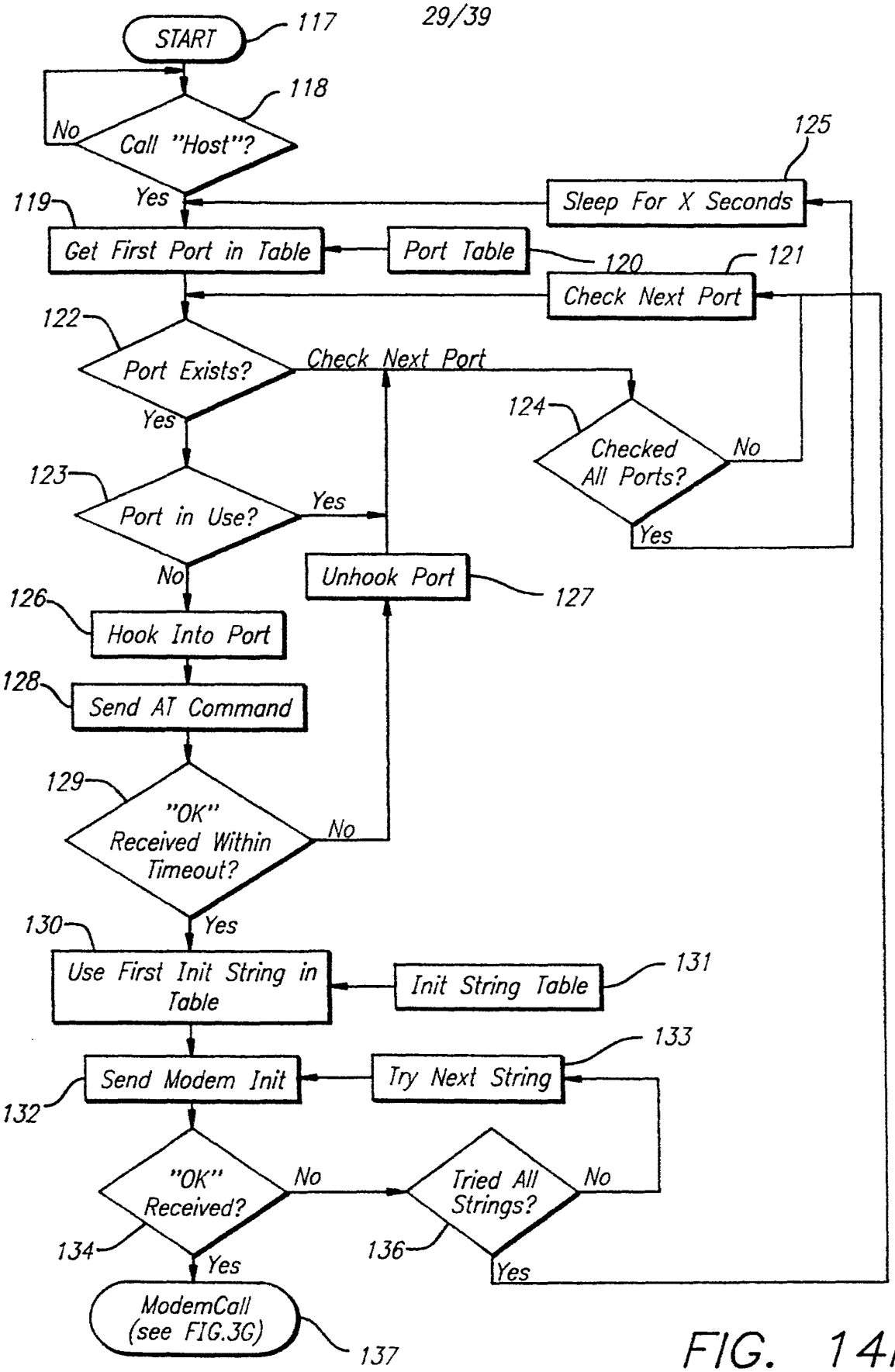


FIG. 14F

DELL EXHIBIT 1002
Page 272 of 659

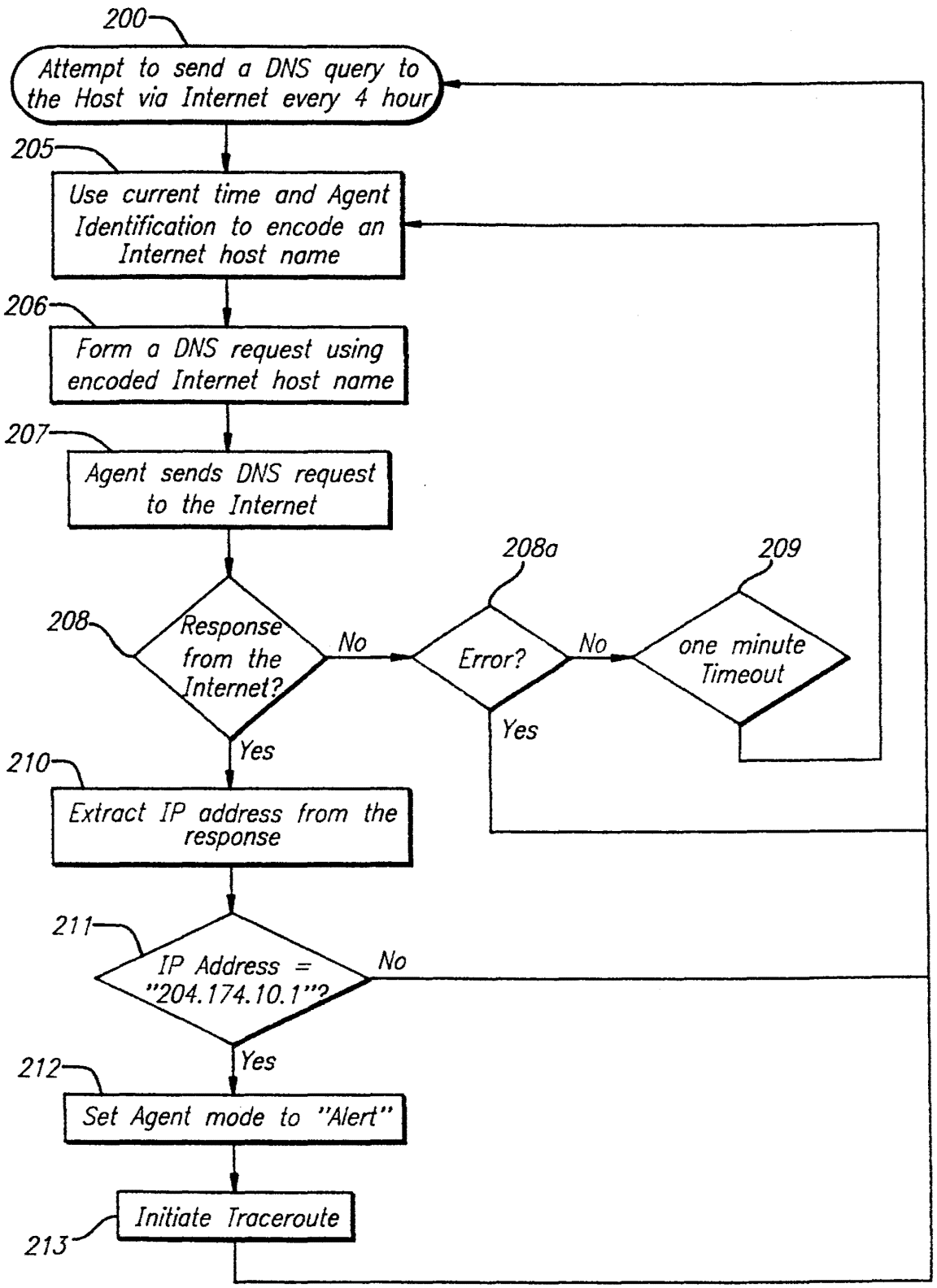

200
Attempt to send a DNS query to the Host via Internet every 4 hour
205
Use current time and Agent Identification to encode an Internet host name
206
Form a DNS request using encoded Internet host name
207
Agent sends DNS request to the Internet
208
Response from the Internet?
No
208a
Error?
No
209
one minute Timeout
Yes
Yes
210
Extract IP address from the response
211
IP Address = "204.174.10.1"?
No
Yes
212
Set Agent mode to "Alert"
213
Initiate Traceroute

FIG. 14F-1

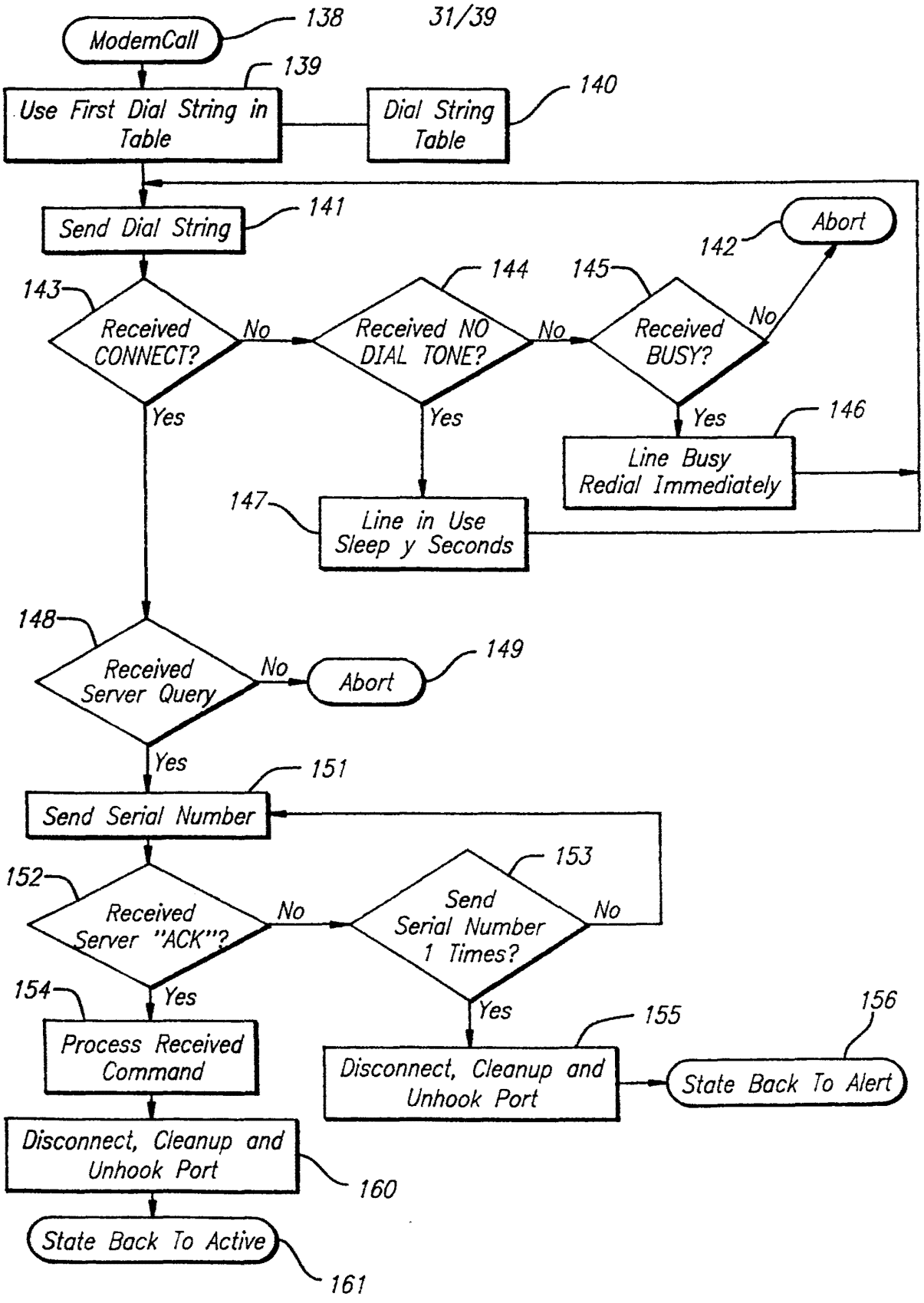


FIG. 14G

DELL EXHIBIT 1002
Page 274 of 659

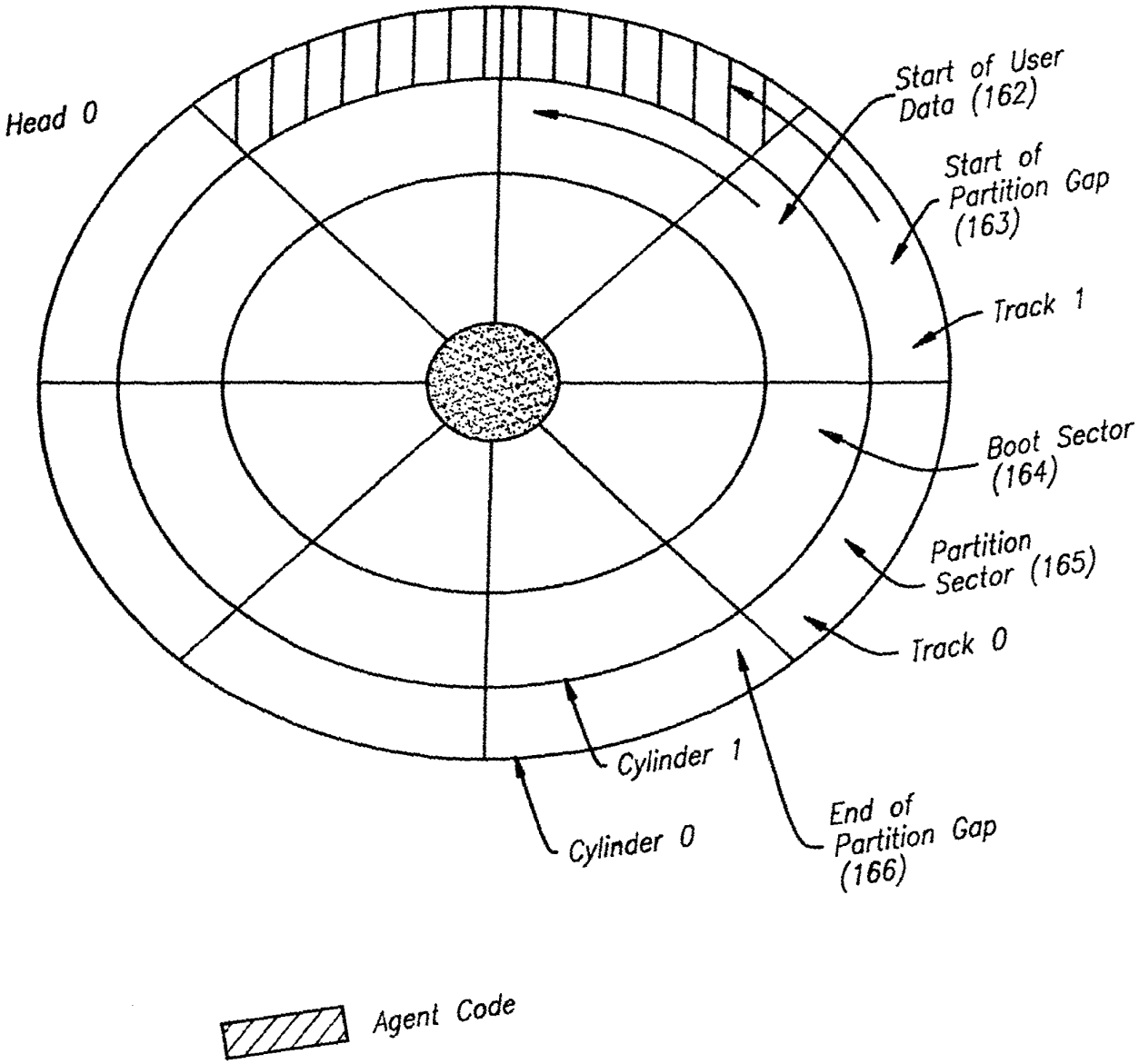

Head 0
Start of User Data (162)
Start of Partition Gap (163)
Track 1
Boot Sector (164)
Partition Sector (165)
Track 0
Cylinder 1
Cylinder 0
End of Partition Gap (166)
Agent Code

FIG. 14H

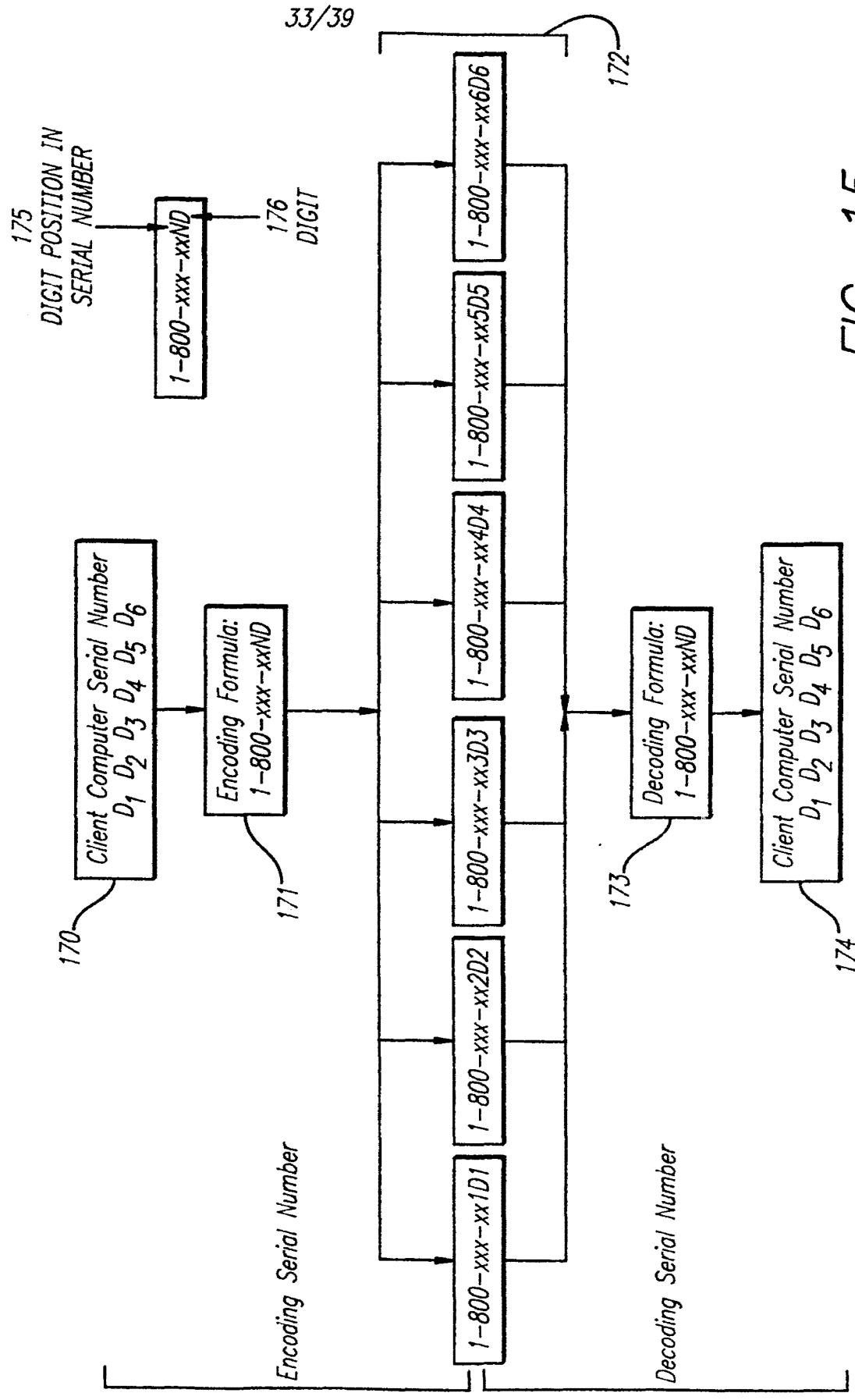


FIG. 15

DELL EXHIBIT 1002
Page 276 of 659

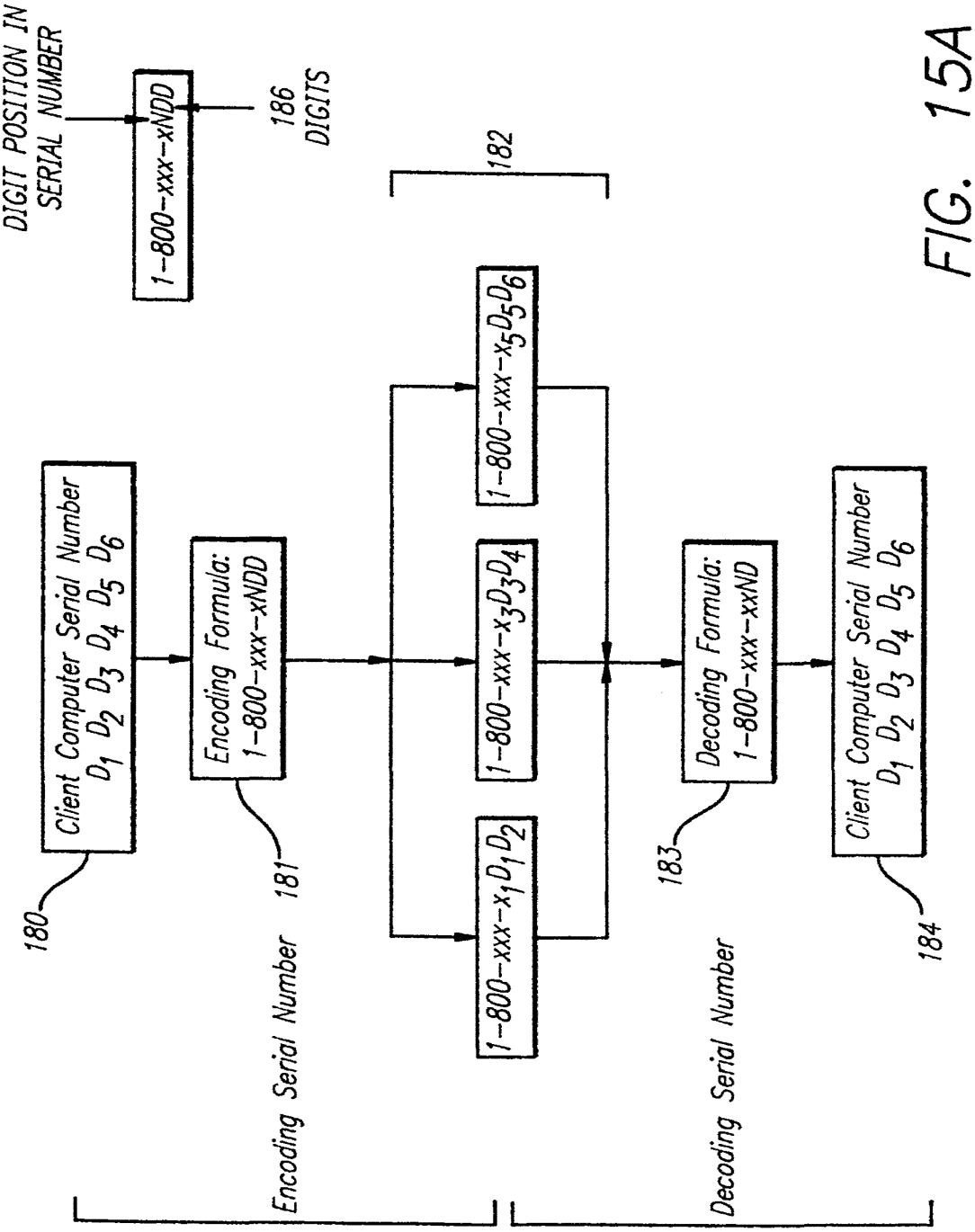


FIG. 15A

DELL EXHIBIT 1002
Page 277 of 659

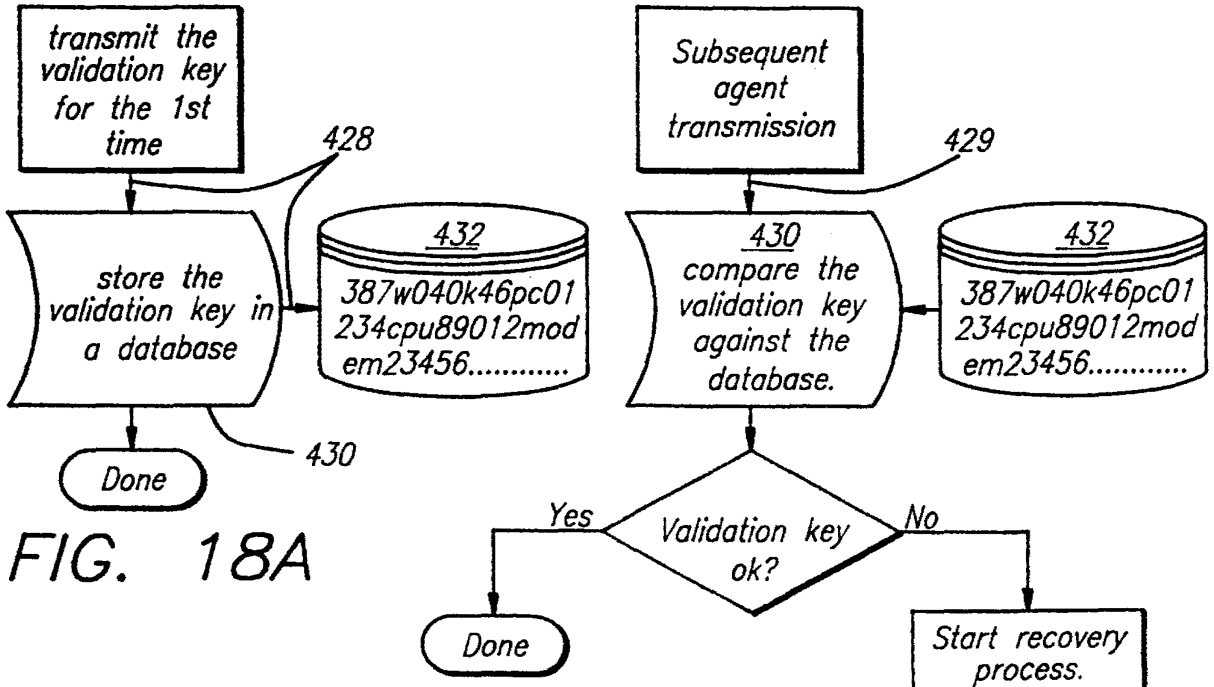
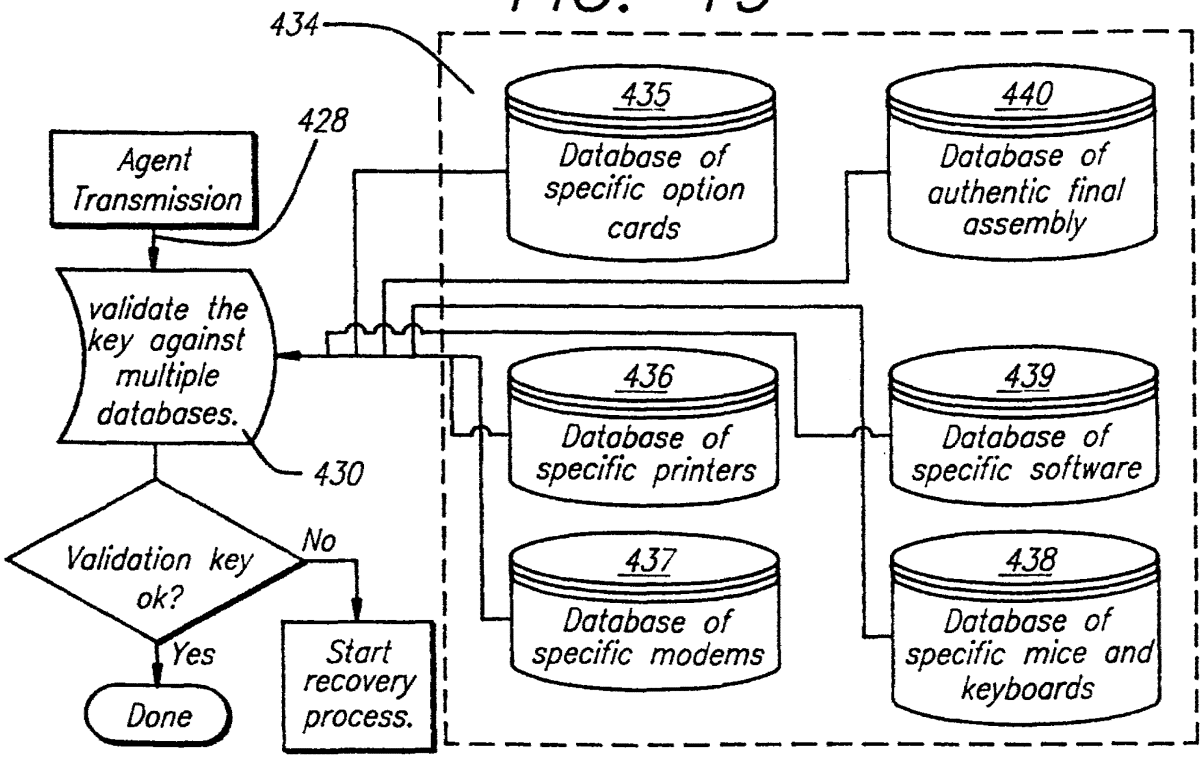


FIG. 18A

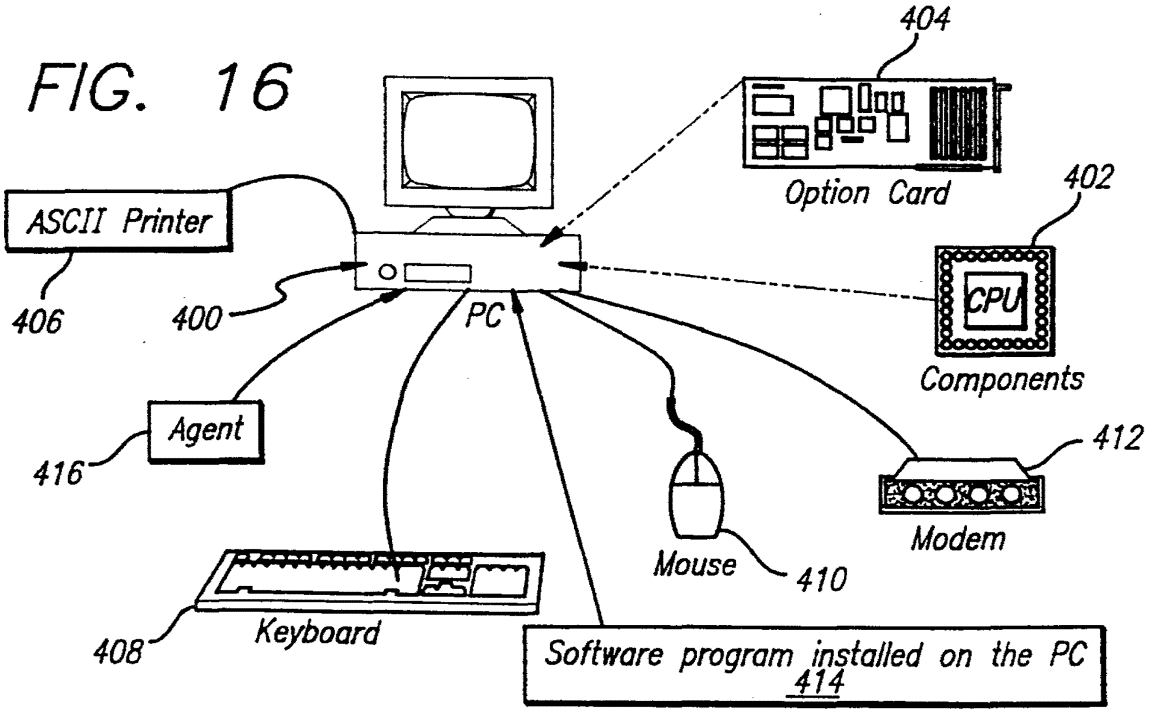
FIG. 18B

FIG. 19



DELL EXHIBIT 1002
Page 278 of 659

FIG. 16



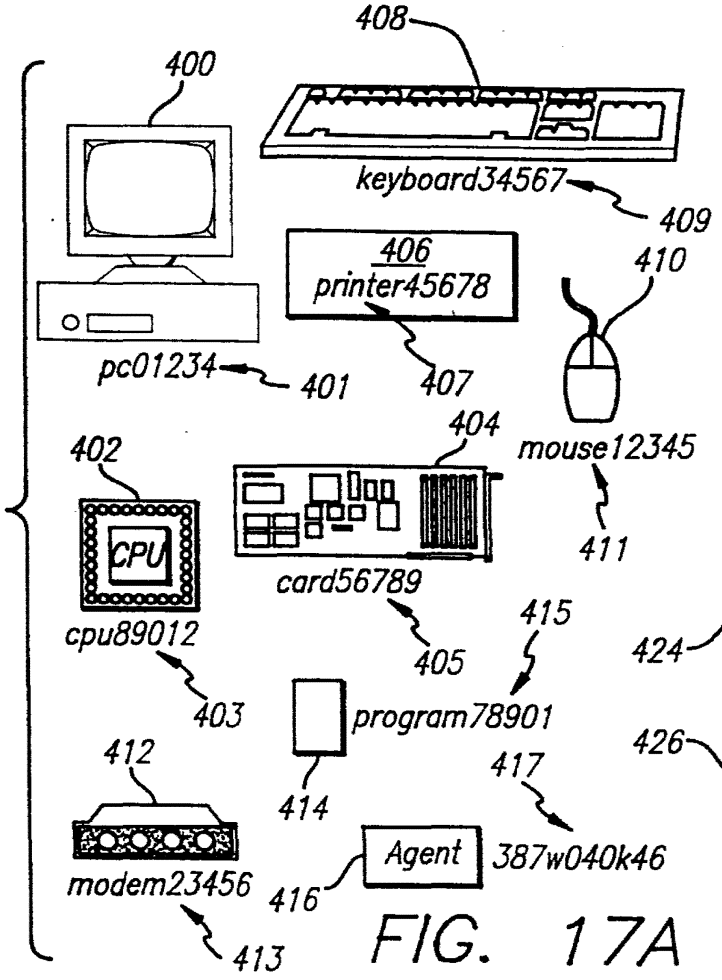


FIG. 17A

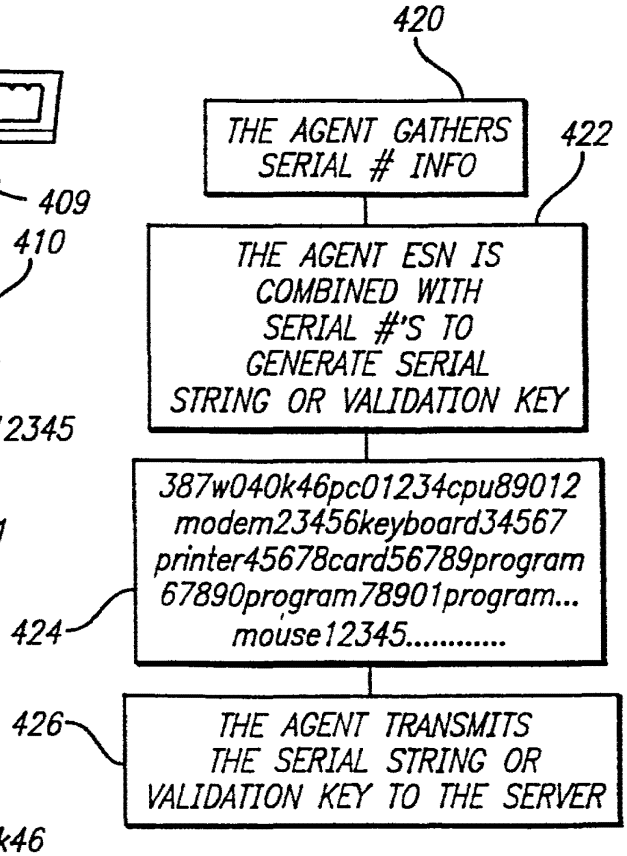


FIG. 17B

DELL EXHIBIT 1002
Page 279 of 659

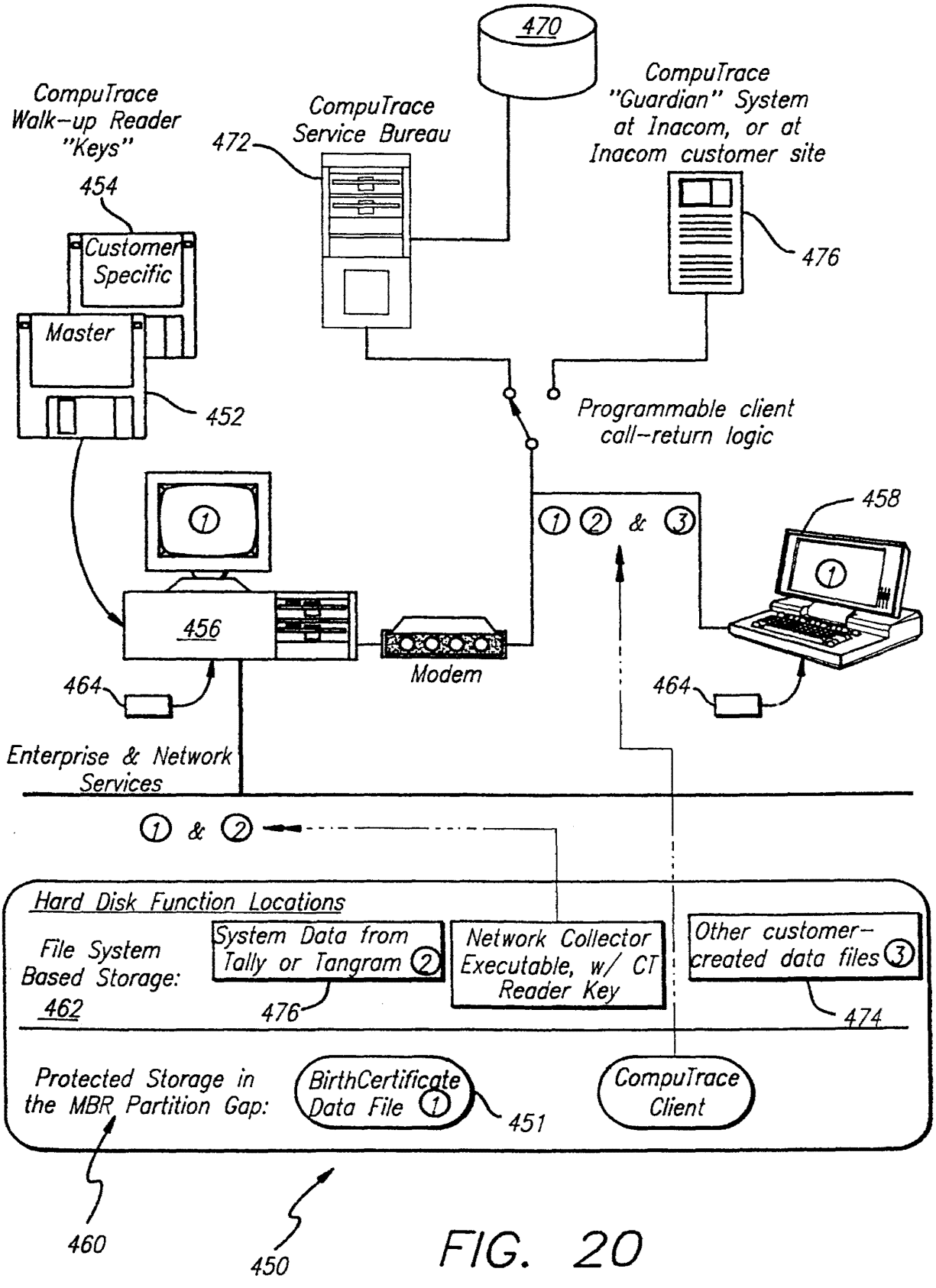


FIG. 20

DELL EXHIBIT 1002
Page 280 of 659

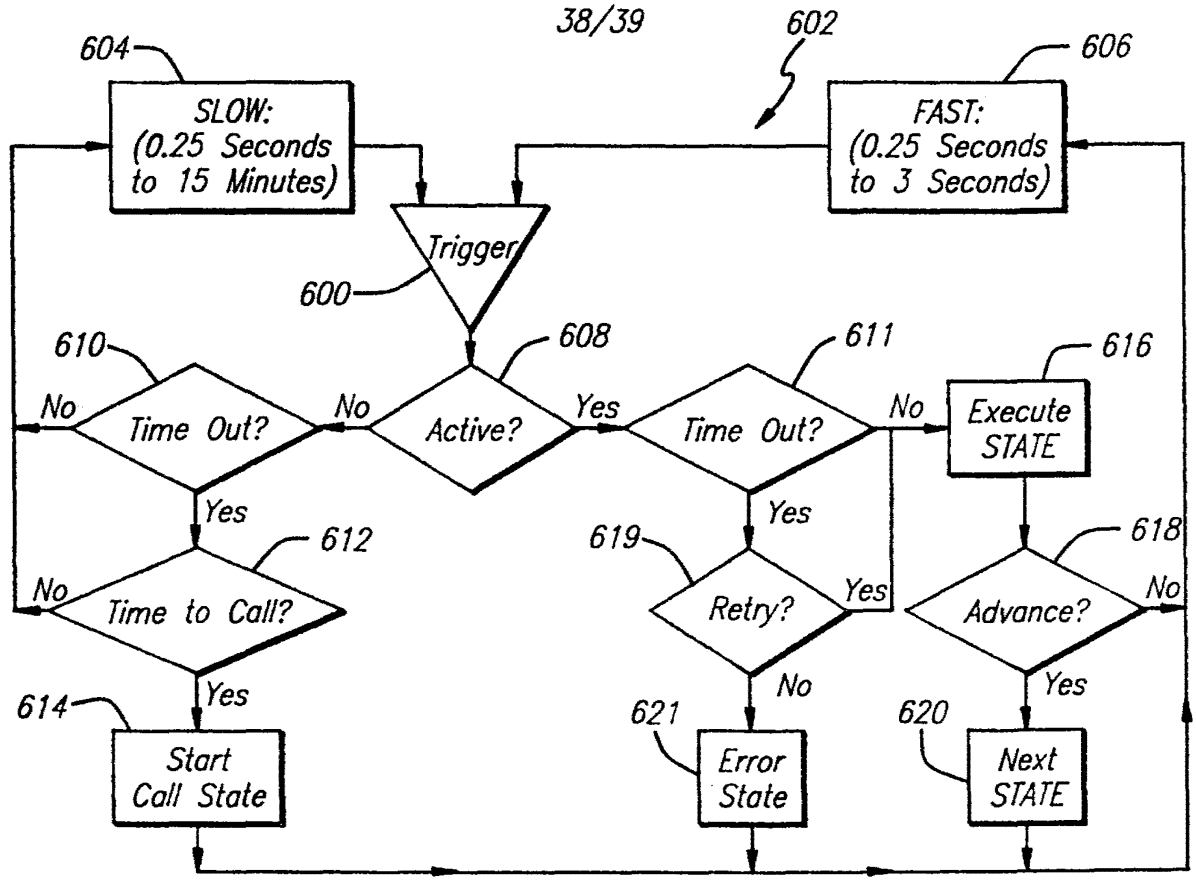


FIG. 21

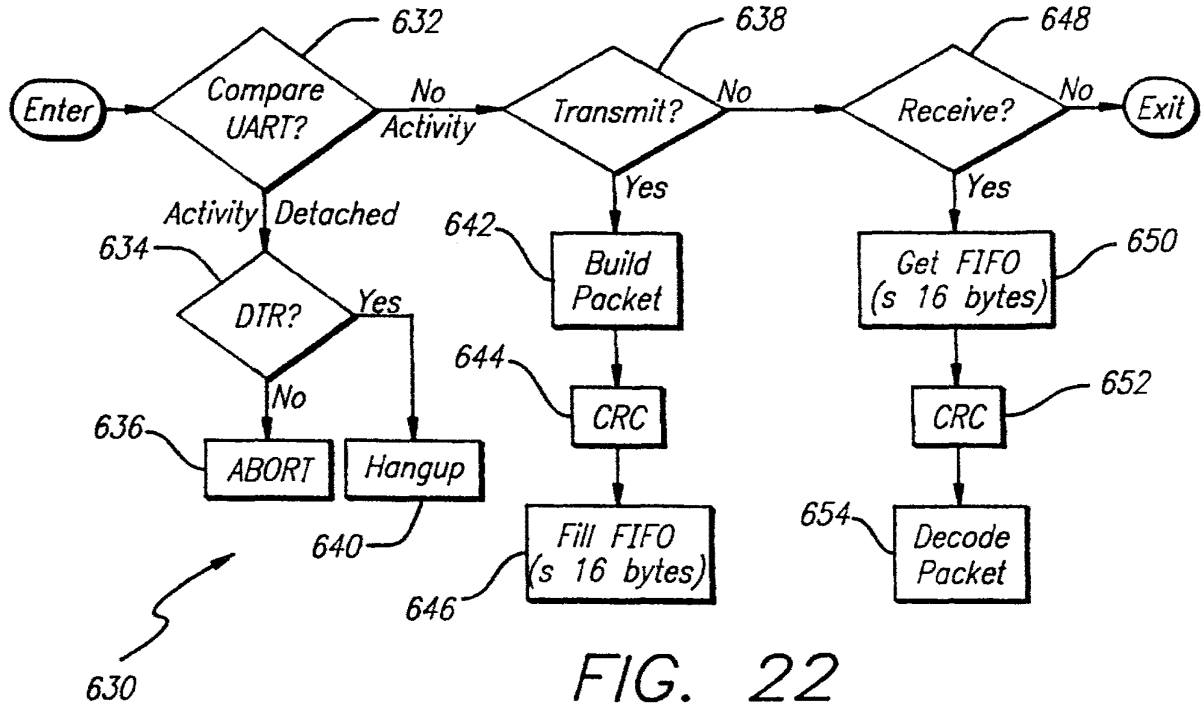


FIG. 22

DELL EXHIBIT 1002
Page 281 of 659

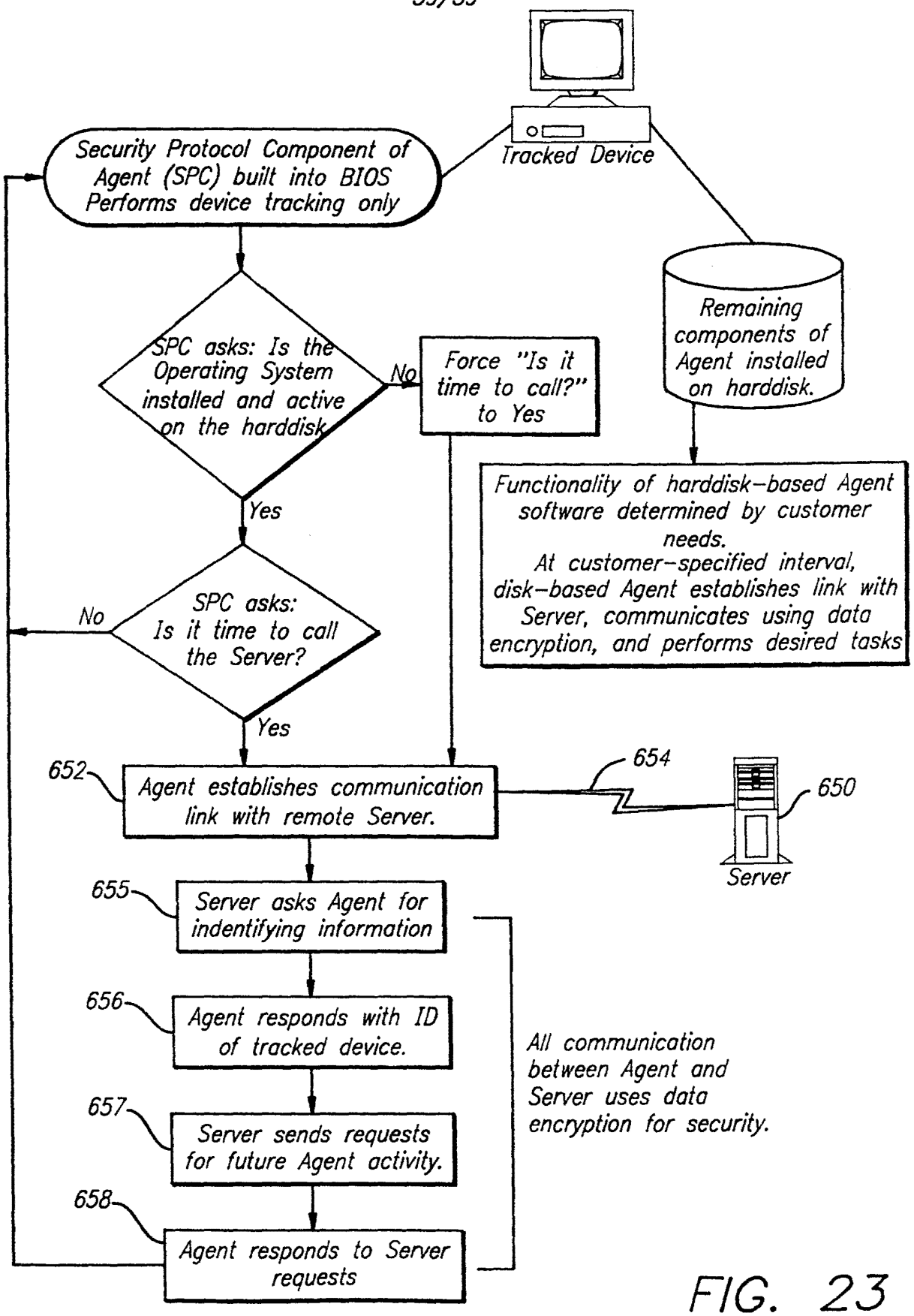


FIG. 23

DELL EXHIBIT 1002
Page 282 of 659

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT, CA 98/00278

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 96 15485 A (ABSOLUTE SOFTWARE CORP) 23 May 1996 see page 2, line 14 - page 3, line 20; claims	1
X	WO 96 03728 A (KANG BALJIT SINGH) 8 February 1996 see page 2, line 1 - line 15 see page 3, line 24 - page 4, line 25 see page 6, line 11 - page 7, line 8	1
Y	US 4 999 621 A (LOEB) 12 March 1991 see the whole document	1
Y	EP 0 588 519 A (AMERICAN TELEPHONE AND TELEGRAPH COMPANY) 23 March 1994 see column 2, line 42 - column 3, line 40	1

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
3 June 1998	10/06/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Durand, J

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

ormation on patent family members

Inter nal Application No
PCT/CA 98/00278

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9615485 A	23-05-1996	US 5715174 A	03-02-1998
		AU 3837595 A	06-06-1996
		EP 0793823 A	10-09-1997
WO 9603728 A	08-02-1996	AU 2986495 A	22-02-1996
		GB 2304443 A	19-03-1997
US 4999621 A	12-03-1991	NONE	
EP 588519 A	23-03-1994	US 5311596 A	10-05-1994
		CA 2104849 A	01-03-1994
		JP 6204998 A	22-07-1994

PTO/SB/21 (04-07)
Approved for use through 09/30/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	11/484100
Filing Date	07-11-2006
First Named Inventor	Apurva M. Bhansali
Art Unit	2134
Examiner Name	Zand, Kambiz
Total Number of Pages in This Submission: 121	Attorney Docket Number: SOFP:115US

ENCLOSURES (*Check all that apply*)

- ☐ Fee Transmittal Form
  - ☐ Fee Attached
- ☐ Amendment/Reply
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☑ Information Disclosure Statement
- ☐ Certified Copy of Priority Document(s)
- ☐ Reply to Missing Parts/ Incomplete Application
  - ☐ Reply to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
  - ☐ Landscape Table on CD
- ☐ After Allowance Communication to TC
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- ☐ Proprietary Information
- ☐ Status Letter
- ☐ Other Enclosure(s) (please Identify below):

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	Chowdhury & Georgakis, P.C.		
Signature	/Charles C. Claunch/		
Printed name	Charles C. Claunch		
Date	07-09-2007	Reg. No.	51,221

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature	/Charles C. Claunch/		
Typed or printed name	Charles C. Claunch	Date	07-09-2007

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of:		Docket No.: SOFP:115US
	Apurva M. Bhansali et al.	Art Unit: 2134
Serial No:	11/484,100	Examiner: Zand, Kambiz
Filed:	July 11, 2006	Conf. No.: 7749
For:	Electronic Device Security and Tracking System and Method	

PRELIMINARY AMENDMENT

Dear Sir:

Please amend the above referenced application as follows.

Amendments to the Specification begin on page 2 of this paper.

Amendments to the Claims are reflected in the listing of claims which begins on page 9 of this paper.

Remarks are on page 18 of this paper.

Amendments to the Specification:

Please replace paragraph [0005] with the following amended paragraph:

[0005] The ESTSM system may include an electronic device with three components and a server computer system. The three components may be an application component, a non-viewable component and a Basic Input/Output System (BIOS) component. In some embodiments of the invention, the application component includes ESTSM application software that executes under any Windows® operating system (OS). In other embodiments of the invention, the application component software may execute under the Disk Operating System (DOS), Linux operating system, Windows® CE (and its derivatives such as Windows® Mobile, ~~SmartPhone~~ Smart Phone, Pocket PC, and so on), Symbian and Palm operating system and others. In some embodiments of the invention, the application component is responsible for communicating over the Internet with the ESTSM server computer system to determine if the electronic device has been reported stolen. If the device has been reported stolen, the application component along with the ESTSM server computer system will determine what services the user has registered for and will take the appropriate action (e.g. disable the device, communicate identifying information to the server, erase the storage device, recover data, encrypt data, etc).

Please replace paragraph [0023] with the following amended paragraph:

[0023] In ~~the preferred embodiment~~ some embodiments of the invention, most of ESTSM services are based on a yearly fee model. Some services such as data recovery may be billed on a per megabyte basis-that is, the user indicates the number of megabytes to be recovered during registration and is billed accordingly. However, if the electronic device is stolen and during data recovery more megabytes are recovered, then a one time fee is charged to the user. The user will automatically be billed at the end of the year to renew the service for one more year. The user will be sent an email before billing to give the user a chance to cancel the service if they wish.

Please replace paragraph [0031] with the following amended paragraph:

[0031] In some other embodiments of the invention, mobile devices such as cell phones, Smart Phones, and Wireless Local Area Network (WLAN) capable computers that may be always connected to the ESTSM server and contacted at anytime by the server can communicate through a message passing scheme. Message passing schemes may be SMS, WWW message passing protocol based on Transmission Control Protocol/Internet Protocol (TCP/IP), or Multimedia Messaging Service (MMS). The state diagram for mobile devices ~~are~~ is shown in Figure 72.

Please replace paragraph [0034] with the following amended paragraph:

[0034] In another embodiment of the invention, ESTSM registration as shown in Figure 10 for a PDA, mobile cellular telephone, or Smart Phone device may be performed using another computer system that can display ESTSM registration web pages. In some embodiments of the invention, a different set of ESTSM services as shown in Figure 11 may be offered for the PDA. Thus, the manufacturer may offer, but not be limited to, a Basic service and a Data backup service for the device ~~as~~ is shown in Figure 11.

Please replace paragraph [0065] with the following amended paragraph:

[0065] In some embodiments of the invention, the BIOS component 4410 consists of a BIOS ROM image that is integrated into the system BIOS. The non-viewable component 4415 consists of a VALIDATOR program 4450 which resides in a special hidden partition 4455 created by ESTSM. Together, the ROM image and VALIDATOR cooperate to make sure that someone cannot bypass or circumvent the ESTSM application component 4405 from running. This is done by the ESTSM BIOS in the three ways shown below. In this document, reference made to "ESTSM BIOS" may refer to the code in the BIOS ROM image or VALIDATOR or combination of both.

1. Validating the integrity of the ESTSM special hidden partition 4455 and VALIDATOR program 4450. The ESTSM hidden partition 4455 contains the VALIDATOR program 4450

and also contains a copy of the original application component fileset 4445. If the ESTSM hidden partition 4455 has been deleted from the electronic device's hard disk drive 4400 or in some other way altered, the ESTSM BIOS ROM image component will detect this and effectively force re-installation of the partition 4455 and original fileset 4445 from the recovery media 4460. This prevents someone from simply low level formatting the hard disk drive, or just replacing the hard disk drive with a new blank disk to bypass ESTSM. The ESTSM VALIDATOR program 4450 can then "re-install" the ESTSM application component 4405 from the ESTSM Backup (Original) fileset 4445 on the special hidden ESTSM partition 4455 of the hard disk drive 4400.

2. Verifying that the application has been run on each boot. The ESTSM BIOS implements a messaging protocol with the ESTSM application components 4405 to ensure that the ESTSM application components 4405 are run on every boot. This messaging protocol utilizes the ESTSM Communications Area (ECA) 4440. In order to bypass ESTSM, someone may delete key ESTSM application files in an attempt to prevent the ESTSM application from running. Furthermore, the thief may develop applications that will prevent ESTSM from running on every boot even though it is correctly installed on the electronic device's hard disk drive. The ESTSM application and BIOS components work together to make sure that the ESTSM application runs on every boot. If the ESTSM application component does not run after the electronic device has booted, the ESTSM system will allow the electronic device to boot a limited number of times and attempt to run the ESTSM application component. If the ESTSM application component does not run during any of these retries, the electronic device will be prevented from booting after system POST. For devices like PDA or ~~SmartPhones~~ Smart Phones this procedure is not required since the application component is not removable or replaceable.
3. Disabling a stolen electronic device reported as stolen so it may not boot the operating system. If the ESTSM application component 4405 detects that the electronic device has been reported stolen, it will inform the BIOS of the theft and freeze the system. If the thief powers off the electronic device and attempts to boot the system again, the ESTSM BIOS will prevent the system from booting the operating system. If the electronic device is recovered and returned to the original user, the user can "unlock" the device as described above so it can boot.

Please replace paragraph [0066] with the following amended paragraph:

[0066] In another embodiment of the invention as shown in Figure 45, the architecture for an ESTSM enabled PDA, WLAN capable computer, mobile phone that in some embodiments may be a cell phone, or ~~SmartPhone~~ Smart Phone may include a Flash memory 4500 containing a changeable area 4510 and a system area 4520. The system area 4520 may include application components 4530 containing ESTSM application programs and a secure non-volatile area 4540 coupled to the application components 4530. In one embodiment of the invention, the system area 4520 may be non-viewable and implemented in non-volatile memory. The ESTSM enabled PDA, WLAN capable computer, mobile phone, or ~~SmartPhone~~ Smart Phone may continuously communicate to an ESTSM Server Computer System 4560 through an always-on Internet connection 4550 or other mobile device communication protocols such as Short Messaging Service (SMS). Server computer system 4560 includes a number of servers 4570a, 4570b, ... 4570n that may be web servers containing the web pages and data for ESTSM described above.

Please replace paragraph [0079] with the following amended paragraph:

[0079] Turning now to Figure 50, a wireless communication device that may be a PDA, WLAN capable computer, mobile phone that in some embodiments is a cell phone, or ~~SmartPhone~~ Smart Phone includes a changeable area and an application component in a system area in accordance with the embodiment of the invention of Figure 45. The wireless communication device 5000 may transmit and receive information with a plurality of base transceiver stations (BTS) not shown in Figure 50. Each BTS may transmit in a forward or downlink direction both physical and logical channels to the mobile station 5000 in accordance with a predetermined air interface standard. A reverse or uplink communication path also exists from the mobile station 5000 to the BTS, which conveys mobile originated access requests and traffic.

Please replace paragraph [0084] with the following amended paragraph:

[0084] As mentioned above with reference to Figure 45, the ESTSM enabled PDA, mobile phone, WLAN capable computer, or ~~SmartPhone~~ Smart Phone may continuously communicate to the ESTSM Server Computer System through an always-on Internet connection. Information such as telephone numbers, email addresses, calendar appointments, sales meetings and other daily reminders on a PDA, mobile phone, WLAN capable computer, or ~~SmartPhone~~ Smart Phone with ESTSM can be retrieved from a stolen device in one embodiment of the invention by the user calling an ESTSM service center to report the device as stolen. Because the PDA, mobile phone, WLAN capable computer, or ~~SmartPhone~~ Smart Phone has an always-on Internet connection, data on the device can be recovered and stored on the ESTSM server computer system as soon as the device is reported stolen. After recovery, the data may be erased off the stolen PDA, mobile phone, WLAN capable computer, or ~~SmartPhone~~ Smart Phone and the device disabled, making it worthless for the thief. Upon the ESTSM user purchasing a replacement PDA, mobile phone, WLAN capable computer, or ~~SmartPhone~~ Smart Phone, the data recovered and stored on the ESTSM server computer system from the user's stolen device can be placed on the user's new replacement device.

Please replace paragraph [0103] with the following amended paragraph:

[0103] Referring now to Figure 58, a flow diagram implemented in the client and server for encoding binary format sequence data into ASCII text format data in accordance with some embodiments of the invention is shown. If the end of the binary format sequence data source 5810 has been reached as determined by the value of the source_length variable then encoding ends 5815. If the end has not been reached, then the next byte to encode is stored 5820 in a variable. Thus, 'n' bits from the variable are extracted 5820 into another variable that in one embodiment may be C1. ASCII text format may have n=6 bits with the highest order 7th and 8th bit being zero. Variable C1 is passed to ENC( ) function that performs binary mapping operations on the binary sequence data to generate an encoded byte 5830. In some embodiments of the invention, the binary mapping operations on C1 ~~includes~~ include mapping C1 to a base 64 number. The encoded byte is placed into a Destination data structure 5840 that may be an array

of bytes for transmission over communication medium 5625. The encoded byte is re-initialized to a zero value in one embodiment of the invention and the source_length variable is decremented.

Please replace paragraph [0104] with the following amended paragraph:

[0104] Referring now to Figure 59, a flow diagram implemented in the client and server for decoding ASCII text format data into binary data in accordance with some embodiments of the invention is shown. Encryption/decryption modules located in the client electronic device or server computer system receive encoded bytes of ASCII text format data that are placed into a source byte stream data structure that may be an array of bytes. The source byte stream data structure is described by a source_length variable that indicates the number of ASCII text format data bytes present in the array. Every time a new byte of data is received by the encryption/decryption module and placed in the array, the source_length variable is incremented and when a byte of data is removed and decoded the source_length variable is decremented. If the end of source 5910 has been reached, the array will become empty and decoding will end 5930. If the end of the source has not been reached, ~~then,~~ then a current ASCII text format byte of data is placed into variable E. The ASCII text format byte of data in variable E is passed to DECODE( ) function that performs mapping operations on the data to generate a decoded byte ED 5950. The lower six bits of the decoded byte ED are placed into a final byte stream data structure 5960 and the upper two bits are discarded. Finally, the source_length variable is decremented as described above. If the end of the source byte stream is reached, every eight bits in the final byte stream 5920 corresponds to the original unencoded data.

Please replace paragraph [0116] with the following amended paragraph:

[0116] Figures 65-70 show screen shots, in accordance with some embodiments of the invention, for registering and using ESTSM in the PDA or mobile phone shown in Figures 45 and 50. ESTSM registration as shown in Figure 65 for a mobile device may be performed using a computer system that can display ESTSM registration web pages. In some other embodiments of the invention, the ESTSM registration pages may be displayed on the mobile device capable

of displaying web pages. Figure 65 shows a service selection screen that may include the cost of each service and the services offered. The services offered and the cost of each service may vary based on the manufacturer and model of the mobile device, the market segment of the mobile device (i.e. business device, home use device) and what the manufacturer has chosen to include for the device. Some manufacturers may want to change the pricing of the services, or offer bundled services to the user. For one embodiment of the invention, as shown below, is a list of the services available to the user.

1. Basic Service – with this service the user has the ability to have the mobile device disabled if it is stolen or lost. The information on the mobile device is made secure so that it cannot be accessed by someone who steals the mobile device or finds the device.
2. Data Recovery Service – this service will recover Contacts, Calendar, and other data such as pictures form the mobile device if the device is stolen or lost. ESTSM may recover this information to the ESTSM server computer system, before performing other service option actions. The user may then restore the data into a new cell phone, ~~SmartPhone~~ Smart Phone or PDA device that they purchase.

Please replace paragraph [0123] with the following amended paragraph:

[0123] In some embodiments of the invention, once the report is completed, the electronic device will be placed into the REPORTED STOLEN state. At this point, because of the always on connection of the mobile device to the Internet, in some embodiments the mobile device files are backed up and the device state will change to RECOVERED state as shown in Figure 69. The user may then manage these files to move them into a new cell phone, ~~SmartPhone~~ Smart Phone or PDA device that they purchase. After the data has been recovered, the ESTSM system informs the user that the mobile device is disabled as shown in Figure 70.

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) An electronic device security and tracking system, comprising:

a nonvolatile storage device;

a changeable area in the nonvolatile storage device, wherein the changeable area further comprises an application component and a secure area coupled to the application component; ~~and,~~ and

a server system capable of communicating through a secure medium with the application component.

2. (Original) The electronic device security and tracking system of claim 1, wherein the server system is capable of communicating through the secure medium with the secure area.

3. (Original) The electronic device security and tracking system of claim 1, wherein the electronic device is a personal digital assistant.

4. (Original) The electronic device security and tracking system of claim 1, wherein the nonvolatile storage device is a Flash memory.

5. (Original) The electronic device security and tracking system of claim 1, wherein the application component comprises an application file.

DELL EXHIBIT 1002
Page 294 of 659

6. (Original) An electronic device security and tracking system, comprising:

a nonvolatile storage device;

a changeable area in the nonvolatile storage device, wherein the changeable area further comprises a system area in the nonvolatile storage device, said system area comprising an application component and a secure area coupled to the application component; and

a server system capable of communicating through a secure medium with the application component.

7. (Original) The electronic device security and tracking system of claim 6, wherein the server system is capable of communicating through the secure medium with the secure area.

8. (Original) The electronic device security and tracking system of claim 7, wherein the system area is not modifiable by a user of the electronic device.

9. (Original) The electronic device security and tracking system of claim 6, wherein the electronic device is a personal digital assistant.

10. (Original) The electronic device security and tracking system of claim 6, wherein the nonvolatile storage device is a Flash memory.

11. (Original) The electronic device security and tracking system of claim 6, wherein the application component comprises an application file.

12. (Currently Amended) An electronic device security and tracking system, comprising:

a nonvolatile storage device;

a changeable area in the nonvolatile storage device, wherein the changeable area further comprises an application component and a communication protocol component coupled to the application component; ~~and,~~ and

one or more servers capable of communicating through a secure medium with the application component.

13. (Original) The electronic device security and tracking system of claim 12, wherein the communication protocol component is a smart messaging service component for mobile devices.

14. (Currently Amended) The electronic device security and tracking system of claim 13, further comprising:

one or more smart messaging service servers capable of communicating through a communications medium with the smart messaging service component; ~~and,~~ and

wherein the one or more servers that communicate with the application component are web servers.

15. (Original) The electronic device security and tracking system of claim 14, wherein the communications medium is from the group consisting essentially of smart messaging service wireless link, Code Division Multiple Access, and Global Mobile System.

16. (Original) The electronic device security and tracking system of claim 13, wherein the electronic device is from the group consisting essentially of Smart phone, smart messaging service capable device, and mobile phone device.

17. (Original) The electronic device security and tracking system of claim 12, wherein the nonvolatile storage device is a Flash memory.

18. (Original) The electronic device security and tracking system of claim 12, wherein the application component comprises an application file.

19. (Currently Amended) An electronic device security and tracking system, comprising:

a nonvolatile storage device;

a changeable area in the nonvolatile storage device, wherein the changeable area further comprises a system area in the nonvolatile storage device, said system area comprising an application component and a communication protocol component coupled to the application component; ~~and,~~ and

one or more servers capable of communicating through a secure medium with the application component.

20. (Original) The electronic device security and tracking system of claim 19, wherein the communication protocol component is a smart messaging service component for mobile devices.

21. (Currently Amended) The electronic device security and tracking system of claim 20, further comprising:

one or more smart messaging service servers capable of communicating through a communications medium with the smart messaging service component; ~~and,~~ and

wherein the one or more servers that communicate with the application component are web servers.

22. (Original) The electronic device security and tracking system of claim 21, wherein the communications medium is from the group consisting essentially of smart messaging service wireless link, Code Division Multiple Access, and Global Mobile System.

23. (Original) The electronic device security and tracking system of claim 20, wherein the electronic device is from the group consisting essentially of Smart phone, smart messaging service capable device, and mobile phone device.

24. (Original) The electronic device security and tracking system of claim 19, wherein the nonvolatile storage device is a Flash memory.

25. (Original) The electronic device security and tracking system of claim 19, wherein the system area is not modifiable by a user of the electronic device.

26. (Original) The electronic device security and tracking system of claim 19, wherein the application component comprises an application file.

27. (Original) A communication system, comprising:

a communication device, comprising:

a controller unit;

a digital signal processor coupled to the controller unit;

a nonvolatile storage device coupled to the controller unit, comprising:

a changeable area, wherein the changeable area further comprises an application component and a secure area coupled to the application component; and

a server system capable of communicating through a secure medium with the application component.

28. (Original) The communication system of claim 27, wherein the server system is capable of communicating through the secure medium with the secure area.

29. (Original) The communication system of claim 27, wherein the communication device is a personal digital assistant.

30. (Original) The communication system of claim 27, wherein the nonvolatile storage device is a Flash memory.

31. (Original) The communication system of claim 27, wherein the application component comprises an application file.

32. (Original) A communication system, comprising:

a communication device, comprising:

a controller unit;

a digital signal processor coupled to the controller unit;

a nonvolatile storage device coupled to the controller unit, comprising:

a changeable area, wherein the changeable area further comprises a system area, said system area comprising an application component and a secure area coupled to the application component; and

a server system capable of communicating through a secure medium with the application component.

33. (Original) The communication system of claim 32, wherein the server system is capable of communicating through the secure medium with the secure area.

34. (Original) The communication system of claim 33, wherein the system area is not modifiable by a user of the communication device.

35. (Original) The communication system of claim 32, wherein the communication device is a personal digital assistant.

36. (Original) The communication system of claim 32, wherein the nonvolatile storage device is a Flash memory.

37. (Original) The communication system of claim 32, wherein the application component comprises an application file.

38. (Currently Amended) A communication system, comprising:

a communication device, comprising:

a controller unit;

a digital signal processor coupled to the controller unit;

a nonvolatile storage device coupled to the controller unit, comprising:

a changeable area, wherein the changeable area further comprises

an application component and a communication protocol component coupled to the application component; ~~and,~~ and

one or more servers capable of communicating through a secure medium with the application component.

39. (Original) The communication system of claim 38, wherein the communication protocol component is a smart messaging service component for mobile devices.

40. (Currently Amended) The communication system of claim 39, further comprising:

one or more smart messaging service servers capable of communicating through a communications medium with the smart messaging service component; ~~and,~~ and

wherein the one or more servers that communicate with the application component are web servers.

41. (Original) The communication system of claim 40, wherein the communications medium is from the group consisting essentially of smart messaging service wireless link, Code Division Multiple Access, and Global Mobile System.

42. (Original) The communication system of claim 39, wherein the communication device is from the group consisting essentially of Smart phone, smart messaging service capable device, and mobile phone device.

43. (Original) The communication system of claim 38, wherein the nonvolatile storage device is a Flash memory.

44. (Original) The communication system of claim 38, wherein the application component comprises an application file.

45. (Currently Amended) A communication system, comprising:

a communication device, comprising:

a controller unit;

a digital signal processor coupled to the controller unit;

a nonvolatile storage device coupled to the controller unit, comprising:

a changeable area, wherein the changeable area further comprises a system area in the nonvolatile storage device, said system area comprising an application component and a communication protocol component coupled to the application component; ~~and,~~ and

one or more servers capable of communicating through a secure medium with the application component.

46. (Original) The communication system of claim 45, wherein the communication protocol component is a smart messaging service component for mobile devices.

47. (Currently Amended) The communication system of claim 46, further comprising:

one or more smart messaging service servers capable of communicating through a communications medium with the smart messaging service component; ~~and,~~ and

wherein the one or more servers that communicate with the application component are web servers.

48. (Original) The communication system of claim 47, wherein the communications medium is from the group consisting essentially of smart messaging service wireless link, Code Division Multiple Access, and Global Mobile System.

49. (Original) The communication system of claim 46, wherein the communication device is from the group consisting essentially of Smart phone, smart messaging service capable device, and mobile phone device.

50. (Original) The communication system of claim 45, wherein the nonvolatile storage device is a Flash memory.

51. (Original) The communication system of claim 45, wherein the application component comprises an application file.

52. (Original) The communication system of claim 45, wherein the system area is not modifiable by a user of the communication device.

DELL EXHIBIT 1002
Page 302 of 659

REMARKS

Claims 1-52 are now pending with claims 1, 12, 19, 27, 32, 38, and 45 being independent.

The specification and claims have been amended to correct grammatical errors and other informalities. Support for corrections and changes to the specification can be found in the drawings, specification, and claims. No new matter has been introduced.

In view of these remarks and amendments, Applicants submit that this application is in condition for allowance and the Examiner's prompt action in accordance therewith is respectfully requested. The Commissioner is authorized to charge any additional fees and/or credit any overpayment to Deposit Account 50-3361 of Indranil Chowdhury, P.C.

Respectfully submitted,

/Charles C. Claunch/

Charles C. Claunch
Reg. No. 51,221
Indranil Chowdhury
Reg. No. 47,490
Attorneys for Applicants

Chowdhury & Georgakis, P.C.
Phone Num.: (281) 207-5327
E-mail: Ichowdhury@cgiplaw.com

Electronic Acknowledgement Receipt

EFS ID:	1982512
Application Number:	11484100
International Application Number:	
Confirmation Number:	7749
Title of Invention:	Electronic device security and tracking system and method
First Named Inventor/Applicant Name:	Apurva Mahendrakumar Bhansali
Correspondence Address:	Apurva M. Bhansali Softex, Inc. Suite 201 9300 Jollyville Rd. Austin TX 78759 US 2812075327 -
Filer:	Charles Christopher Claunch
Filer Authorized By:	
Attorney Docket Number:	SOFP:115US
Receipt Date:	17-JUL-2007
Filing Date:	11-JUL-2006
Time Stamp:	21:16:23
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes) /Message Digest	Multi Part /.zip	Pages (if appl.)
1	Miscellaneous Incoming Letter	SOFP115US_TransmittalForm_PrelimAmendment_17Jul07.pdf	49742 94e179f41bde0f6a9d422b2e5e0610f6ff8deb48	no	1
Warnings:					
Information:					
2		SOFP115US_PreliminaryAmendment_17Jul07.pdf	88389 2980696a3cfb342e2072d518a8eb462b9f49acf3	yes	18

Multipart Description/PDF files in .zip description

Document Description	Start	End
Preliminary Amendment	1	1
Specification	2	8
Claims	9	17
Applicant Arguments/Remarks Made in an Amendment	18	18

Warnings:	
Information:	
Total Files Size (in bytes):	138131

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/21 (04-07)
Approved for use through 09/30/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission	19

Application Number	11/484100
Filing Date	07-11-2006
First Named Inventor	Apurva M. Bhansali
Art Unit	2134
Examiner Name	Zand, Kambiz
Attorney Docket Number	SOFP:115US

ENCLOSURES (*Check all that apply*)

- ☐ Fee Transmittal Form
  - ☐ Fee Attached
- ☑ Amendment/Reply
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
- ☐ Certified Copy of Priority Document(s)
- ☐ Reply to Missing Parts/ Incomplete Application
  - ☐ Reply to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
  - ☐ Landscape Table on CD
- ☐ After Allowance Communication to TC
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- ☐ Proprietary Information
- ☐ Status Letter
- ☐ Other Enclosure(s) (please Identify below):

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	Chowdhury & Georgakis, P.C.		
Signature	/Charles C. Claunch/		
Printed name	Charles C. Claunch		
Date	07-17-2007	Reg. No.	51,221

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature	/Charles C. Claunch/		
Typed or printed name	Charles C. Claunch	Date	07-17-2007

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/484,100	07/11/2006	Apurva Mahendrakumar Bhansali	SOFP:115US	7749

7590 09/03/2009

Apurva M. Bhansali
Softex, Inc.
Suite 201
9300 Jollyville Rd.
Austin, TX 78759

EXAMINER	
TOLENTINO, RODERICK	
ART UNIT	PAPER NUMBER
2439	

MAIL DATE	DELIVERY MODE
09/03/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	11/484,100	BHANSALI ET AL.	
	Examiner	Art Unit	
	Roderick Tolentino	2439	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 July 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-52* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-52* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11 July 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *7/9/2007 7/11/2006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1 – 52 are pending.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 2, 4, 5, 6, 7, 10, 11, 12, 17, 18, 19, 24, 26, 28, 30, 31, 33, 36, 37, 43, 44, 50 and 51are rejected under 35 U.S.C. 103(a) as being unpatentable over Watanabe U.S. Patent No. (7,096,366) in view of Hamilton et al. U.S. Patent No. (7,404,202).

4. As per claims 1, 6, 12 and 19, Watanabe teaches a nonvolatile storage device (Watanabe, Col. 1 Lines 59 – 62, nonvolatile memory), a changeable area in the nonvolatile storage device, wherein the changeable area further comprises an application component and a secure area coupled to the application component (Watanabe, Col. 1 Lines 59 – 62, nonvolatile memory with area for storing security function) but fails to teach a server system capable of communicating through a secure medium with the application component. However, in an analogous art Hamilton teaches a server system capable of communicating through a secure medium with the application component (Hamilton, Col. 2 Lines 35 – 41, server in communication with security device).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Hamilton's system for providing secure electronic commerce transactions in view of Watanabe's portable electronic device with a security function and a nonvolatile memory because it offers the advantage of positively determining that a transmission is from an authentic source (Hamilton, Col. 2 Lines 2 – 4).

5. As per claims 2, 7, 28 and 33, Watanabe as modified teaches wherein the server system is capable of communicating through the secure medium with the secure area (Watanabe, Col. 1 Lines 59 – 62, nonvolatile memory with area for storing security function).

6. As per claims 4, 10, 17, 24, 30, 36, 43 and 50, Watanabe as modified teaches the nonvolatile storage device is a Flash memory (Watanabe, Col. 3 Lines 36 – 39, EEPROM).

7. As per claims 5, 11, 18, 26, 31, 37, 44 and 51, Watanabe as modified teaches the application component comprises an application file (Watanabe, Col. 1 Lines 59 – 62, nonvolatile memory with area for storing security function).

8. As per claims 27, 32, 38 and 45 Watanabe teaches a controller unit, a digital signal processor coupled to the controller unit (Watanabe, Col. 1 Lines 49 – 51, portable electronic device), a nonvolatile storage device (Watanabe, Col. 1 Lines 59 – 62, nonvolatile memory), a changeable area in the nonvolatile storage device, wherein the changeable area further comprises an application component and a secure area coupled to the application component (Watanabe, Col. 1 Lines 59 – 62, nonvolatile

memory with area for storing security function) but fails to teach a server system capable of communicating through a secure medium with the application component. However, in an analogous art Hamilton teaches a server system capable of communicating through a secure medium with the application component (Hamilton, Col. 2 Lines 35 – 41, server in communication with security device).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Hamilton's system for providing secure electronic commerce transactions in view of Watanabe's portable electronic device with a security function and a nonvolatile memory because it offers the advantage of positively determining that a transmission is from an authentic source (Hamilton, Col. 2 Lines 2 – 4).

9. Claims 3, 9, 13 – 16, 20 – 23, 29, 35, 39 – 42, 46 – 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Watanabe U.S. Patent No. (7,096,366) and Hamilton et al. U.S. Patent No. (7,404,202) and in further view of Kikinis et al. U.S. Patent No. (6,523,079).

10. As per claims 3, 9, 29 and 35, Watanabe fails to teach the electronic device is a personal digital assistant. However, in an analogous art Kikinis teaches the electronic device is a personal digital assistant (Kikinis, Col. 3 Lines 1 – 10, Personal digital assistant).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Kikinis' micropersonal digital assitant in view of

Watanabe's portable electronic device with a security function and a nonvolatile memory because it offers the advantage of providing communication in the fastest available means between a host and pda (Kikinis, Col. 2 Lines 37 – 40).

11. As per claims 13, 20, 39 and 46, Watanabe as modified fails to teach the communication protocol component is a smart messaging service component for mobile devices. However, in an analogous art Kikinis teaches the communication protocol component is a smart messaging service component for mobile devices (Kikinis, Col. 3 Lines 1 – 10, Personal digital assistant with text capabilities).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Kikinis' micropersonal digital assitant in view of Watanabe's portable electronic device with a security function and a nonvolatile memory because it offers the advantage of providing communication in the fastest available means between a host and pda (Kikinis, Col. 2 Lines 37 – 40).

12. As per claims 14, 21, 40 and 47, Watanabe as modified teaches one or more smart messaging service servers capable of communicating through a communications medium with the smart messaging service component; and, wherein the one or more servers that communicate with the application component are web servers (Kikinis, Col. 3 Lines 1 – 10, Personal digital assistant with text capabilities).

13. As per claims 15, 22, 41 and 48, Watanabe as modified teaches the communications medium is from the group consisting essentially of smart messaging service wireless link, Code Division Multiple Access, and Global Mobile System (Kikinis, Col. 3 Lines 1 – 10, Personal digital assistant with text capabilities).

14. As per claims 16, 23, 42 and 49, Watanabe as modified teaches the electronic device is from the group consisting essentially of Smart phone, smart messaging service capable device, and mobile phone device (Kikinis, Col. 3 Lines 1 – 10, Personal digital assistant with text capabilities).

15. Claims 8, 25, 34 and 52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Watanabe U.S. Patent No. (7,096,366) and Hamilton et al. U.S. Patent No. (7,404,202) and in further view of Kamibayahsi et al. U.S. Patent No. (7,181,008).

16. As per claims 8, 25, 34 and 52, Watanabe fails to teach the system area is not modifiable by a user of the electronic device. However, in an analogous art Kamibayashi teaches the system area is not modifiable by a user of the electronic device (Kamibayashi, Col. 5 Lines 56 – 67, secure area in the Flash memory)

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Kamibayashi's contents management method with Watanabe's portable electronic device with a security function and a nonvolatile memory because it offers the advantage of protecting data (Kamibayashi, Col. 1 Lines 37 – 39).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Roderick Tolentino whose telephone number is (571) 272-2661. The examiner can normally be reached on Monday - Friday 9am to 5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Roderick Tolentino
Examiner
Art Unit 2439

/R. T./
Examiner, Art Unit 2439

/Christopher J Brown/
Primary Examiner, Art Unit 2439

Notice of References Cited	Application/Control No. 11/484,100	Applicant(s)/Patent Under Reexamination BHANSALI ET AL.	
	Examiner Roderick Tolentino	Art Unit 2439	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-7,096,366	08-2006	Watanabe, Takafumi	713/182
*	B	US-6,523,079	02-2003	Kikinis et al.	710/303
*	C	US-7,181,008	02-2007	Kamibayashi et al.	380/22
*	D	US-7,404,202	07-2008	Hamilton et al.	726/5
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11484100	BHANSALI ET AL.
	Examiner	Art Unit
	Roderick Tolentino	2439

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	08/19/2009								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								
	21	✓								
	22	✓								
	23	✓								
	24	✓								
	25	✓								
	26	✓								
	27	✓								
	28	✓								
	29	✓								
	30	✓								
	31	✓								
	32	✓								
	33	✓								
	34	✓								
	35	✓								
	36	✓								

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11484100	BHANSALI ET AL.
	Examiner	**Art Unit**
	Roderick Tolentino	2439

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	08/19/2009								
	37	✓								
	38	✓								
	39	✓								
	40	✓								
	41	✓								
	42	✓								
	43	✓								
	44	✓								
	45	✓								
	46	✓								
	47	✓								
	48	✓								
	49	✓								
	50	✓								
	51	✓								
	52	✓								

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	11484100	BHANSALI ET AL.
	Examiner	Art Unit
	Roderick Tolentino	2439

SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
EAST Keyword Search (see search history)	8/19/2009	RT
Class Search (EAST) with text limiting (see search history)	8/19/2009	RT

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

PTO/SB/08a (08-07)
Approved for use through 09/30/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	11484100
Filing Date	2006-07-11
First Named Inventor	Bhansali
Art Unit	2134
Examiner Name	Zand, Kambiz
Attorney Docket Number	SOFP:115US

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/R.T./	1	5680547		1997-10-21	Chang	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/R.T./	1	20030051090	A1	2003-03-13	Bonnett et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
/R.T./	1	WO98/43151	WO	A1	1998-10-01	Cotichini et al.		☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]

Receipt date: 07/09/2007	Application Number	11484100	11484100 - GAU: 2439
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Filing Date	2006-07-11	
	First Named Inventor	Bhansali	
	Art Unit	2134	
	Examiner Name	Zand, Kambiz	
	Attorney Docket Number	SOFP:115US	

	1		☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	/Roderick Tolentino/	Date Considered	08/23/2009

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

PTO/SB/08A (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	TBA
Filing Date	July 11, 2006
First Named Inventor	Apurva M. Bhansali
Art Unit	TBA
Examiner Name	TBA
Attorney Docket Number	SOFP:115US

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
/R.T./		US- 5,715,174	02/03/1998	Cotichini et al.	
		US- 5,764,892	06/09/1998	Cain et al.	
		US- 5,802,280	09/01/1998	Cotichini et al.	
		US- 6,244,758 B1	06/12/2001	Solymar et al.	
		US- 6,269,392 B1	07/31/2001	Cotichini et al.	
		US- 6,300,863 B1	10/09/2001	Cotichini et al.	
		US- 6,507,914 B1	01/14/2003	Cain et al.	
		US- 20020194500	12/19/2002	Bajikar	
		US- 20030172306	09/11/2003	Cain et al.	
		US- 20030005316	01/02/2003	Girard	
		US- 20050216757 A1	09/29/2005	Gardner	
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/Roderick Tolentino/	Date Considered	08/23/2009

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	4420783	@ad<"20030823"	US-PGPUB; USPAT	OR	OFF	2009/08/19 12:26
S2	0	S1 and (nonvolatile near4 security near4 track$3)	US-PGPUB; USPAT	OR	OFF	2009/08/19 12:26
S3	159	S1 and (nonvolatile near4 security)	US-PGPUB; USPAT	OR	OFF	2009/08/19 12:27
S4	0	S1 and (nonvolatile near4 security near4 devic)	US-PGPUB; USPAT	OR	OFF	2009/08/19 12:28
S5	0	S1 and (nonvolatile near4 security near4 devicd)	US-PGPUB; USPAT	OR	OFF	2009/08/19 12:28
S6	36	S1 and (nonvolatile near4 security near4 device)	US-PGPUB; USPAT	OR	OFF	2009/08/19 12:28
S7	36	S1 and (nonvolatile near4 security near4 device)	US-PGPUB; USPAT	OR	OFF	2009/08/19 12:29
S8	104108	S1 and (non-volatile)	US-PGPUB; USPAT	OR	OFF	2009/08/19 12:30
S9	1	S1 and (nonvolatile near4 security near4 device near4 application)	US-PGPUB; USPAT	OR	OFF	2009/08/19 12:30
S10	11	S1 and (nonvolatile near4 security near4 server)	US-PGPUB; USPAT	OR	OFF	2009/08/19 12:37
S11	1	("5933605").PN.	USPAT; USOCR	OR	OFF	2009/08/20 08:07
S12	4420786	@ad<"20030823"	US-PGPUB; USPAT	OR	OFF	2009/08/20 14:25
S13	36	S12 and (nonvolatile near4 security near4 device)	US-PGPUB; USPAT	OR	OFF	2009/08/20 14:25
S14	20	S12 and (Flash near4 (section area) near4 secure)	US-PGPUB; USPAT	OR	OFF	2009/08/20 14:26
S15	4	S12 and (secure near4 SMS near4 device)	US-PGPUB; USPAT	OR	OFF	2009/08/20 14:28
S16	15	S12 and (secure near4 text near4 device)	US-PGPUB; USPAT	OR	OFF	2009/08/20 14:29
S17	14	S12 and (secure near4 pda near4 device)	US-PGPUB; USPAT	OR	OFF	2009/08/20 14:30
S18	11	S12 and (nonvolatile near4 security near4 server)	US-PGPUB; USPAT	OR	OFF	2009/08/20 14:33

S19	0	S18 and pda	US-PGPUB; USPAT	OR	OFF	2009/08/20 14:33
S20	36	S12 and (nonvolatile near4 security near4 device)	US-PGPUB; USPAT	OR	OFF	2009/08/20 14:34
S21	3	S20 and pda	US-PGPUB; USPAT	OR	OFF	2009/08/20 14:34

8/23/2009 8:13:54 PM
C:\Documents and Settings\rtolentino\My Documents\EAST\Workspaces\Case_11484100.wsp

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 7749

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
11/484,100	07/11/2006 RULE	726	2439	SOFP:115US

APPLICANTS

Apurva Mahendrakumar Bhansali, Austin, TX;
Manoj Kumar Jain, Austin, TX;
Shradha Dube, Austin, TX;
Gayathri Rangarajan, Austin, TX;
Mehul Ramjibhai Patel, Austin, TX;
Rayesh Kashinath Raikar, Austin, TX;
Kamal Mansukhlal Dhanani, Austin, TX;
Ranjit Kapila, Austin, TX;
Elza Abraham Varghese, Houston, TX;
Thomas David Tucker, Austin, TX;

**** CONTINUING DATA ***************************

This application is a DIV of 10/925,161 08/23/2004
which claims benefit of 60/497,182 08/23/2003

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **
08/03/2006

			STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
Foreign Priority claimed ☐ Yes ☑ No		☐ Met after Allowance	TX	79	52	8
35 USC 119(a-d) conditions met ☐ Yes ☑ No						
Verified and Acknowledged	/RODERICK TOLENTINO/ Examiner's Signature	/RT/ Initials				

ADDRESS

Apurva M. Bhansali
Softex, Inc.
Suite 201
9300 Jollyville Rd.
Austin, TX 78759
UNITED STATES

TITLE

Electronic device security and tracking system and method

FILING FEE RECEIVED		
1925	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

54. (New) A mobile electronic device according to claim 53, wherein the operation of allowing the security application in the mobile electronic device to communicate with the security service comprises:

automatically causing user data to be copied from the mobile electronic device to at least one of the servers, in response to the theft report.

55. (New) A mobile electronic device according to claim 54, wherein the theft report includes no third-party certification.

56. (New) A mobile electronic device according to claim 53, wherein:

the one or more machine-readable media comprises non-volatile memory;

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;

the security application resides at least partially in the system area; and

the security application receives the theft report from at least one of the servers via the system area.

57. (New) A mobile electronic device according to claim 53, wherein:

the mobile electronic device comprises a mobile phone; and

the operation of automatically disabling at least one user function of the mobile electronic device comprises preventing a person from using the mobile phone for calls, while allowing the security application in the mobile phone to communicate with one or more servers.

58. (New) A mobile phone according to claim 57, wherein the operation of enabling the owner to register the mobile electronic device with the security service comprises providing the security service with at least three items from the group consisting of: a phone number for the mobile phone, a phone service provider for the mobile phone, an International Mobile Equipment Identifier (IMEI) number for the mobile phone, and a phone description for the mobile phone.