

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
8 October 2009 (08.10.2009)

(10) International Publication Number  
**WO 2009/122309 A2**

(51) International Patent Classification:  
*H04W 12/12* (2009.01)

**DERGAST, Paul** [IE/IE]; Evergreen House, Congress Road, Cork (IE).

(21) International Application Number:  
PCT/IB2009/005823

(74) Agents: **DE ANNA, Pier Luigi** et al.; c/o Notarbartolo & Gervasi GmbH, Bavariaring 21, 80336 Munich (DE).

(22) International Filing Date:  
1 April 2009 (01.04.2009)

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:  
12/060,862 1 April 2008 (01.04.2008) US  
12/203,832 3 September 2008 (03.09.2008) US

(71) Applicant (for all designated States except US):  
**YOUGETITBACK LIMITED** [IE/IE]; Evergreen House, Congress Road, Cork (IE).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **FITZGERALD, William** [IE/IE]; Evergreen House, Congress Road, Cork (IE). **BERMINGHAM, Peter** [IE/IE]; Evergreen House, Congress Road, Cork (IE). **HANNIGAN, Frank** [IE/IE]; Evergreen House, Congress Road, Cork (IE). **PREN-**

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR),

[Continued on next page]

(54) Title: METHOD FOR MONITORING THE UNAUTHORIZED USE OF A DEVICE

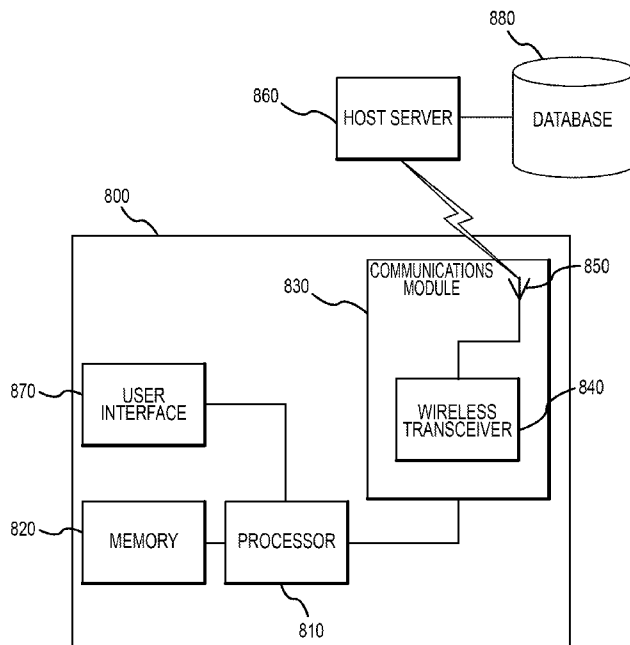


FIGURE 8

(57) Abstract: The invention is directed to systems and methods for detecting the loss, theft or unauthorized use of a device and/or altering the functionality of the device in response. In one embodiment, a device monitors its use, its local environment, and/or its operating context to determine that the device is no longer within the control of an authorized user. The device may receive communications or generate an internal signal altering its functionality, such as instructing the device to enter a restricted use mode, a surveillance mode, to provide instructions to return the device and/or to prevent unauthorized use or unauthorized access to data. Additional embodiments also address methods and systems for gathering forensic data regarding an unauthorized user to assist in locating the unauthorized user and/or the device.

WO 2009/122309 A2

OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG). **Published:**

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

**METHOD FOR MONITORING THE  
UNAUTHORIZED USE OF A DEVICE**

**CROSS REFERENCE TO RELATED APPLICATIONS**

5           This application is a continuation-in-part of United States Utility Patent Application number 12/060,862 filed April 1, 2008 titled, "Method For Monitoring the Unauthorized Use Of A Device," the disclosure of which is fully incorporated herein by reference for all purposes.

**NOTICE OF INCLUDED COPYRIGHTED MATERIAL**

10           A portion of the disclosure of this patent document contains material which is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction by anyone of the patent document or the patent disclosure, as it appears in the Patent and Trademark Office patent file or records, but otherwise reserves all copyright rights whatsoever. All trademarks and service marks identified herein are owned by the applicant.

**DESCRIPTION OF THE INVENTION**

**Field of the Invention**

          The present invention relates to systems and methods for altering the function of an electronic device in response to the device being lost, stolen or used in an unauthorized manner. The altered functionality could facilitate (1) the return of the device, and/or (2) altering the  
20           operation of the device. The invention may also facilitate the monitoring of an unauthorized user of the device.

**Background of the Invention**

          Today, the use of electronic devices is widespread. Such devices can increase a user's productivity and quality of life, but they are susceptible to loss, theft, or unauthorized use.  
25           Examples of such devices are cellular phones, portable digital assistants (PDAs), digital cameras, and laptop computers. These devices often carry private, confidential and/or difficult-to-replace data, and the loss of such data further compounds the loss of the electronic device since, while an electronic device that has been lost or stolen can be physically replaced, oftentimes the data stored on such a device is confidential and/or irreplaceable.

30           Additionally, the authorized user (which may or may not be the owner) of a lost or stolen device may have to deal with ramifications, such as the misuse of information if an unauthorized user (as used herein, "unauthorized user" means anyone than the authorized user or someone authorized by the authorized user to use the device) gains access to information stored on the device. Further, it is not uncommon for hours or even days to elapse before the owner or

authorized user of such a device discovers the loss, and during that time, an unauthorized user may be accessing sensitive data, misappropriating information, or running up charges for goods or services on the authorized user's accounts.

### **SUMMARY OF THE INVENTION**

5 Both the foregoing summary and the following detailed description are exemplary and explanatory only and are not restrictive of the invention as claimed.

Methods and systems according to the present invention provide one or more of the following functions: (1) enhancing the likelihood that the device is recovered by providing information to assist the unauthorized user in returning the device, (2) altering the function of the  
10 device (optionally including the prevention of access to information on the device), and (3) obtaining information about the unauthorized user to improve the chance that the unauthorized user will be identified and both the unauthorized user and device located. Further, a system and method of the invention may provide a rapid response to alert the authorized user that the device has either been misplaced or stolen.

### **BRIEF DESCRIPTION OF THE DRAWINGS**

15 A more complete understanding of the present invention may be derived by referring to the detailed description and claims when considered in connection with the following illustrative figures.

Figure 1 is a flow diagram depicting an exemplary process of the present invention.

20 Figure 2 is a flow diagram depicting an exemplary process of the present invention with respect to a device on which telephone calls can be made.

Figure 3 is a flow diagram depicting substeps of step 120 according to an exemplary method of the invention.

25 Figure 4 is a flow diagram depicting substeps of step 120 according to an exemplary method of the invention.

Figure 5 is a flow diagram depicting substeps of step 120 according to an exemplary method of the invention.

Figure 6 is a diagram showing various functionalities of the invention, one or more of which may be included in step 140.

30 Figure 7 is a diagram depicting various functionalities of the invention, one or more of which may be included in step 680.

Figure 8 is a block diagram depicting an exemplary system according to various aspects of the present invention.

Figures 9-16 depict exemplary notification measures that can be provided on a mobile computing device such as a laptop computer in accordance with the present invention.

Figures 17-25 depict exemplary notification messages that may be displayed on a cellular phone, a PDA, or handheld mobile device.

5        Figures 26-37 depict exemplary screens and processes associated with a host server as exemplified by embodiments of the present invention.

Figures 38-58 illustrate installation and registration of a software application downloaded onto a mobile device.

10       Figures 59-64 illustrate embodiments of the present invention showing a process for uninstalling the application from a mobile device.

### **DETAILED DESCRIPTION OF EXEMPLARY EMBODIMENTS**

As used herein, the term “mobile device,” “mobile electronic device,” or “device” generally refers to any electronic device capable of being lost or stolen. A mobile device may be a stand-alone device such as a laptop computer, a desktop computer, a mobile subscriber  
15       communication device, a mobile phone, a personal digital assistant (PDA), a data tablet, a digital camera, a video camera, a video game console, a media player, a global positioning system (GPS), Universal Serial Bus (USB) keys, mobile weapons, and combinations thereof. A mobile electronic device may also be any electronic device integrated with another system or device.  
20       For example, a stereo, global positioning system, or other electronic device contained within a vehicle may be monitored and protected in accordance with the present invention. Software to implement methods of the present invention can be (1) installed on, or (2) downloaded onto a mobile device indirectly or directly at any time by an authorized user through the Internet, SMS text message, or in any other suitable manner and at any suitable time for carrying out a method  
25       according to the invention. For example, the software may be installed on the device when purchased or downloaded after the device is purchased, or even after the device is lost or stolen. The mobile device may be insured against loss or theft, and systems and methods of the present invention may operate as part of, or in addition to, an insurance policy on the mobile device.

An authorized user of a mobile device may qualify for a lower insurance premium if the  
30       insured mobile device is protected by a lockout or recovery service as provided by embodiments of the present invention. In another embodiment, an insurance company may mandate recovery or lockout services be provided with an insured device where a claim against the policy may result in replacement for lost or stolen mobile devices. Therefore, embodiments of the present invention assist with preventing insurance fraud. For example, if a parent buys a new phone and

insures the phone against loss or theft, the parent may desire to give the insured phone to one of his/her children and file an insurance claim to replace the donated phone, claiming it as a lost or stolen device, thus avoiding the cost of purchasing a new phone. The present invention may be used to prevent such a fraudulent claim, by, for example, disabling use of the alleged lost or  
5 stolen phone, detecting attempted use of the alleged lost or stolen phone, or tracking location or users of the alleged lost or stolen phone.

In one embodiment, a mobile device operating in conjunction with the present invention includes a wireless transceiver to communicate with other systems and devices through a wireless system such as a wireless mobile telephony network, General Packet Radio Service  
10 (GPRS) network, wireless Local Area Network (WLAN), Global System for Mobile Communications (GSM) network, Personal Communication Service (PCS) network, Advanced Mobile Phone System (AMPS) network, and/or a satellite communication network. Mobile devices operating in conjunction with the present invention may also communicate with other systems and devices through any other type of connection, such as a wired Internet connection, a  
15 wireless Internet connection, a cellular telephone network connection, a wireless LAN connection, a wireless WAN connection, an optical connection, a USB connection, a mobile device synchronization port connection, a power connection, and/or a security cable.

Systems and methods of the present invention may be employed as part of a subscriber-based service to help protect and recover a wide variety of different mobile devices. Authorized  
20 users can be linked to multiple mobile devices using a unique identifier for each device. Any suitable identifier may be provided, such as the serial number of the mobile device (or a component thereof), or a numeric, alphabetic, alphanumeric, or other identifier. The identifier can be used to verify the identity of authorized users associated with the device, as well as to monitor the mobile device and provide for its recovery should it be lost or stolen. In one  
25 embodiment of the present invention, for example, the identifier and information for associated authorized users may be stored in a storage medium (such as a memory on the mobile device or a central server) for future reference.

Moreover, a system and method according to the invention may have a different response for different inputs or conditions, including the sensing of varying threat levels. For example, a  
30 laptop sensing that it is in a prohibited area (such as outside of a building to which it is assigned or in a foreign country) might prevent access with one or more encryption techniques, delete data or corrupt the hard drive to make data retrieval difficult or impossible. The same laptop, upon receiving a signal that it is lost within a building to which it is assigned could simply provide notification describing how to return the laptop.

Any combination and/or subset of the elements of the methods depicted herein may be practiced in any suitable order and in conjunction with any suitable system, device, and/or process. The methods described and depicted herein can be implemented in any suitable manner, such as through software operating on the mobile device and a host server. The software may  
5 comprise computer-readable instructions stored in a medium (such as the memory of the mobile device or host server) and can be executed by one or more processors to perform the methods of the present invention.

Turning now to the figures, where the purpose is to describe preferred embodiments of the invention and not to limit same, exemplary methods according to various aspects of the  
10 present invention are depicted in Figures 1-7.

In method 100 illustrated in Figure 1, a notification is provided by a mobile device to an authorized user (110) describing how to return the mobile device. As used herein, “unauthorized user” means any person other than the authorized user. The notification can be provided in any number of ways and be triggered by any suitable event. For example, the notification may be a  
15 visual display or an audio signal, such as a voice. The notification should provide adequate information to the unauthorized user to enable the unauthorized user to return the device, and could include one or more of a phone number, address or email address. The notice could also offer a reward for return of the device.

The notice could be triggered in any suitable manner. For instance, the authorized user  
20 could send a signal to the device to display the notice, or the authorized user could contact a service that would send a signal to the device to activate the notice. The notice could also be displayed automatically, for example, if the wrong password were keyed in a predetermined amount of times or if the device sensed it was in a certain geographical area. Any other suitable self-triggering event could also be utilized.

Another and optional feature of the device is detection of a security compromise event  
25 (120) and a determination (130) of whether the function of the device should be altered in response to the security compromise event. If appropriate, the functionality of the device is altered (140) if a security compromise event (including the device being lost or stolen).

### 30 PROVIDING NOTIFICATION DESCRIBING HOW TO RETURN THE MOBILE DEVICE

In an exemplary process 100 according to the present invention depicted in Figure 1, an event 105 triggers a notification to be provided 110 by the device describing how to return the device. The notification may be provided in any manner, such as by using a display, microphone, or other user interface feature(s) of the mobile device. The notification may include

any symbols, characters, numbers, graphics, sounds (including recorded voice messages and/or music), and/or any other indicia to aid in describing how to return the device (for example a message displayed on a screen).

5 The notification may include, for example, one or more of a telephone number for a service providing recovery instructions or the telephone number of the authorized user, a turn-in location or address, instructions to activate a feature of the mobile device to initiate a return process, a web address for a service providing recovery instructions, and/or a clickable link to a website comprising recovery instructions. The notification may also include a message that a reward is available for turning in the device to a recovery service. In one embodiment of the present invention, the notification is displayed on the login screen (including the mechanism for returning the device) such that it is the first information seen by a user before the user can access the device. If an authorized user (such as the owner) fears they have lost control of the device they can remotely activate the application on the mobile device and make sure that access is restricted to only showing a notification and details on how to return the device. One benefit of 10 this approach is the preservation of the confidential nature of the information located on the mobile device, essentially protecting sensitive information from unauthorized access. An innocent finder of the mobile device is also able to return the device without having to bypass or break the password on the mobile device to determine the identity of the authorized user. 15

When the notification is provided a separate signal or message that the mobile device has been lost or stolen. The notification can help an unauthorized user of the mobile device return it to its authorized user, and the notification is likely to increase the probability that the unauthorized user will do so, since he/she is provided with the appropriate instructions or information. Additionally, the conspicuousness of the notification may also deter an unauthorized user who is a thief from stealing the mobile device or attempting to keep, use, or 20 sell the mobile device. 25

The notification may be provided to any person (such as the unauthorized person currently in possession of the mobile device), as well as other individuals, systems, and devices in communication with the mobile device. In one exemplary embodiment of the present invention, referring to Figure 2, providing a notification (110) describing how to return a mobile device (such as a mobile phone) may include: determining a phone number (210) dialed by the current unauthorized user of the mobile device, calling the phone number (220), and presenting a message (such as pre-recorded, text or message from a live person) (230). The message may include any desired information, such a notice that the mobile device has been reported lost or stolen, and/or instructions to assist in initiating return of the mobile device. 30



Alternate embodiments may include presenting an SMS text message, an email message (e.g., sent to an email address of the current user), a sequence of dual-tone multi-frequency (DTMF) tones, and/or any other message type. This allows the mobile device to alert the unauthorized user in possession of the mobile device that he/she is not authorized to use the device and/or provides instructions on how to return the device. This may expedite the return of the mobile device, as well as to deter individuals from stealing or withholding the device from its rightful owner.

The notification may be provided using some or all of the user interface capabilities of the mobile device. For example, a notification for a laptop computer may include a large, message on the screen to draw the attention of observers that it is protected, and/or one or more sounds (including music, pre-recorded speech and alarm) played through the laptop's speaker. Similarly, a cell phone could present a text display and/or emit sounds to instruct the unauthorized user how to return the device or an alarm sound to attract attention to the unauthorized user and make it undesirable to keep the device. The notification may be presented through one or more of any other user interface feature(s) integrated with, or in communication with, the mobile device, such as a printer.

#### DETECTING A SECURITY COMPROMISE EVENT

In the exemplary method shown in Figure 1, the mobile device detect that a security compromise event (120) has occurred. As used herein, a "security compromise event" generally refers to any situation where the mobile device (or any physical or functional portion thereof) is (or may be) outside the exclusive control of an authorized user, and a device may be able to detect multiple types of security compromise events, in which case the device may have different responses for different types of security compromise events.

The mobile device may in various embodiments include a removable or interchangeable SIM card. In an implementation of methods of the present invention, detecting that a security compromise event has occurred further comprises detecting that a SIM card associated with the mobile device has been exchanged. Detecting the exchange may be by any method, such as detecting that an access door to a SIM card storage area has been opened, detecting that an identifier within the SIM card does not match a stored identifier corresponding to a previous SIM card in use by the mobile device, or detecting the failure of an authorization protocol between the SIM card and the mobile device.

In one embodiment, detecting that a security compromise event has occurred further comprises obtaining from the authorized user a set of criteria indicating unauthorized use of the mobile device; and determining that at least one of the criteria indicating unauthorized use has

occurred. The criteria may comprise any information specified by the user that may indicate conditions or limits indicating that the device is not being used in an authorized manner. For example, the criteria indicating unauthorized use of the mobile device may comprise at least one of: a maximum number of calls that may be placed to numbers not included in a pre-stored authorized number list; a maximum number of calls that may be received by numbers not included in the pre-stored authorized number list; and a call being placed to a country code not included in the pre-stored authorized number list. In one embodiment, the set of criteria indicating unauthorized use of the mobile device are stored in the mobile device. In another embodiment, the set of criteria indicating unauthorized use of the mobile device are stored in a database associated with a security authority.

The mobile device may include a read-only memory. For purposes of the present application, a read only memory (also known as a "ROM") includes not only non-modifiable memories such as mask ROMs and one-time programmable PROMs, but also persistent memories that may not be directly or indirectly modified through the user interface of a mobile device. Such persistent memories may include such storage devices such as field programmable ROMs, EPROMs, EEPROMs, FLASH memory, magnetic storage devices, optical storage devices, or other storage devices. In various embodiments of the present invention, an application may reside in a read-only memory of the mobile device detects that a security compromise event has occurred. In selected instances, the application may not be terminated by a current user of the mobile device if the current user is not the authorized user, providing additional security to prohibit unauthorized users from tampering with security protocols.

A security compromise event may be actual (e.g., the mobile device has actually been stolen), or perceived (e.g., an authorized user is uncertain as to the status of the mobile device, but believes it may be lost or stolen). A security compromise event may include the loss of control of the mobile device by the authorized user, the theft of the mobile device, a loss of knowledge as to the whereabouts of the mobile device, the intrusion of an electronic threat (e.g., an electronic virus, an electronic worm, and/or an electronic trojan horse), the unauthorized access or attempted unauthorized access to private information in the mobile device, use of the mobile device in a manner not authorized by a wireless service provider, the device sensing it is in an unauthorized location, entering an incorrect password multiple times, any other event where compromise of the ownership or security of the mobile device is indicated.

A security compromise event may be detected by the mobile device itself, and may be also be reported by an authorized user directly to the device or indirectly such as through a security authority or other entity, system or device in communication with the mobile device.

The mobile device may in various embodiments include a SIM card. In an implementation of methods of the present invention, detecting that a security compromise event has occurred further comprises detecting that a SIM card associated with the mobile device has been exchanged. Detecting the exchange may be by any method, such as detecting that an access  
5 door to a SIM card storage area has been opened, detecting that an identifier within the SIM card does not match a stored identifier corresponding to a previous SIM card in use by the mobile device, or detecting the failure of an authorization protocol between the SIM card and the mobile device.

In one embodiment, detecting that a security compromise event has occurred further  
10 comprises obtaining from the authorized user a set of criteria indicating unauthorized use of the mobile device; and determining that at least one of the criteria indicating unauthorized use has occurred. The criteria may comprise any information specified by the user that may indicate conditions or limits indicating that the device is not being used in an authorized manner. For example, the criteria indicating unauthorized use of the mobile device may comprise at least one  
15 of: a maximum number of calls that may be placed to numbers not included in a pre-stored authorized number list; a maximum number of calls that may be received by numbers not included in the pre-stored authorized number list; and a call being placed to a country code not included in the pre-stored authorized number list. In one embodiment, the set of criteria indicating unauthorized use of the mobile device are stored in the mobile device. In another  
20 embodiment, the set of criteria indicating unauthorized use of the mobile device are stored in a database associated with a security authority.

The mobile device may include a read-only memory. For purposes of the present application, a read only memory (also known as a "ROM") includes not only non-modifiable memories such as mask ROMs and one-time programmable PROMs, but also persistent  
25 memories that may not be directly or indirectly modified through the user interface of a mobile device. Such persistent memories may include such storage devices such as field programmable ROMs, EPROMs, EEPROMs, FLASH memory, magnetic storage devices, optical storage devices, or other storage devices. In various embodiments of the present invention, an application may reside in a read-only memory of the mobile device detects that a security  
30 compromise event has occurred. In selected instances, the application may not be terminated by a current user of the mobile device if the current user is not the authorized user, providing additional security to prohibit unauthorized users from tampering with security protocols.

The mobile device may detect a security compromise event in any manner, such as by receiving a message from an authorized user or a security authority (such as a governmental law

enforcement organization, private security firm, and/or insurance agency), and in response to the message determining that a breach of security has occurred. The security authority may communicate with the mobile device in any desired manner, such as through software operating on a host server in communication with a database. As an example, an authorized user can  
5 report his/her mobile device is missing to the security authority and instruct the security authority to signal the mobile device of a security threat (i.e., the user believes the mobile device has been lost, stolen, or may otherwise be subject to unauthorized access). The functionality of the mobile device can then be altered as a result (140), as discussed further below.

The mobile device may authenticate the validity of a message from a security authority,  
10 such as by computing a digest of the message and comparing the digest value to a previously stored authorization digest value. The computed digest value may be produced by providing the received message to a hashing algorithm such as the MD5 or SHA-1 Secure Hashing Algorithm as specified in National Institute of Standards and Technology Federal Information Processing Standard Publication Number 180-1, the disclosure of which is incorporated by reference herein  
15 in its entirety. The authorization digest value can be any number, code, value, or identifier that allows a received message to be identified as a valid transmission from a security authority. The stored authorization digest value can be provided to the mobile device upon activation of a loss/theft recovery service, as well as in any other desired manner. Unless the authorization digest value matches the stored digest value, the message will not be authenticated and can be  
20 disregarded (if desired). A mobile device acting on a message from a security authority need not necessarily be predicated upon successful authentication of the message, however. The mobile device may authenticate the validity of the message in any other desired manner.

The mobile device may also authenticate the validity of a message from a security authority or other source by decrypting at least part of the message with a public key associated  
25 with the sender of the message as part of an asymmetric encryption algorithm. Asymmetric encryption algorithms and techniques are well known in the art. See, for example, RSA & Public Key Cryptography, by Richard A. Mollin, CRC Press, 2002, and United States Patent No. 4,405,829, issued September 20, 1983, the disclosures of which are fully incorporated by reference herein. In an illustrative example, if two parties (for example, "Alice" and "Bob")  
30 wish to communicate securely using public key cryptography, each party begins by generating a unique key pair, where one of the keys is a private key that is kept in confidence by that party, and the other key is a public key that may be publicly distributed, published only to a message recipient, or made available through a public key infrastructure. The key generation step need be done by a party only once, provided that the party's private key does not become compromised

or known by another party. If Alice wants to send a message confidentially to Bob, she may use Bob's public key to encrypt the message, and once sent, only Bob can decrypt and view the message using Bob's private key. But if Alice also wanted Bob to have assurance that the message was in fact coming from her, she could further encrypt the message with her private key  
5 before sending, then when Bob's private key and Alice's public key are used to decrypt the message, Bob knows for certain that he was the intended recipient and that Alice was the one who originated the message, and Alice knows that only Bob will be able to decrypt and read her message.

Such a scheme may be utilized with embodiments of the present invention. In an  
10 embodiment, full two-way public encryption is used to authenticate that the sender is in fact the security authority (for example) and that the recipient of the message indicating a security compromise event has occurred is in fact the intended recipient. Alternatively, messages may be encrypted with only the private keys of the sending entity, and decrypted with the public keys to expedite processing time. Such encryption schemes assist with validation of security  
15 compromise event communications, both in providing validation of the source and destination of messages, as well as providing a means to security transmit commands to a compromised mobile device.

In alternate embodiment, encrypted or unencrypted data can be transmitted to and from the mobile device through an encrypted transmission protocol, such as the wireless encryption  
20 protocols (WEP, WPA and WPA2) associated with the IEEE 802.11 wireless protocols. Any number of other encryption methods can be used to encrypt data communicated to and from the mobile device in conjunction with the present invention.

A mobile device operating in conjunction with the present invention may receive information that a security compromise event has occurred from a security authority or other  
25 source using any number of messages in any format. For example, embodiments of the present invention may receive information in an SMS text message, a voice mail message, an email message, and/or a predetermined sequence of one or more DTMF tones. The message can be of any desired format. For example, the message can be included in a file having a tokenized format such as standard ASCII text format, or any other suitable standardized file format, such as  
30 an MS Word document, MS Excel file, Adobe PDF file, or binary picture file (JPEG, bitmap, etc.). The data within such a file can be ordered in any manner and have any suitable delimiters, notations, or other features. The message may also have a unique and/or propriety format.

In one embodiment, the message indicating a security compromise event occurred may be encoded in files such as binary picture files via steganographic techniques, so that any person

viewing the file or picture may see an acceptable image while a hidden message is encoded in the data in the file and may be accessed by appropriate software techniques. For example, by sending a graphic image in a file that is named in a manner to solicit a user to open the message/file (for example, "HotJessica.JPG"), then the current user of the mobile device may  
5 open the file which then triggers software on the mobile device to scan the image file, thereby extracting and decoding the steganographically encoded data from the image file. The mobile device may then interpret the decoded data, and if a lockdown event is indicated, the device may take predetermined actions to partially or completely disable use of the device in any of the manners described herein. The software on the mobile device may execute surreptitiously,  
10 whereby the application may execute forensic evidence gathering features such as taking a picture of the current user's face while the user is looking at the image file just opened while the current user is unaware that he/she is being photographed or otherwise logged. Other commands may be sent via encoded or concealed messages, such as commands resetting the password of the device to an alternate or more secure password.

15 The format of the message can also be based on the method by which the message is transmitted to the mobile device. For example, where the message is transmitted to the mobile device using a wireless telephone connection, the message can be formatted as an SMS text message. Similarly, the message may be formatted as an XML record, email, and/or facsimile. The message can include multiple formats and/or multiple messages, and may be formatted  
20 having different formats for transmission in a variety of methods or to a variety of different mobile devices. A message received from a security authority, host server, authorized user, or other source may also include other information, such as instructions for altering the functionality of the mobile device as discussed further below.

In one embodiment of the present invention, a mobile device may be configured to  
25 assume a low-power, quiescent, or standby state, whereby the device may receive notifications from an authorized user or server such as a server administered by a security authority. Upon receiving such notification, the mobile device may take action at an appropriate time, based on contents of the notification. The mobile device may transition from a standby state to poll a server to determine whether a notification is waiting, and if so, downloads and acts upon the  
30 contents of the notification. Additionally or alternatively, the mobile device has a buffering provision that is capable of receiving notifications transmitted by a server or security authority, and acting upon the contents of the message at an appropriate time, such as when the message is received or at a predetermined time interval.

A mobile device may also detect a security compromise event by determining that the mobile device has been disassociated from a designated companion device. The mobile device may be associated with any desired type of device(s). For example, a mobile telephone may be a companion device to another mobile telephone. The two mobile telephones may be associated through a wireless connection (such as a Bluetooth connection), and the loss of the wireless connection may be used to trigger a security compromise event. Similarly, a security compromise event can be triggered when a mobile device is separated from a plurality of companion devices.

The mobile device may determine that it has been disassociated from the companion device in any desired manner, such as by measuring a power level of a wireless signal transmitted by the companion device, and determining that the measured power level has decreased below a predetermined threshold level. Additionally, the mobile device can determine it has been disassociated from the companion device by transmitting a message to the companion device and determining that a message was not received from the companion device that satisfies a predetermined confirmation criterion (e.g., an expected acknowledgement transmission). Additionally, the mobile device can determine it has been disassociated from the companion device where it is unable to establish a communications link with the companion device, or where the companion device sends a signal to the mobile device indicating that access to the mobile device should be restricted. The mobile device may determine it has been disassociated from the companion device when an amount of incident light illuminating at least one surface of the mobile device has varied from a predetermined threshold range. For example, if the mobile device is removed from a companion device such as a purse, carrying case, holster or briefcase, the increase in ambient light on at least one surface of the mobile device could be detected by an included sensor, indicating the device has been removed from a desired location. Similar approaches may include activating a security event check when, a case enclosing the mobile device is opened or if a light sensor in a mating surface between the mobile device and its companion device suddenly detects light when the two devices are disconnected or undocked.

Other embodiments for determining that the mobile device has been disassociated from the companion device are provided, including measuring a current power level of a wireless signal transmitted by the companion device; and determining that the measured current power level has decreased by a predetermined amount. A plurality of power levels of the wireless signal transmitted by the companion device may be measured; and from these measurements steps may include computing an average power level from the plurality of measured power levels; measuring a current power level of a wireless signal transmitted by the companion device;

determining that the measured current power level has varied from the average power level by a predetermined amount. In yet another embodiment, determining that the measured current power level has varied from the an average power level by a predetermined amount further comprises: computing a standard deviation of the plurality of measured power levels; and  
5 determining that the current power level exceeds an allowed signal range determined by a predetermined constant times the standard deviation of the plurality of measured signals. One or more standard deviations may be desirable, based on the desired sensitivity of the system to fluctuations in signal strengths. For instance, in an electronically noisy environment or when the mobile device by necessity needs to move small distances with respect to the companion device,  
10 the predetermined range or standard deviations may be set to a higher level, such as plus or minus three standard deviations.

In another embodiment, determining that the mobile device has been disassociated from the companion device comprises: measuring a plurality of power levels of a wireless signal transmitted by the companion device; computing an average power level from the plurality of  
15 measured power levels; measuring a plurality of current power levels of a wireless signal transmitted by the companion device; determining that for a predetermined number of times within a predetermined time period, one of the plurality of current power levels has varied from the average power level by a predetermined amount. In such an embodiment, for example, it is the relative change of signal power levels compared to a measured average that determines when  
20 a security event is triggered, so the system adapts over time to changes in the signal environment and relative motions of the mobile device and the companion device.

The mobile device may be associated with a companion device in any desired manner, such as by pairing the mobile device with the companion device via a wired link and/or a wireless link. Any desired wireless link and communications protocol may be used to pair a  
25 mobile device with a companion device. For example, a wireless link may include an ISO 14443 protocol, an ISO 18000-6 protocol, a Bluetooth protocol, a Zigbee protocol, a Wibree protocol, an IEEE 802.15 protocol, an IEEE 802.11 protocol, an IEEE 802.16 protocol, an ultra-wideband (UWB) protocol; an IrDA protocol, and combinations thereof. Likewise, a wired link may be  
30 implemented to pair a mobile device with a companion device, such as by using a computer network connection, a USB connection, a mobile device synchronization port connection, a power connection, and/or a security cable.

In various embodiments, when the companion device is disassociated from the mobile device, the mobile device is further configured to format a message for transmission to a security authority, the message comprising information regarding the disassociation of the mobile device



with the companion device; wherein the message is formatted by the companion device. The formatted message may comprise any desired information and may be transmitted to the security authority by wired or wireless means, such as by a cell phone link, or a wired or wireless network interface. The information regarding the disassociation of the mobile device with the companion device comprises, for example: a date that the companion device and the mobile device were disassociated; a time that the companion device and the mobile device were disassociated; a location that the companion device and the mobile device were disassociated; an identifier corresponding to the mobile device; an identifier corresponding to the companion device; and an identifier corresponding to a current user of the mobile device.

A security compromise event may be associated with a change in the hardware of the mobile device. For example, a security compromise event may be determined when an identifier of a hardware identity module (such as a universal subscriber identity module and/or a removable user identity module) in communication with the mobile device does not match one or more predetermined authorized identifiers. Any desired identifier may be used in conjunction with the present invention, such as an electronic serial number, a local area identity identifier, an integrated circuit identifier, an international mobile subscriber identifier, an authentication key identifier, and/or an operator-specific emergency number identifier.

The hardware identity module identifier may be transmitted to a host server, stored in a storage medium (such as the memory of the mobile device or host server), or processed in any other desired manner. For example, the identifiers associated with hardware of a mobile device (e.g., hard drive, SIM card, or other hardware) can be used to determine whether an unauthorized user is attempting to circumvent software or hardware security protocols protecting the mobile device. The hardware identity module identifier (as well as any other data used in conjunction with the present invention) may be stored in any suitable manner, such as by using a memory storage device integrated with, or in communication with, the mobile device. The hardware identity module may also be encrypted, hidden, or protected in any other desired manner.

A security compromise event can be based on a change in a single hardware component of a mobile device, as well as on an overall hardware configuration of the mobile device. For example, the hardware configuration for a mobile device such as a laptop computer may include the identities of a particular hard drive, battery, RAM, BIOS, and other components of the laptop. The hardware configuration for the laptop can be stored (e.g., by a central server and/or the mobile device) and then compared against the current hardware configuration for the laptop (e.g., periodically and/or upon the occurrence of an event, such as a change in a hardware component). If the current hardware configuration has changed from the stored configuration

beyond a predetermined threshold (e.g., more than two individual components are different), a security compromise event can be triggered. This allows a security compromise event to be issued where a thief may be swapping out components of a stolen mobile device in an attempt to circumvent security measures associated with (or stored on) the swapped components. Changes in the hardware configuration of a mobile device (such as changes in SIM card) can be tracked over time and reported to a security authority or authorized user to help locate the mobile device.

A security compromise event may be determined based on the use of the mobile device and/or the behavior of the current user. For example, referring to Figure 3, determining a security compromise event (120) may include accumulating a usage profile of the mobile device over a predetermined time period (310), accumulating information regarding continued usage of the mobile device (320), and determining that the continued usage deviates from the usage profile by a predetermined threshold (330).

The usage profile and the accumulated information may include any desired information about how the mobile device is used, such as a ratio of the number of calls placed from numbers residing within a contact list stored in the mobile device to numbers not residing within the contact list, the time of day that one or more calls were placed by the mobile device, a mean time interval between button presses, a pressed button type, a mean pressure exerted when pressing buttons, a number of times within a predetermined time interval that a password was input incorrectly, a number of consecutive times that a password was input incorrectly, and combinations thereof. The usage profile of an authorized user can then be compared to the accumulated information in order to determine whether or not the authorized user is still in control of the device. The mobile device may take any desired action to verify the current user is authorized to use the mobile device, such as prompting the current user to enter a password, and preventing further use of the device until the password is correctly entered.

The usage profile can be compiled over any desired time period(s). The time period may include a fixed period of time, or may be dynamically determined (e.g. – shifting in time as the mobile device is utilized). The predetermined time period can be specified by an authorized user of the mobile device, as well as determined by the mobile device itself. The predetermined time period can be based on any desired criteria, such as the manner in which the device is used and/or on the amount of information needed to compile the usage profile. Likewise, the period of time in which information about the continued usage of the mobile device can be accumulated may be specified in the same manner as that of the usage profile.

The accumulated continued usage information and the usage profile may be compared to determine the degree to which the continued usage deviates from the usage profile. A

predetermined threshold may be selected according to any desired criteria to determine whether the continued usage is indicative of unauthorized use. For example, if the continued usage includes a significant number of calls outside the time range calls are usually made in the usage profile, the continued usage may be indicative of unauthorized use. Similarly, the time interval  
5 between button presses (i.e., the speed the current user is using the mobile device), the types of buttons pressed, the pressure exerted when pressing the buttons, the number of times (including consecutive times) a password is input incorrectly, and other events may be indicative (alone or in combination) of unauthorized use.

A combination of events may be weighted such that the occurrence of a security  
10 compromise event is based on a predetermined voting threshold. Individual events may be given more significance than other events, such that only a repeated occurrence of a particular event deviates from the predetermined threshold, while a single occurrence of another event deviates from the threshold. For example, a call outside the usage profile's normal time range may need to occur a total of four times before the predetermined threshold is exceeded, while the entering  
15 of an incorrect password two times in succession deviates from the threshold. Similarly, an incorrect password entry in combination with two calls outside the normal time range in the usage profile can deviate from the predetermined threshold. Events may be weighted or scored for the predetermined voting threshold in any desired manner.

A security compromise event may be determined based on the failure of a user to provide  
20 the proper biometric data. In one embodiment of the present invention, for example, a biometric measurement of a current user of the mobile device is obtained, and the biometric measurement is compared to a previously stored reference value. A security compromise event can then be determined where the biometric measurement exceeds a predetermined threshold variance from the previously stored reference value. The security compromise event may be based on any  
25 number of biometric measurements from the current user of a mobile device, such as a fingerprint scan, an iris scan, a retina scan, a voice sample, a breath sample, and/or a photograph of a portion of the body of the current user of the mobile device.

A security compromise event may be determined based on the location of the mobile device. For example, referring now to Figure 4, determining a security compromise event (120)  
30 may include obtaining a physical location of the mobile device (410), analyzing the physical location of the mobile device to determine that the device is located in an unauthorized area (420), and comparing the physical location of the mobile device to a previously stored location list (430).

The physical location of the mobile device may be obtained in any manner. For example, the location of the mobile device may be ascertained using a global positioning system (GPS), through the triangulation of a signal emitted by the mobile device, through an Internet protocol (IP) address and/or traceroute, or in any other manner. A global positioning system may include, for instance, a receiver that detects signals transmitted by transmission sources with known transmission timing and/or known location, and through analyzing the received time-encoded signals at the mobile device. The mobile device may also ascertain its location with respect to the transmission sources. The transmission sources may be terrestrial, mobile, space-based, airborne, or any combination thereof. In one embodiment, the mobile device may ascertain its location on the surface of the earth by receiving and interpreting geolocation signals received from satellites in orbit about the earth. In another embodiment, the global positioning system may include a collection of terrestrial antennas and receivers that receive a signal transmitted from the mobile device, and by analyzing the angle of arrival, time of arrival, and/or time differential of arrival of the mobile device's signal, the location of the mobile device may be ascertained via conventional multilateration approaches. Alternatively, the mobile device may receive one or more signals from known terrestrial transmitting sources such as cellular base station antennae, and through analyzing the received signals, compute its location with respect to the known terrestrial transmitting sources.

The area a mobile device is authorized to operate in may be defined in any manner. For example, the area may be a geographical area defined by a boundary, an area corresponding to a postal code, and/or an area corresponding to a telephone area code. The area may include any number of separate individual areas. An area may be defined based on where the mobile device may operate (i.e. "whitelisting"), as well as on where the mobile device may not operate (i.e. "blacklisting").

The location of the mobile device may be compared to a list that defines one or more locations where the mobile device is authorized to be operated, one or more locations where the mobile device is not authorized to be operated, one or more locations where functionality of the mobile device is at least partially restricted, and/or combinations thereof. The list may be defined by an authorized user of the device and/or a security authority. In one exemplary embodiment of the present invention, a central server (such as host server 860 depicted in Figure 8) monitors the location of the mobile device and compares the device's location to a location list previously stored in a database to determine if a security compromise event has occurred based on the location of the mobile device, and if the functionality of the device should be modified as a result. Among other things, this embodiment allows employers, parents, and other "super-

users” of mobile devices to define boundaries in which the mobile devices should operate when in the hands of employees or children.

5 A security compromise event may be determined based on the location of the mobile device. For example, referring now to Figure 5, determining a security compromise event (120) may include measuring a first environmental parameter at a first time point (510), measuring a second environmental parameter at a second time point (520), comparing the first environmental parameter and second environmental parameter to a predetermined authorized use condition (530), determining that the mobile device has been moved from a first location (540), and transmitting at least one of the first and second measured environmental parameter to a security authority (550).  
10

As used herein, an “environmental parameter” generally includes any parameter pertaining to the mobile device’s environment. The mobile device can measure any desired environmental parameter in any desired format, such as an image taken by the mobile device. Digital cameras (including cameras inside other devices, such as mobile phones), and other devices with imaging capability may thus be used to take an image of the mobile device’s environment, including physical objects and people around the mobile device. Such images can then be used to identify the location of the mobile device and/or the individual(s) responsible for taking or withholding the mobile device from its authorized user(s).  
15

An environmental parameter may also include information from or about systems and devices in communication with the mobile device. In one embodiment of the present invention, for example, a wireless receiver in communication with the mobile device can be activated and used to sense one or more wireless network addresses from one or more signals received by the mobile device at different points in time. The network addresses sensed at different points in time can be compared to determine whether the sensed network addresses differ, and thus determine if the mobile device has moved.  
20  
25

An environmental parameter may further include geolocation information. The geolocation information may be measured from a global positioning system (GPS) in communication with the mobile device, as well as from any other desired source. In one exemplary embodiment of the present invention, the mobile device may receive a signal comprising geolocation information and decode location signals received at the different points in time. The locations corresponding to the signals measured at different times may be compared to determine whether the location of the mobile device has changed, as well as whether the distance between two sampled locations exceeds a predetermined threshold. Any number of location samples can be similarly measured and compared, either to an initial location or to  
30

subsequently-measured locations. The predetermined threshold distance can be configured by a user, a security authority, and/or automatically by the mobile device. This embodiment thus allows the movement of a mobile device to be monitored and a security compromise alert issued if it moves more than a predetermined distance.

5           In various embodiments of the invention, security compromise events may be detected when an unauthorized user attempts to tamper with a security provision of the mobile device. For example, conditions leading to a determination of tampering may include determining that an unauthorized user attempted to mask the reported location of the mobile device; attempted to re-  
10           route an electronic address in the mobile device; attempted to bypass a password prompt provided by the mobile device; attempted a brute force password attack on the mobile device; attempted to install applications intended to thwart operation system security, and combinations thereof.

#### ALTERING THE FUNCTIONALITY OF THE MOBILE DEVICE

15           In the exemplary process depicted in Figure 1, a determination is made as to whether the function of the device should be altered in response to the security compromise event (130), and the functionality of the mobile device altered accordingly (140). The functionality of a mobile device can be altered in any manner and to achieve any purpose, such as to mitigate the harm arising from the compromised status of the device, gather evidence to apprehend and convict a  
20           thief, as well as to encourage/incentivize the return of the device to the proper owner. Referring to Figure 6, altering the functionality of the mobile device (140) may include providing a notification to the current user (610), inhibiting the functionality of the mobile device (620), providing a notification to an authorized user and/or security authority (630), altering the manner in which communications to and from the mobile device are handled (640), protecting data in the  
25           mobile device (650), tracking the mobile device (660), gathering and transmitting information on the usage of the mobile device to a security authority (670), and communicating with other devices (680).

          The functionality of a mobile device can be altered in any manner in response to a security compromise event, including partially or completely disabling features of the device  
30           and/or providing functionality not available prior to the security compromise event. In one embodiment of the present invention for example, the functionality of the mobile device can be altered to present an automated message to the current user of the mobile device (610). The automated message may be in any format and may contain any desired information. For example, the automated message may notify the current user that the mobile device has been lost

or stolen, that a reward is offered for the prompt return of the mobile device, and/or provide instructions for returning the mobile device to the authorized user. The automated message may also notify the current user that any button may be depressed on the mobile device to initiate the recovery process, and/or that a phone number need not be entered to contact a party to return  
5 device to its rightful owner. In such an instance, the mobile device may accept a single button press to initiate contact with a security authority or the authorized user to begin the recovery process. The message may be presented in any manner, such as an audio message, a textual message, and/or a video message. In one embodiment of the present invention, for example, an SMS text message is transmitted by a security authority to a mobile device. The text message is  
10 decoded and a command sent to an application residing on the mobile device, such as a web browser, a text editor, graphic image displayer, a message screen, or a bitmap displayer and/or any other application capable of displaying a notification. The command may, for example, display a pre-stored message or image, instructing the user in regards to returning the device to the authorized user. The application may reside on a hardware component within the mobile  
15 device, such as a SIM card installed in a mobile phone or laptop computer. The message may also be presented at any desired time or in response to any desired event, such as when the current user is attempting to utilize the mobile device (e.g., by placing a call on a mobile telephone). For example, the message may be presented upon startup of the device. In this manner, a user that has found a lost device may obtain information regarding returning the  
20 device even where the device has not established a connection to a host server such as one operated a security authority.

The functionality of the mobile device may be altered to inhibit a user's ability to utilize the mobile device (620). For example, a sequence of DTMF tones (e.g., for a mobile telephone) or an unpleasant sound may be played over a speaker in the mobile device while the current user  
25 is attempting to use the mobile device. Additionally, the illumination level of a display on the mobile device may be altered to frustrate the use of the mobile device (e.g., by decreasing the illumination level) and/or to draw attention to the mobile device (e.g., by increasing the illumination level) so that bystanders may notice the device or its unauthorized use.

A predetermined set of features of the mobile device can be inhibited in response to a  
30 security compromise event, such as when the mobile device is reported stolen or lost by the authorized user. In one embodiment of the present invention, for example, the functionality of the mobile device is modified based on a list of features to be restricted upon occurrence of the security compromise event. The list of features may be defined in any manner, such as by an authorized user accessing a web interface and selecting features to be disabled if the mobile

device is lost or stolen. The list of features may then be transferred to, and stored by, the mobile device. One or more specifically configured lists of features for various security compromise events may be provided to the mobile device, for example one list may indicate that or more of the features on the list could be disabled if the phone is reported stolen, while a less restrictive list may be provided for when the phone is reported as misplaced. In this manner, multiple feature modification lists for the mobile device may provide for event-appropriate responses based on the type of security compromise that has occurred. In another embodiment, a default security compromise action list is executed by the mobile device if the mobile device detects a security compromise event and no other list of restricted features has been transferred to the mobile device by the authorized user or a verified security authority. For example, but not by way of limitation, a default security compromise action list defines common features of a mobile device that need to be altered when control of the mobile device is lost. Alternately, the list of features may be identified by a user through a software interface on the mobile device itself.

The functionality of the mobile device may be modified from a first set of features to a second set of features based on the occurrence of a security compromise event. The differences between the first feature set and second feature set can be based on any desired criteria, such as the context of use of the mobile device. For example, the feature sets may be based on a level of security desired for the mobile device, an application the mobile device is being used for, the location of the mobile device, or any other contextual factor(s).

The functionality of the mobile device may be inhibited in any other desired manner. For example, a mobile phone may be prevented from placing phone calls, sending emails or text messages, or engaging in other forms of communication. In the case where the mobile device comprises a mobile telephone, the phone numbers that may be called from the mobile device can be restricted to a predetermined list of numbers, or to only one or more predetermined numbers within a contact list on the mobile phone. For example, a mobile device may be restricted to only allow emergency calls to be placed, and/or to place a call to a security authority (for example, a user may press a single key to place a call to the security authority). Additionally, DTMF tones can be played on a loudspeaker of the mobile device while the mobile phone is in use to interfere with the current user using the mobile phone. Similarly, frequent messages (e.g. a text message and/or audio message) can be provided, instructing the current user of a mobile device to contact a security authority to initiate return of the mobile device to the authorized user. The subscriber identity module (SIM) of a mobile phone can also be locked out until the user enters a personal unblocking code. The unblocking code may be known to the authorized user(s) prior to the occurrence of the security compromise event, or can be provided to the



authorized user(s) by a security authority. Additionally, an authorized user(s) may unlock the mobile device through a host server such a server operated by a security authority. Any other functions of a mobile device can be disabled (in part or in whole), or interfered with, to diminish the usefulness of the mobile device to an unauthorized user.

5           The functionality of the mobile device can be inhibited by requiring entry of a password before the mobile device may be used by a current user. Where an invalid password is entered, a delay may additionally be introduced before entry of another password may be attempted by the current user. In conjunction with requiring the password, selectable indicia (e.g., a web link and/or button on a display) may be provided that give instructions on how to return the mobile  
10 device. The instructions can be provided without the current user needing to enter a valid user id and password. Additionally, the current user may be prompted to enter his or her identification information, which is stored on the mobile device and transferred to a security authority when the mobile device has an opportunity to make a communications connection to the security authority. This may allow a security authority to locate an innocent finder of the device, as well  
15 as someone who stole the device. For example, but not by way of limitation, the prompt can include a message that notifies the current user of the device that they have won a substantial prize and need to take an action to redeem the prize offer. In such a case, the current user of a device may be solicited to provide information that could be used to redeem the spurious prize, but in fact is used to locate and or apprehend current user. Alternatively, or in combination, the  
20 current user of the mobile device may be sent a graphical image with a name or image that encourages the current user to open a message or file, and while looking at the file or image, a command is decoded from the image via steganographic techniques, whereby the command may be executed by the mobile device to mitigate the loss of control of the mobile device.

          The mobile device can be significantly disabled or entirely shut down to prevent its use  
25 and help prevent an unauthorized user from attempting to circumvent security protections on the mobile device. In some cases, such as when information stored on the mobile device is sensitive, or when there is a very small likelihood of recovering the mobile device (or its data), it may be desirable to command the mobile device to perform a destructive function that renders the mobile device inoperable. The destructive function may include erasing and/or overwriting data  
30 and software stored on the mobile device. The destructive function may also include physically damaging the hardware of the mobile device, such as by commanding the mobile device to deliver an electric charge or current to damage an electronic component of the mobile device.

          The functionality of the mobile device may be altered to send a message to an authorized user of the device, a security authority, or other recipient (630). The message may include any

desired information, such as a phone number called by the mobile device, the current operational status of the mobile device, the location of the mobile device, a statement indicating that the mobile device has been removed from a predetermined location and/or is in motion, a date and time stamp indicating when the device was first used after occurrence of the security event, and/or instructions to call a security authority to initiate a recovery process. The mobile device can thus provide information on its use and location to aid a security authority or authorized user in finding the mobile device.

The authorized user(s) of the mobile device may not necessarily be aware that a security compromise event has occurred. In order to alert an authorized user that a security compromise event has occurred, a theft notification record for an authorized user can be stored at a central server as well as on the mobile device itself to allow the authorized user to be contacted and notified. The theft notification record can include any desired information regarding the authorized user, such as the authorized user's contact information and information that can be used to validate the authorized user's identity. A message to the authorized user may be in any format and may include any desired information. For example, a phone call can be placed to a phone number specified in the theft notification record, whereupon audio instructions (from a live operator or pre-recorded) are provided to the authorized user regarding how to contact the current user of the mobile device to recover the mobile device. Likewise, a text message can be sent electronically, or a printed message may be sent by conventional mail, to an address specified in the theft notification record regarding how to contact the current user of the mobile device to recover it. The message may be provided by any system, device, or individual, such as a security authority monitoring the mobile device and/or the mobile device itself.

The functionality of the mobile device may be altered with regards to the handling of communications to and from the mobile device (640). In addition to prohibiting or restricting communications to and from the device as discussed above, communications from the device by an unauthorized user can be intercepted and forwarded to a security authority, an authorized user, or other recipients to aid in identifying the unauthorized user and the location of the mobile device. In this manner, the present invention will route calls that were directed to the authorized user's lost or stolen device to an alternate number designated by the authorized user; the authorized user will then be able to receive calls that would have otherwise been missed. In the case where the mobile device comprises a mobile telephone, telephone numbers dialed by the unauthorized user can be logged and transmitted to the security authority and/or authorized user, and authorized user and/or security authority can be alerted as the mobile device is engaging in a telephone call. A third party (such as a security authority) may request to access the telephone

call, and then establish a conference connection to the telephone call. The third party may actively participate in the conversation or listen to the conversation surreptitiously.

The data stored on a mobile device may be protected (650) in any desired manner, such as by encryption. Any portion of the stored data may be encrypted, such as files or other data elements designated (e.g., by a list, flag on the file, location of the file, or other method) to be encrypted upon the occurrence of a security compromise event. Alternatively, files and data elements may be encrypted as they are created so that they cannot be viewed by an unauthorized user even before a security compromise event has been determined. An authorized user may designate individual files to be encrypted, as well as types of files to encrypt. In addition to, or as an alternative to, encryption, files may be hidden from the file system of the mobile device to prevent their access by an unauthorized user. Authorized users can gain access to such files through, for example, a software application independent of the operating system of the mobile device that verifies the user is authorized to access the files.

Designated files can be encrypted independent of the mobile device's operating system, such as through an independent software application that encrypts/decrypts files and allows a user to access them. The operating system is thus blocked from accessing such files, preventing an unauthorized user from exploiting security flaws in the operating system to view protected files. Operating system calls to open such files can be intercepted and the files opened and decrypted if the current user is authorized to access the files. Similarly, operating system calls to close such files can be intercepted and the files closed and decrypted by the independent software application. Files stored on the mobile device may be encrypted and decrypted in any desired manner, such as with a password known by a security authority and/or the authorized user.

In one embodiment of the present invention for example, to increase the level of protection for data stored on the mobile device, a password on the mobile device can be modified to utilize a password that is more secure, for example, by using a longer and/or more complex password code, or setting a password where the mobile device was not protected by a password. Normally, these more secure or enhanced-strength passwords are considered less user friendly and are often not used as primary passwords by the authorized users. Therefore, embodiments of the present invention may adaptively modify the strength of passwords on mobile devices depending on the security state and context of a mobile device.

Some or all of the data stored on the mobile device may be erased in response to a security compromise event to protect it from unauthorized access. Any desired files or other data elements can be erased. For example, an authorized user may specify a list of data elements to

be deleted upon occurrence of the security compromise event. Additionally, deleted data elements may be overwritten with other data to prevent forensic recovery of the data. Deleted data may be overwritten any desired number of times, and with any desired data (such as random data, alternating data values, predetermined data patterns, and a combination thereof).

5           Some or all of the data stored on the mobile device may further be archived to allow an authorized user to recover the data, even if the mobile device is not recovered. As with files marked for encryption and/or deletion, an authorized user may specify particular files or other data to be archived in any desired manner. The authorized user may also specify one or more destinations to which the archived data should be transmitted to in the event of a security  
10 compromise event, such as a security authority, host server, or an alternate device accessible by the authorized user (e.g., another mobile device of the same type or a central data server). The archived data may be transmitted from the mobile device to a specified destination in conjunction with the encryption or deletion of the data upon a successful transfer. An authorized user may then retrieve the archived data to a replacement mobile device, or may instruct that the  
15 archived data be delivered to any other desired destination. For example, the authorized user may specify a destination address (such as an email address or physical mailing address) to which an electronic copy or physical copy (e.g., the archived data stored on a portable storage medium) can be delivered. Any type of data stored on the mobile device may be archived, such as documents, email or telephone contact information, software applications, media files, and/or  
20 pictures. Additionally, licensing information pertaining to one or more data elements may be archived.

          Data may be archived at any time, including, upon occurrence of a security compromise event, according to a predetermined schedule, and or at a time specified by an authorized user, security authority, or other authorized entity.

25           Systems and methods of the present invention may store sensitive data in a specified location for special processing upon the occurrence of a security compromise event. The specified location may be a physical location in a memory, as well as a location designated through the file system of the mobile device. For example, an authorized user may store sensitive data elements in a special folder on the file system of the mobile device. When a  
30 security compromise event occurs, one or more functions can be executed on the data elements within the folder, such as encrypting one or more of the sensitive data elements with a password known to the authorized user and/or a security authority, deleting one or more of the sensitive data elements, multiply overwriting one or more of the sensitive data elements, and/or transmitting one or more of the sensitive data elements to an address specified by the authorized

user. The special designation of files allows, among other things, important data to be quickly protected, archived, and/or destroyed before handling less sensitive data in the event of a security compromise event.

5 The functionality of the mobile device may be altered to aid in tracking the device (660) following the occurrence of a security compromise event. For example, the mobile device may determine a network address (including a wireless network address) assigned to the mobile device, as well as wireless access point identifiers from signals received by the mobile device. The mobile device can store and transmit the address(es) and identifier(s) to a security authority. The security authority may then determine, based on the network addresses and wireless access  
10 point identifiers, a location of the mobile device.

Similarly, the mobile device may receive a signal from a GPS or other source providing geolocation information. The geolocation information from the signal can be stored and transmitted to a security authority. A security authority or authorized user receiving location information from the mobile device can present the location on a map overlay to track the current  
15 position of the mobile device, as well as the date and time of any changes in the mobile device's position. The map of the mobile device's position can be provided through a web site over the Internet to allow police officers or other security authority members to locate the mobile device.

The functionality of a mobile device may be altered to gather information on how the mobile device is being used by an unauthorized user and provide that information to an  
20 authorized user or security authority to aid in locating the device and/or unauthorized user (670). For example, phone numbers and email addresses to which messages are sent after occurrence of the security compromise event may be stored by the mobile device and transmitted to a security authority. Data-capturing equipment onboard a mobile device (such as a digital camera or microphone) can also be used to gather information on the user of the mobile device, mobile  
25 device's present environment. A camera in communication with the mobile device, for example, can be activated to capture a still image or video clip, which can be stored in the mobile device and transmitted to a security authority. Similarly, a microphone may be used to capture audio clips. Data-capturing equipment such as the camera and microphone can be used to take continuous samples of data to help locate the device, inhibit use of the data capture device by the  
30 unauthorized user, and/or to wear down the battery of the mobile device to diminish its usefulness to the unauthorized user. Alternately, the data capture device may be disabled to preserve battery life and/or to prevent its use by the unauthorized user.

In order to help capture an image of the face of an unauthorized user, the mobile device may prompt the user to undertake an activity that involves looking at the mobile device, such as

prompting the user to enter a password, playing an audio sequence on the mobile device, strobing a light source on the mobile device, announcing that the current user has won a prize and instructing him/her to watch for prize redemption details, and/or displaying a video sequence. While the current user's attention is focused on the mobile device, the camera may be used to capture an image of his/her face for transmittal to a security authority. Similarly, a camera or microphone in communication with the mobile device can be activated in conjunction with initiating a surreptitious communication session with a security authority. Still images, video, and audio data captured by the mobile device can then be transmitted to the security authority. The security authority can use images/video of the unauthorized user to identify him/her (e.g., through comparing the images/video to police booking photos), and can also use the images/video to identify the surroundings of the mobile device. The unauthorized user may also be identified from samples of the unauthorized user's voice (taken from captured audio clips).

As discussed previously, messages sent to and from the mobile device may be intercepted and/or rerouted to a security authority to prevent unauthorized use of the device and to help identify an unauthorized user and/or the location of the mobile device. In addition, the mobile device may be configured to maintain a record of each key depressed on the mobile device, and transmit that log to an authorized user or security authority. The logging of keystrokes in this manner may further aid in identifying the unauthorized user by capturing usernames, passwords, contact entries, and other information entered by the unauthorized user.

In addition to passively receiving data from the mobile device, an authorized user or security authority may actively access or command the mobile device in accordance with the present invention. A security authority or authorized user may transmit commands to the mobile device to execute various functions, as well as to provide software updates, applets, sections of executable code, interpretable scripts, or data elements to be processed by the mobile device. The mobile device may thus be provided with software to perform various tasks upon the occurrence of a security compromise event, as well as at any other desired time.

In one exemplary embodiment of the present invention, a security authority and/or the authorized user may log into a remote access service configured to communicate with the mobile device and activate an application programming interface in the mobile device to forward to the remote access service the current status of the mobile device, the current location of the mobile device, an image taken by a camera in communication with the mobile device, a real-time video captured by a camera in communication with the mobile device, a list of keys pressed on the mobile device, and/or a list of services currently running on the mobile device. Additionally, an

authorized user or security authority may issue a command to the mobile device to initiate a chat session and provide an interface on the mobile device for enabling a text-based interaction with the current user.

5 The functionality of the mobile device may be altered to communicate with other devices to assist in locating and recovering the mobile device (680). For example, referring now to Figure 7, communication with other devices (680) may include initiating a wireless connection between the mobile device and a wireless transceiver (710), relaying information regarding the current location of the mobile device to a security authority through the wireless transceiver (720), transmitting a message to the wireless transceiver (730), and transmitting a message to a  
10 second wireless transceiver (740).

A mobile device can initiate a connection between any device, system, or person through a wireless transceiver, and may connect to the wireless transceiver using any desired communication protocol. The mobile device may connect to any number of wireless transceivers. Once connected to a wireless transceiver, the mobile device may relay any desired  
15 information regarding the current location of the mobile device to a security authority, as well as files and data stored on the mobile device. For example, a mobile device that initiates a connection with a wireless access point (WAP) connected to the Internet may send an email to a security authority that includes text and attachments to aid the security authority in locating the device and apprehending an unauthorized possessor of the device. Similarly, a mobile device  
20 initiating a connection with a cellular telephone network may dial the security authority and provide information regarding the location of the mobile device through an audio message and/or DTMF tones.

The mobile device can provide any other desired information to (or through) a wireless transceiver it initiates contact with. For example, in one embodiment of the present invention the  
25 mobile device can transmit a message to a wireless transceiver indicating that a lost or stolen device is present within a signal range accessible by the wireless transceiver. Similarly, a mobile device may determine the signal strength of its wireless connection with the wireless transceiver, and obtain identifying indicia (such as a device name, IP address, or other identifier) for the wireless transceiver and transmit a message to a different wireless transceiver including the  
30 identification and signal strength information. The signal strength and identification information for multiple wireless transceivers can then be used to triangulate the location of the mobile device. Additionally, where the wireless transceiver (or device in communication thereto) is capable of determining its own physical location, the mobile device may request that the

wireless transceiver provide its physical location, which in turn can be provided to a security authority.

The mobile device may transmit any other desired information to any number of wireless transceivers. In one embodiment of the present invention, for example, a message to a wireless transceiver may include a request for a response that includes the physical location of a wireless transceiver in communication with the mobile device, a request that a person in communication with the wireless transceiver report that a lost or stolen device is within its communication range, a phone number for the authorized user, a phone number for a security authority, and/or a request to place a call to a security authority.

#### 10 EXEMPLARY SYSTEM

An exemplary system for use in conjunction with the present invention is depicted in Figure 8. This system may be used in conjunction with the methods described in Figure 1-7, as well as with any subset or combination of the elements thereof. The system shown in Figure 8 may also be used in conjunction with any other suitable embodiments of the present invention.

15 The exemplary system depicted in Figure 8 comprises a mobile device 800 that includes a processor 810 coupled to a memory 820 which may include volatile memory, nonvolatile memory or a combination thereof. A communications module 830 comprises a wireless transceiver 840 for wirelessly communicating with one or more servers 860 and other entities through antenna 850. The mobile device also includes a user interface 870 coupled to the processor 810. The mobile device 800 may include any suitable power source, such as a battery (not shown). The mobile device 800 may include any other desired components, such as a global positioning system (GPS) to provide geolocation information for locating the mobile device. Some or all of the components of the mobile device 800 may include (or be in communication with) a hardware identification module (not shown) such as a universal subscriber identity module and/or removable user identity module. The hardware identification module may be coupled to the processor 810 and may include an identifier that can be compared to a predetermined identifier to determine whether the hardware of the mobile device 800 has been altered and whether a security compromise event has occurred as a result. The hardware identification module (and predetermined identifier) may include any suitable identifier, such as an electronic serial number, a local area identity identifier, an integrated circuit identifier, an international mobile subscriber identifier, an authentication key identifier, and/or an operator-specific emergency number identifier. The identifier may be stored in the memory 820 and transmitted to the host server 860 for comparison to a predetermined identifier.

20  
25  
30



The functionality of the mobile device 800, including the methods depicted in Figures 1-7 (in whole or in part), may be implemented through the processor 810 executing computer-readable instructions stored in the memory 820 of the mobile device 800. The memory 820 may store any computer-readable instructions and data, including software applications, applets, and embedded operating code. In one exemplary embodiment, a software application performing methods of the present invention includes a terminate and stay resident (TSR) application (or equivalent) configured to remain loaded in memory whenever the mobile device is in operation, which can help prevent the inadvertent or intentional deletion of the TSR. The software application may also be hidden (i.e., not viewable in an application list or task list) and/or protected from being stopped or deleted by a user or other software process. Aspects of embodiments of the present invention provide for tamper-resistant applications to prevent unauthorized users from disabling or otherwise removing the applications from operational status. In one exemplary embodiment, applications may be installed on mobile devices running the Symbian operating system, whereby applications that are running may not be unloaded or disabled.

Additionally, the software application may be configured to operate with minimal underlying hardware functionality. For example, the application may be initiated before the mobile device establishes a network connection. Such a situation may be provided, for instance, when the software application is installed on a SIM card in the mobile device, and the application launches before other software in the mobile device operating system. Alternately or in addition, a data element such as a link or a URL (universal resource locator) may reside on the SIM card, and by launching an application such as a browser with the URL or link, an application referenced by the link or URL may be loaded into the mobile device from a remote server and/or executed directly from on the remote server.

Software performing methods of the present invention may be provided with the device or downloaded onto the mobile device by an authorized user. The functionality of the mobile device 800 may also be implemented through various hardware components storing machine-readable instructions, such as application-specific integrated circuits (ASICs), field-programmable gate arrays (FPGAs) and/or complex programmable logic devices (CPLDs). Systems according to aspects of the present invention may operate in conjunction with any desired combination of software and/or hardware components.

The processor 810 retrieves and executes instructions stored in the memory 820 to control the operation of the mobile device 800. Any number and type of processor such as an integrated circuit microprocessor, microcontroller, and/or digital signal processor (DSP), can be

used in conjunction with the present invention. The memory 820 stores instructions, data, messages transmitted from (or received by) the mobile device 800, and any other suitable information. A memory 820 operating in conjunction with the present invention may include any combination of different memory storage devices, such as hard drives, random access  
5 memory (RAM), read only memory (ROM), FLASH memory, or any other type of volatile and/or nonvolatile memory. Data can be stored in the memory 820 in any desired manner. In one embodiment of the present invention, for example, data stored within the memory 820 is partitioned into one or more logically disjoint groups. Each of the data groups are encrypted with a respective unique encryption key to prevent all the data on the mobile device from being  
10 accessed if a single encryption key is compromised. This also increases the time it will take a “brute force” attempt to try all possible encryption keys to succeed. The groups of data can be partitioned across a plurality of physical storage media, such a RAID array.

The communications interface 830 communicates with one or more servers 860 or other suitable entities. Any suitable communications device, component, system, and method may be  
15 used in conjunction with the present invention. For example, the wireless transceiver 840 may be configured to communicate using any number and type of cellular protocols, such as General Packet Radio Service (GPRS), Global System for Mobile Communications (GSM), Enhanced Data rates for GSM Evolution (EDGE), Personal Communication Service (PCS), Advanced Mobile Phone System (AMPS), Code Division Multiple Access (CDMA), Wideband CDMA  
20 (W-CDMA), Time Division-Synchronous CDMA (TD-SCDMA), Universal Mobile Telecommunications System (UMTS), and/or Time Division Multiple Access (TDMA). A mobile device operating in conjunction with the present invention may alternatively (or additionally) include wireless transceiver(s) (and related components) to communicate using any other method of wireless communication protocol, such as an ISO 14443 protocol, an ISO  
25 18000-6 protocol, a Bluetooth protocol, a Zigbee protocol, a Wibree protocol, an IEEE 802.15 protocol, an IEEE 802.11 protocol, an IEEE 802.16 protocol, an ultra-wideband (UWB) protocol; an IrDA protocol, and combinations thereof. The antenna 850 may be configured to transmit and receive any wireless signal in any format, and may comprise a plurality of different antennas to transmit and receive using different wireless protocols.

30 The communications module 830 can communicate with the server 860 or another device using any other form of connection, such as a wired Internet connection, a wireless Internet connection, a cellular telephone network connection, a wireless LAN connection, a wireless WAN connection, an optical connection, a USB connection, a mobile device synchronization port connection, a power connection, and/or a security cable. The communications module 830

can be used to communicate with one or more companion devices to monitor the position or status of the mobile device 800 (e.g., by monitoring whether a communication link between the mobile device and companion device is intact), as well as with any number of other devices to help track/locate a lost or stolen mobile device 800.

5           The mobile device 800 includes a user interface 870. The user interface 870 may include any number of input devices (not shown) to receive commands, data, and other suitable input from a user, as well as any number of output devices (not shown) to provides the user with data, notifications, and other suitable information from the mobile device 800.

10           Any number of input devices may be included in the user interface 870 such as a touch pad, a touch screen, and/or an alphanumeric keypad to allow a user to enter instructions and data into the mobile device 800. The user interface 870 may be configured to detect pressure exerted by a user on the keys of a keypad, as well as the time interval between key presses in order to determine if the current user is authorized to use the device. The user interface may also include a microphone to allow the user to provide audio data to the mobile device 200, as well as a  
15           camera to allow the mobile device to capture still or video images. The mobile device 200 may include speech recognition software to process verbal input through the user interface 870. The user interface 870 may also include any number of suitable output devices, such as a display screen to visually display information (such as video and text), and/or a speaker to provide auditory output. The mobile device 800 may be configured to provide words, phrases, tones,  
20           recorded music, or any other type of auditory output to a user through the speaker. As discussed previously, the user interface 870 can be activated to provide information and/or hinder the operation of the mobile device 800 when an unauthorized user attempts to use the mobile device 800. For example, the illumination level of the display may be modulated to draw attention to the mobile device, and unpleasant and/or loud sounds can be played over the speaker.

25           The mobile device 200 may include one or more biometric devices configured to receive biometric information, such as a fingerprint scanner, an iris scanner, a retinal scanner, and/or a breath analyzer. Input devices such as a microphone or camera may also be utilized to perform biometric analyses, such as a voice analysis or facial recognition.

30           Information provided or received by the user interface 870 may be in any appropriate format. For example, a user interface that communicates information to a user in an auditory format may first provide a data header followed by a data value to identify the data to the user. The user interface 870 may provide information in any number of desired languages, regardless of whether the information is provided audibly or visually.

The user interface can also provide/receive information to a user in a machine-readable format. In one exemplary embodiment of the present invention, for example, the user interface 870 of a mobile device 800 may send and receive messages using dual-tone multi-frequency (DTMF) tones. The mobile device 800 can be configured to send, receive, and process machine-readable data in any standard format (such as a MS Word document, Adobe PDF file, ASCII text file, JPEG, or other standard format) as well as any proprietary format. Machine-readable data to or from the user interface may also be encrypted to protect the data from unintended recipients and/or improper use. In an alternate embodiment, a user must enter a passcode to enable use of some or all of the functionality of the mobile device 800. Any other user interface feature may be utilized to allow a human or non-human user to interact with one or more devices operating in conjunction with the present invention.

The mobile device 800 may include any other suitable features, components, and/or systems. For example, the mobile device 800 may be configured to preserve the life of its battery by shutting off some or all of its components, such as a camera or microphone. Components can be selectively shut down in response to a security compromise event, as well as in response to a command from an authorized user or security authority. Alternately, the mobile device 800 can be configured to use its components excessively to drain the battery as quickly as possible, to, for example, limit the usefulness of the mobile device 800 to an unauthorized user.

The mobile device 800 may be configured to implement one or more security measures to protect data, restrict access, or provide any other desired security feature. For example, a mobile device 800 may encrypt transmitted data and/or data stored within the device itself. Such security measures may be implemented using hardware, software, or a combination thereof. Any method of data encryption or protection may be utilized in conjunction with the present invention, such as public/private keyed encryption systems, data scrambling methods, hardware and software firewalls, tamper-resistant or tamper-responsive memory storage devices or any other method or technique for protecting data. Similarly, passwords, biometrics, access cards or other hardware, or any other system, device, and/or method may be employed to restrict access to any device operating in conjunction with the present invention.

The host server 860 communicates with mobile devices 200, authorized users, unauthorized users, security authorities, and other entities to monitor and protect the mobile devices 200 from unauthorized use and to mitigate the harm associated with a security compromise event. The host server 860 may comprise any number of separate computer systems, processors, and memory storage devices, as well as human operators (e.g., to answer calls from authorized users reporting the loss/theft of a mobile device) and any other suitable

entity. The host server 860 may include, or be in communication with, one or more databases 880 storing information regarding authorized users and mobile devices 200 in order to monitor and track the mobile devices 200 and provide instructions to the mobile devices 200 in the event a security compromise event occurs.

5 For example, a database 880 may store a usage profile for a mobile device to allow software on the host server 860 to detect whether continued usage of the mobile device deviates from the usage profile by a predetermined threshold. The host server 860 may also receive, process, and store (e.g., in the database 880) information from the mobile device 800. The host server 860 may handle any type of data in any format to achieve any purpose, such as receiving  
10 and processing environmental parameters captured by the mobile device to track the position and location of the mobile device 800 as discussed previously. The database 880 may also store location information that can be used to determine whether the mobile device 800 is operating in a valid location (e.g., “whitelisting” and “blacklisting” as discussed previously).

Databases 880 in communication with the host server 860 may also store archived data  
15 from mobile devices 800 for recovery in the event the mobile devices 800 are lost or stolen, or the data on the mobile devices 800 is destroyed (e.g., by a virus or other malicious program). The functionality of the host server 860 may be performed automatically or semi-automatically, such as through software/hardware operating on one or more computer systems, and/or by one or more human operators.

20 The host server 860 may include one or more system processors that retrieve and execute computer-readable instructions stored in a memory to control (at least partially) the operation of the host server 860. Any number and type of conventional computer, computer system, computer network, computer workstation, minicomputer, mainframe computer, or computer processor, such as an integrated circuit microprocessor or microcontroller, can be used in  
25 conjunction with the present invention. Computer systems used in accordance with aspects of the present invention may include an operating system (e.g., Windows NT, 95/98/2000/XP/Vista, OS2, UNIX, Linux, Solaris, MacOS, etc.) as well as various conventional support software and drivers typically associated with computers. In certain embodiments, dedicated applications may be entirely or partially served or executed by the system processor to perform methods of  
30 the present invention

The host server 860 may be accessed in any desired manner, such as through a website on the Internet, and/or through a telephone network. The host server 860 may include any number of human operators, computer systems, mobile telephones, mobile computing devices, interactive voice response (IVR) systems, and any other suitable system and device for

communicating with a user, security authority, computing device, or other entity. In one exemplary embodiment of the present invention, authorized users wishing to subscribe to a service providing monitoring and protection of their mobile devices can access a web site hosted by the host server 860 to create an account, pay for the service, identify one or more mobile devices to be protected, select options for the service, identify how the functionality of the device should be altered (e.g. features to implement or restrict ) in the event the mobile device is lost or stolen, select an alternate caller identification indicia such as text to delivered in a caller ID data stream, report a security compromise event (such as the loss/theft of the device), and/or download software to operate on their mobile device to aid in monitoring and protecting the mobile device. Alternately, authorized users may interface with an automated IVR system and/or human operator over a telephone network. In the event a mobile device is lost or stolen, authorized users may interface with the host server 860 to report the security compromise event (i.e., the loss/theft of the device), track the status/location of the mobile device, recover data archived from the mobile device and stored by the host server 860, and/or to provide information on a security compromise event (such as reporting that the device has been located by the authorized user). Communications to and from the host server 860 may be protected (e.g., through encryption) as discussed above, or in any other manner.

The host server 860 can communicate with unauthorized users of a lost or stolen mobile device, both through the mobile device or through other communication methods. The host server 860 may notify the unauthorized user that the mobile device is lost or stolen, provide recovery information (such as a shipping address) to the unauthorized user, and facilitate the delivery of a reward to an unauthorized user who returns the mobile device. The host server 860 also communicates with the mobile device 800 to provide software updates, receive data for archival, identify files and other data to be protected, and to perform any other aspect of the present invention.

The host server 860 may be controlled by, or operate in conjunction with, an authorized user, telecommunications service provider, mobile device monitoring/tracking service provider, security authority, and/or any other desired entity. For example, authorized users and security authorities may communicate with or through the host server 860 to monitor a mobile device 800 and to recover the mobile device 800 if it is lost or stolen. The host server 860 may be configured to provide notifications on how to return a lost/stolen mobile device 800, detect a security compromise event, and determine whether a mobile device's functionality should be altered and (if so) determine the manner in which the functionality of the mobile device 800 should be altered, as depicted in Figures 1-7 and discussed previously. The host server 860 may

operate in conjunction with any other desired systems, devices, human operators, or other entities.

### OPERATION

5 Figures 9-64 depict various aspects of the operation of exemplary embodiments according to the present invention. Figures 9-16 depict exemplary notification measures that can be provided on a mobile computing device such as a laptop computer in accordance with the present invention. As shown in the illustrated embodiments, a notification icon or graphic is provided in proximity to input fields where users normally log in to access the mobile computing device. The notification icon or graphic is accompanied by text providing information regarding  
10 returning of the device. The various notification messages allow a finder of the mobile device to see that the device is protected by an application operating in conjunction with the present invention as well as to provide information to allow the user to return the device. For example, referring now to Figure 13, screen 1300 provides a link to a website that an innocent finder can click on to return the device. Similarly, referring now to Figure 14, screen 1400 provides entry  
15 fields for a finder of the device to enter his or her name, phone number, and email address, and submit this information to a security authority. Screens 1500 and 1600 in Figures 15 and 16 respectively, provide a toll-free phone number and information regarding how to return the mobile device.

20 Figures 17-25 depict exemplary notification messages that may be displayed on a cellular phone, a PDA, or handheld mobile device. The notification messages alert the finder of the mobile device that the device is protected by an application operating in conjunction with the present invention as well as to provide information to allow the user to return the device. For example, referring now to Figures 18 and 22, the notification message may include buttons the user may select to return the mobile device. Figures 19, 20, and 21 depict notification messages  
25 that may be displayed when a user of a found mobile device places a call, such as to a security authority. Referring to Figure 23, the notification message may include an identification number associated with the mobile device as well as any other desired information.

A user of a mobile device protected in accordance with the present invention may interface with a host server such as one administered by a security authority through a website.  
30 Figures 26-37 depict exemplary screens and processes associated with a host server as exemplified by embodiments of the present invention. A user may be given an opportunity to sign up for a service to protect one or more mobile computing devices in accordance with the present invention (Figures 26-34). After a user has created an account, he/she may download a software application to the mobile device to be protected, as depicted in flow diagram 2900 in

Figure 29. The user is thus provided with information regarding installation and user of the security application (Figure 30). Referring to Figure 31, after the user has downloaded and installed the product and has restarted the mobile device (if necessary), once a network connection is available the application will launch a browser to a web page using a unique identifier such as an identifier tag previously obtained from the host server. As shown in Figures 32-33, a summary of the registration information is also presented to the user through the browser screen, and the screen may present a list of multiple devices protected by the service.

A user may be given an opportunity to sign up for a service to protect one or more mobile devices in accordance with the present invention. Figure 34 illustrates an exemplary process for creating an account and registering a mobile device in accordance with the present invention. A user creates an account (Figure 35), selects a mobile device (Figure 36), and completes the registration (Figure 37).

Figures 38-55 pertain to the installation and registration of a software application downloaded onto the mobile device. The user initiates an installation program (Figure 38), agrees to a license agreement (Figure 39), selects a destination in the file system of the mobile device for the software application (Figure 40), and confirms installation of the software application (Figure 41). The installation verifies that the software application installs properly, and if not, reinitiates the installation program (Figures 42-47). The user registers the software application with the host server (Figures 48-57). A finder of a mobile device protected in accordance with the mobile device may be directed to a web page hosted by the host server, which allows the finder to report that the mobile device has been found (Figure 58). If desired, an authorized user may uninstall the application from the mobile device (Figure 59-64).

The particular implementations shown and described above are illustrative of the invention and its best mode and are not intended to otherwise limit the scope of the present invention in any way. Indeed, for the sake of brevity, conventional data storage, data transmission, and other functional aspects of the systems may not be described in detail. Methods illustrated in the various figures may include more, fewer, or other steps. Additionally, steps may be performed in any suitable order without departing from the scope of the invention. Furthermore, the connecting lines shown in the various figures are intended to represent exemplary functional relationships and/or physical couplings between the various elements. Many alternative or additional functional relationships or physical connections may be present in a practical system.



Changes and modifications may be made to the disclosed embodiments without departing from the scope of the present invention. These and other changes or modifications are intended to be included within the scope of the present invention, as expressed in the following claims.

**WHAT IS CLAIMED IS:**

1. A method comprising:  
providing, by a mobile device, a notification describing how to return the mobile device to an authorized user;
- 5        detecting, by the mobile device, that a security compromise event has occurred; and  
determining whether the function of the device should be altered in response to said security compromise event.
2. The method as disclosed in Claim 1, wherein detecting that a security compromise event has occurred further comprises detecting that a SIM card associated with the mobile device has  
10        been exchanged.
3. The method as disclosed in Claim 1, wherein detecting that a security compromise event has occurred further comprises detecting that a SIM card associated with the mobile device has been removed from the mobile device.
4. The method as disclosed in Claim 1, wherein detecting that a security compromise event  
15        has occurred further comprises:  
obtaining from the authorized user a set of criteria indicating unauthorized use of the mobile device; and  
determining that at least one of the criteria indicating unauthorized use has occurred.
5. The method as disclosed in Claim 4, wherein the criteria indicating unauthorized use of  
20        the mobile device comprise at least one of:  
a maximum number of calls that may be placed to numbers not included in a pre-stored authorized number list;  
a maximum number of calls that may be received by numbers not included in the pre-stored authorized number list; and  
25        a call being placed to a country code not included in the pre-stored authorized number list.
6. The method as disclosed in Claim 1, wherein detecting, by the mobile device, that a security compromise event has occurred further comprises:  
associating the mobile device with a companion device; and  
30        determining that the mobile device has been moved relative to the location of the companion device.
7. The method as disclosed in Claim 6, further comprising:

formatting a message for transmission to a security authority, the message comprising regarding movement of the mobile device with respect to the companion device; wherein the message is formatted by the companion device.

8. The method as disclosed in Claim 1, wherein detecting, by the mobile device, that a security compromise event has occurred further comprises:
- 5 associating the mobile device with a companion device; and  
determining that the mobile device has been disassociated from the companion device.
9. The method as disclosed in Claim 8, further comprising:
- 10 formatting a message for transmission to a security authority, the message comprising information regarding the disassociation of the mobile device with the companion device; wherein the message is formatted by the companion device.
10. The method as disclosed in Claim 8, wherein associating the mobile device with a companion device further comprises pairing the mobile device with a companion device via at least one of a wired link and a wireless link.
- 15 11. The method as disclosed in Claim 10, wherein the wired link is implemented with at least one of a computer network connection, a USB connection, a mobile device synchronization port connection, a power connection, and a security cable.
12. The method as disclosed in Claim 11, wherein determining that the mobile device has been disassociated from the companion device comprises determining that a connection  
20 between the wired link and the mobile device has been severed.
13. The method as disclosed in Claim 8, wherein determining that the mobile device has been disassociated from the companion device comprises:
- measuring a current power level of a wireless signal transmitted by the companion  
device; and
- 25 determining that the measured current power level has decreased below a predetermined threshold level.
14. The method as disclosed in Claim 8, wherein determining that the mobile device has been disassociated from the companion device comprises:
- measuring a current power level of a wireless signal transmitted by the companion  
30 device; and
- determining that the measured current power level has decreased by a predetermined amount.
15. The method as disclosed in Claim 8, wherein determining that the mobile device has been disassociated from the companion device comprises:

measuring a plurality of power levels of a wireless signal transmitted by the companion device;

computing an average power level from the plurality of measured power levels;

measuring a current power level of a wireless signal transmitted by the companion

5 device;

determining that the measured current power level has varied from the average power level by a predetermined amount.

16. The method as disclosed in Claim 15, wherein determining that the measured current power level has varied from the an average power level by a predetermined amount further

10 comprises:

computing a standard deviation of the plurality of measured power levels; and

determining that the current power level exceeds an allowed signal range determined by a predetermined constant times the standard deviation of the plurality of measured signals.

15 17. The method as disclosed in Claim 16, wherein the predetermined constant is 1.

18. The method as disclosed in Claim 8, wherein determining that the mobile device has been disassociated from the companion device comprises:

measuring a plurality of power levels of a wireless signal transmitted by the companion device;

20 computing an average power level from the plurality of measured power levels;

measuring a plurality of current power levels of a wireless signal transmitted by the companion device;

25 determining that for a predetermined number of times within a predetermined time period, one of the plurality of current power levels has varied from the average power level by a predetermined amount.

19. The method as disclosed in Claim 8, wherein determining that the mobile device has been disassociated from the companion device comprises transmitting a message to the companion device and determining that a message was not received from the companion device that satisfies a predetermined confirmation criterion.

30 20. The method as disclosed in Claim 8, wherein determining that the mobile device has been disassociated from the companion device comprises determining that an amount of incident light illuminating at least one surface of the mobile device has varied from a predetermined threshold range.

1/64

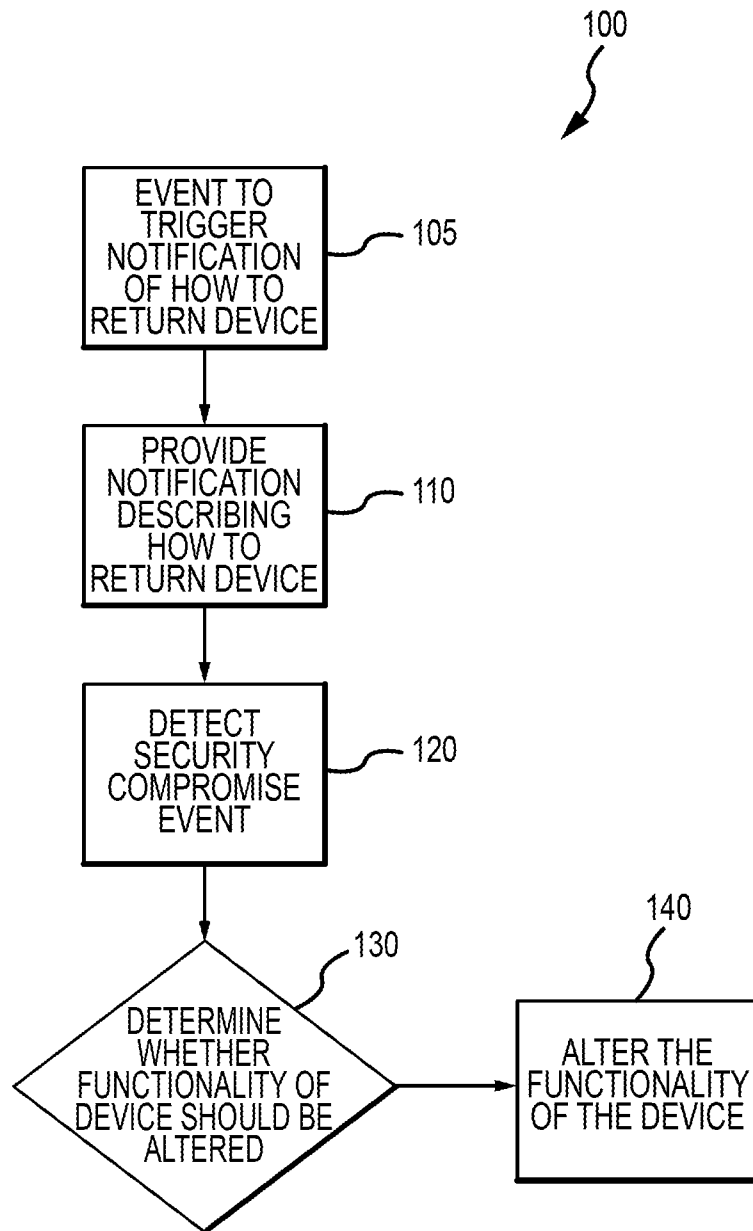


FIGURE 1

2/64

110  
↙

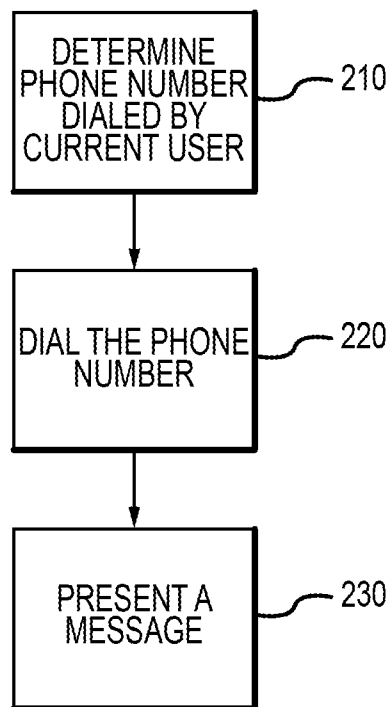


FIGURE 2

3/64

120  
↙

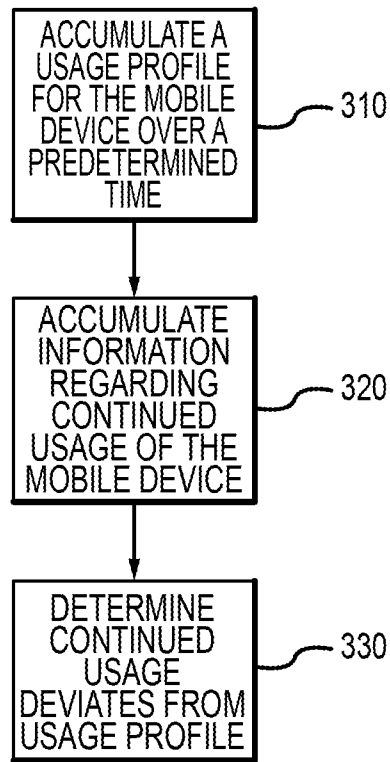


FIGURE 3

4/64

120  
↙

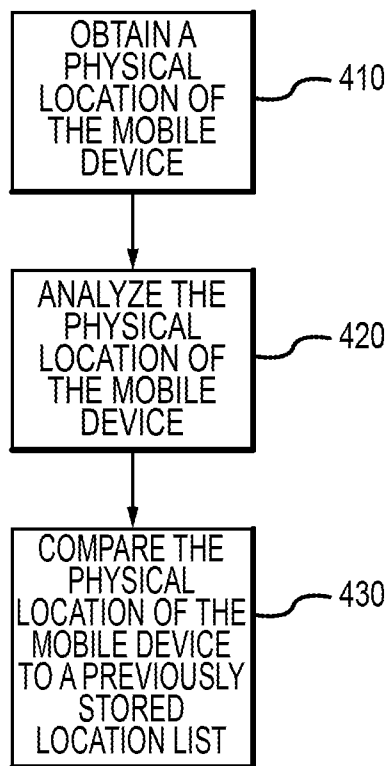


FIGURE 4



5/64

120

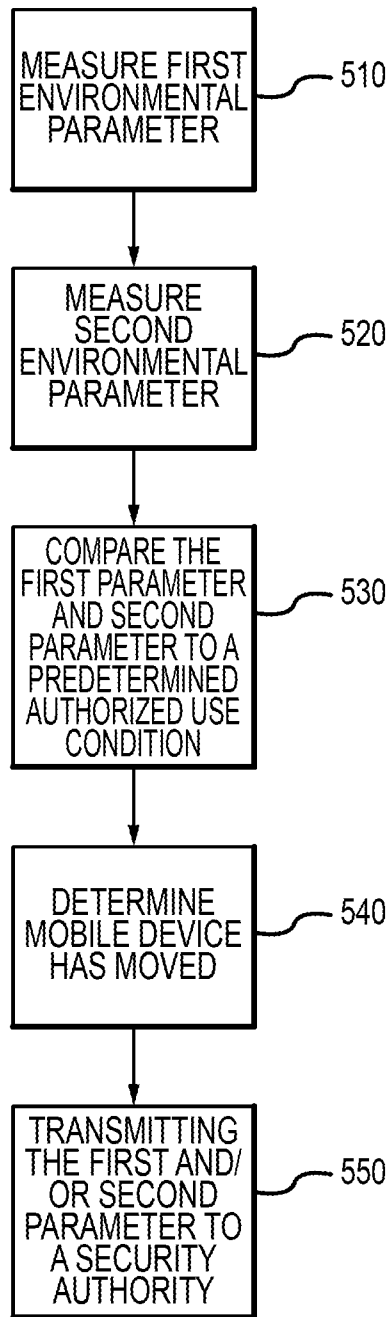


FIGURE 5

6/64

140  
↙

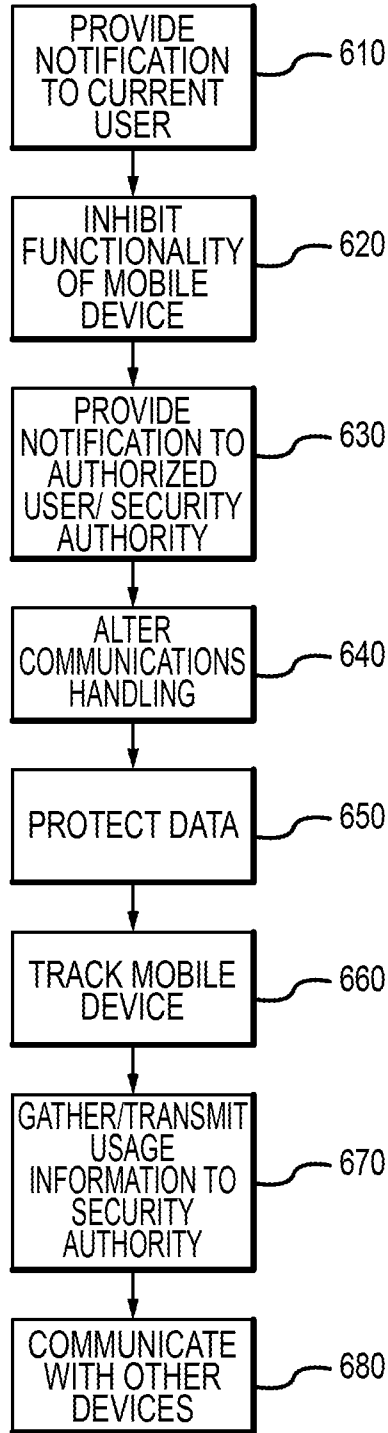


FIGURE 6

7/64

680

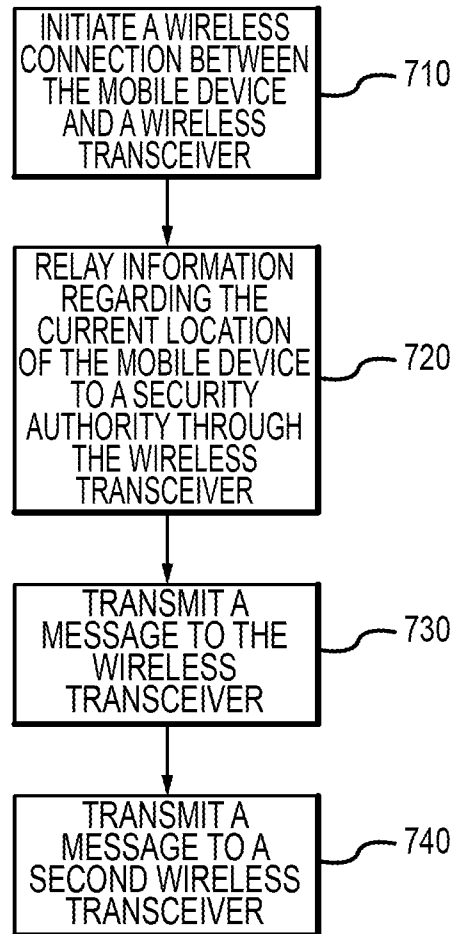


FIGURE 7

8/64

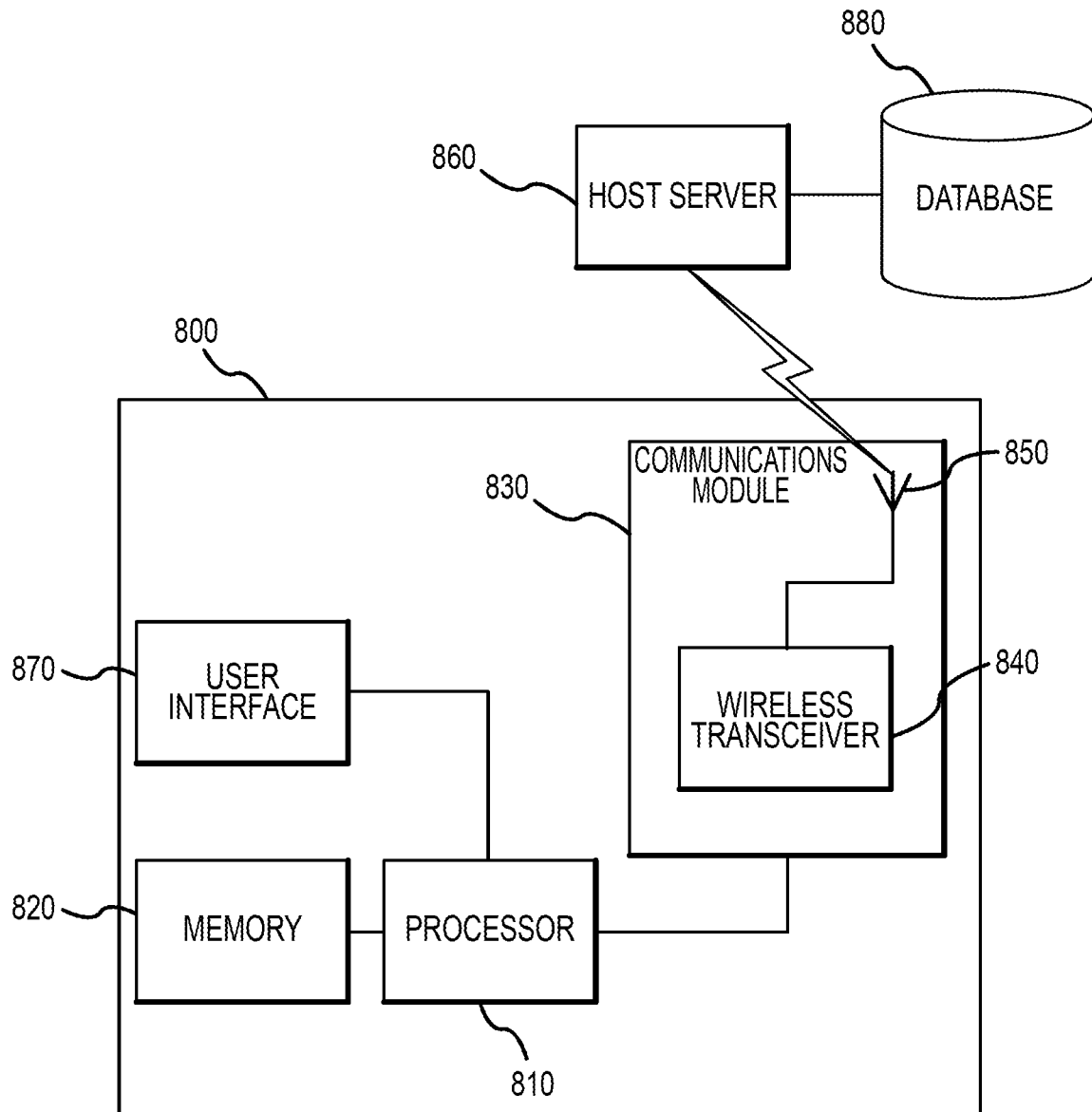


FIGURE 8

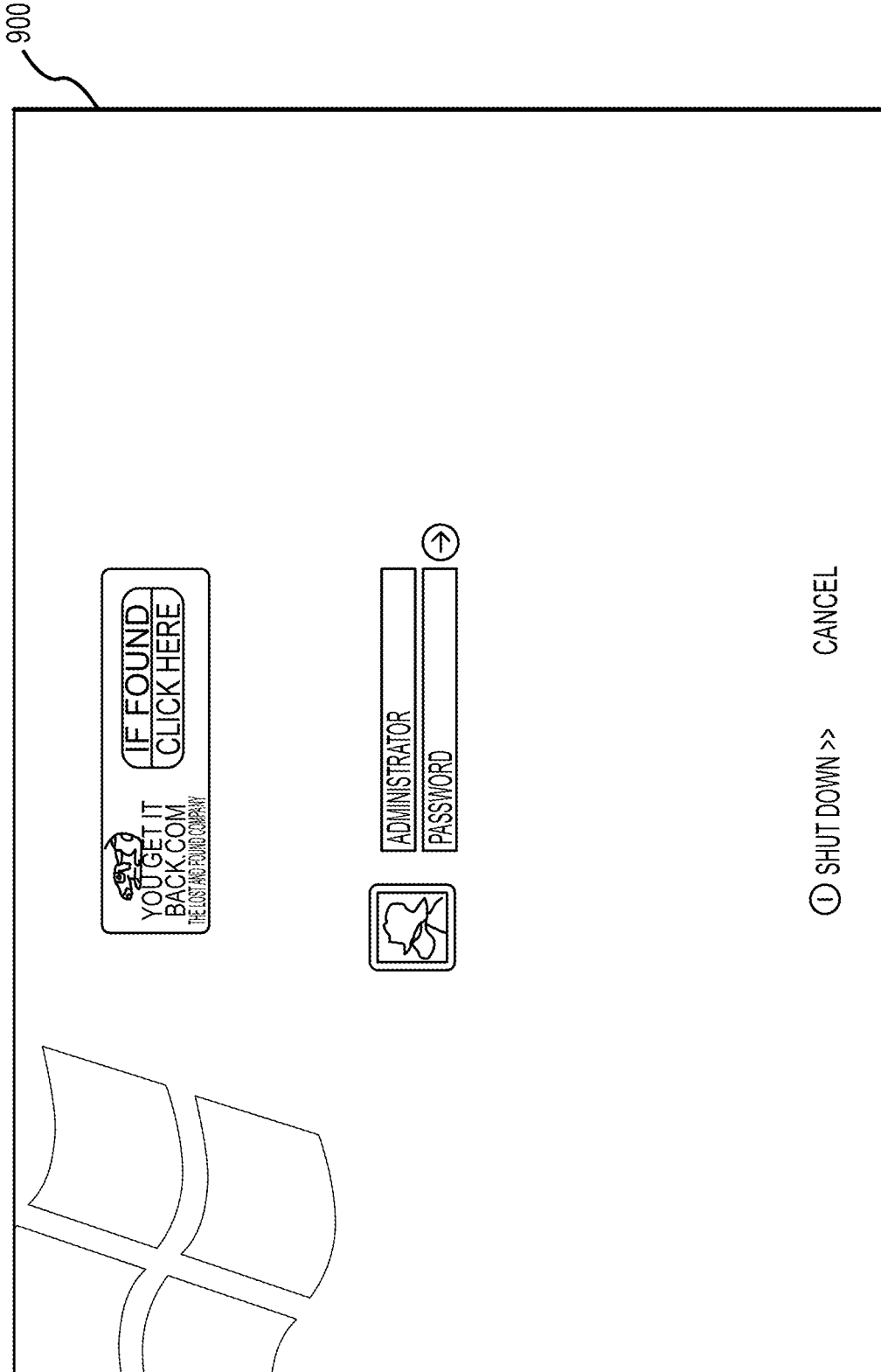


FIGURE 9

1000

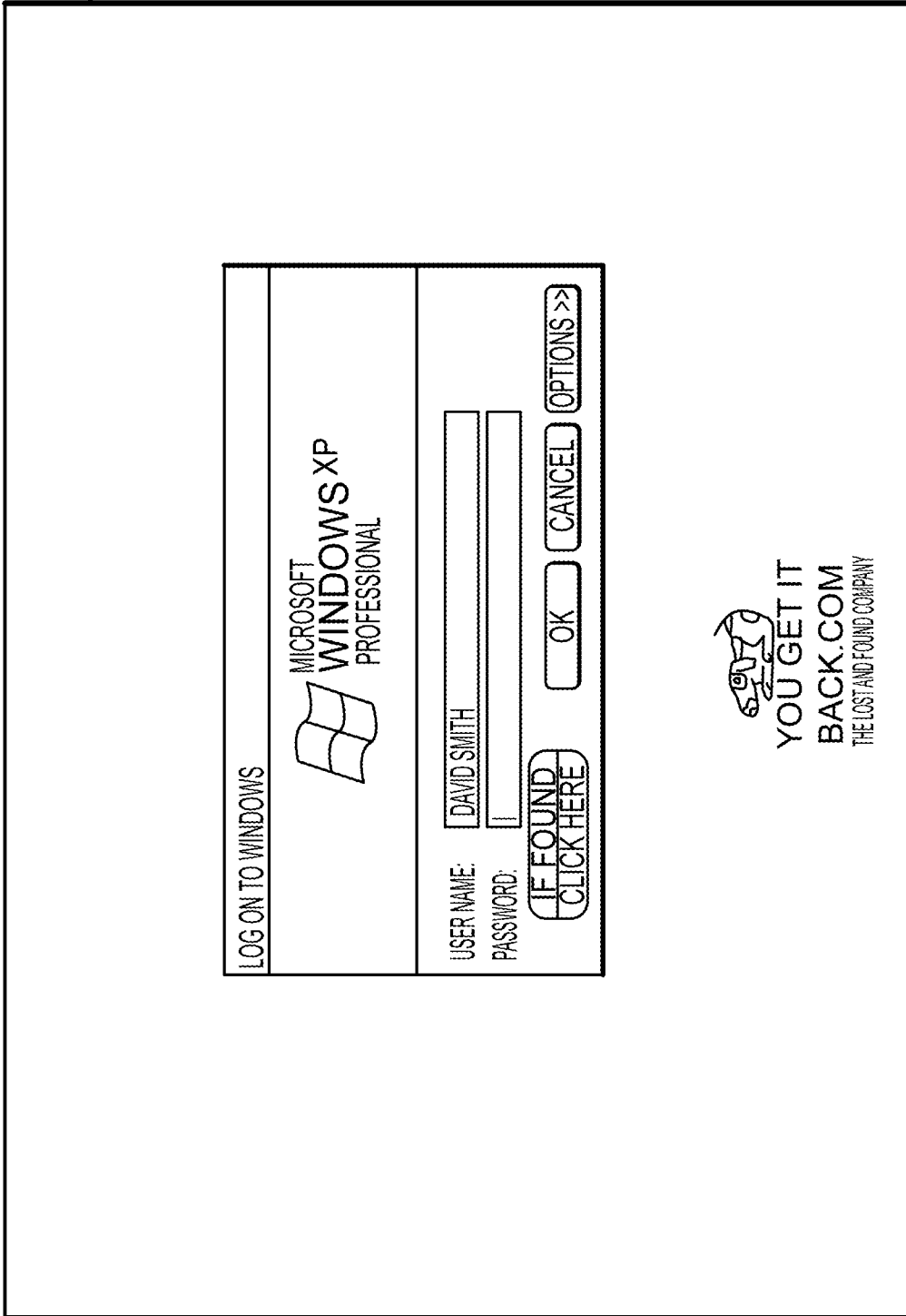


FIGURE 10

1100

11/64

**eTag CLIENT ONLINE**

NAME

PHONE

EMAIL

THIS DEVICE IS NOW CONNECTED TO THE INTERNET. PLEASE FILL IN THE INFORMATION AND CLICK SUBMIT. WE WILL BE IN CONTACT WITH YOU TO ARRANGE COLLECTION OF THIS DEVICE.

**YOUR REWARD! ONCE THIS COMPUTER IS RETURNED TO ITS RIGHTFUL OWNER YOUGETTBACK.COM WILL PAY YOU A FINDERS FEE OF \$50 TO SHOW OUR APPRECIATION FOR YOUR ACT OF KINDNESS.**

**REPORT LOSS** THIS ALLOWS YOU TO SEARCH FOR THE MANUALLY OWNER WITHOUT CONNECTING TO THE YOUGETTBACK.COM WEBSITE.

XP  
WS  
NAME

PETER BERMINGHAM  
TYPE YOUR PASSWORD

EN →

---

TURN OFF COMPUTER

AFTER YOU LOG ON, YOU CAN ADD OR CHANGE ACCOUNTS, JUST GO TO CONTROL PANEL AND SELECT USER ACCOUNTS.

FIGURE 11

1200

12/64

**THANK YOU!**

UNFORTUNATELY THE COMPUTER IS UNABLE TO ESTABLISH A CONNECTION WITH THE YOUGETITBACK.COM WEBSITE AT THIS TIME. IF YOU SELECT THE COUNTRY YOU ARE LOCATED IN FROM THE DROP DOWN MENU BELOW, WE WILL GIVE YOU THE LOCAL FREE PHONE NUMBER TO OUR LOST AND FOUND DEPARTMENT.

COUNTRY

FREE PHONE: (1) 212 444 0301 OR 866 4 268 692  
ID: 62860993532534

**YOUR REWARD! ONCE THIS COMPUTER IS RETURNED TO IT'S RIGHTFUL OWNER YOUGETITBACK.COM WILL PAY YOU A FINDERS FEE OF \$50 TO SHOW OUR APPRECIATION FOR YOUR ACT OF KINDNESS.**

**CLOSE THIS FORM** THIS ALLOWS YOU TO SEARCH FOR THE OWNER WITHOUT CONNECTING TO THE YOUGETITBACK.COM WEBSITE.

XP  
WS  
NAME

---

PETER BIRMINGHAM  
TYPE YOUR PASSWORD

TURN OFF COMPUTER

AFTER YOU LOG ON, YOU CAN ADD OR CHANGE ACCOUNTS. JUST GO TO CONTROL PANEL AND SELECT USER ACCOUNTS.

FIGURE 12



1300

13/64

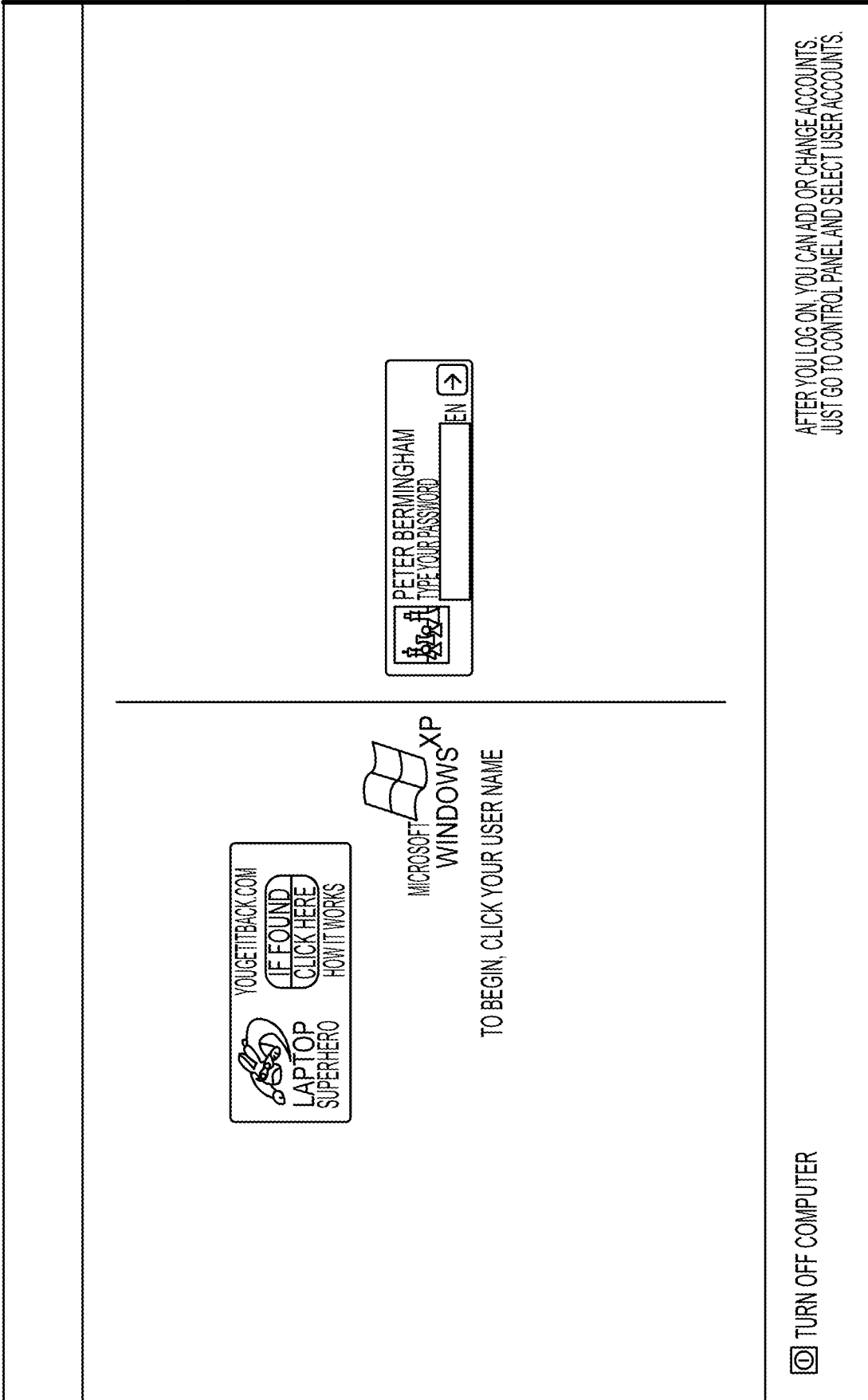


FIGURE 13

1400

14/64

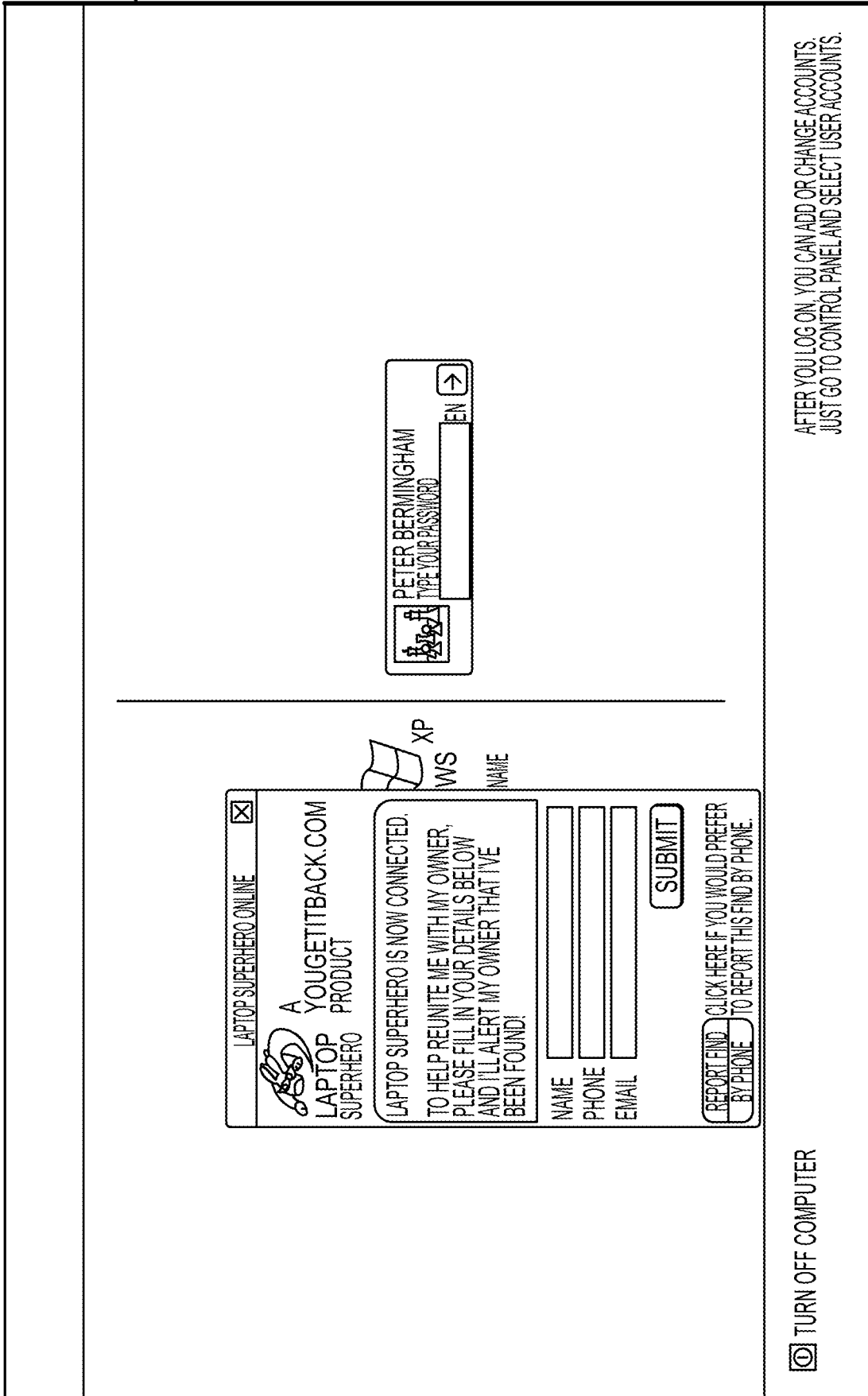


FIGURE 14

1500

15/64

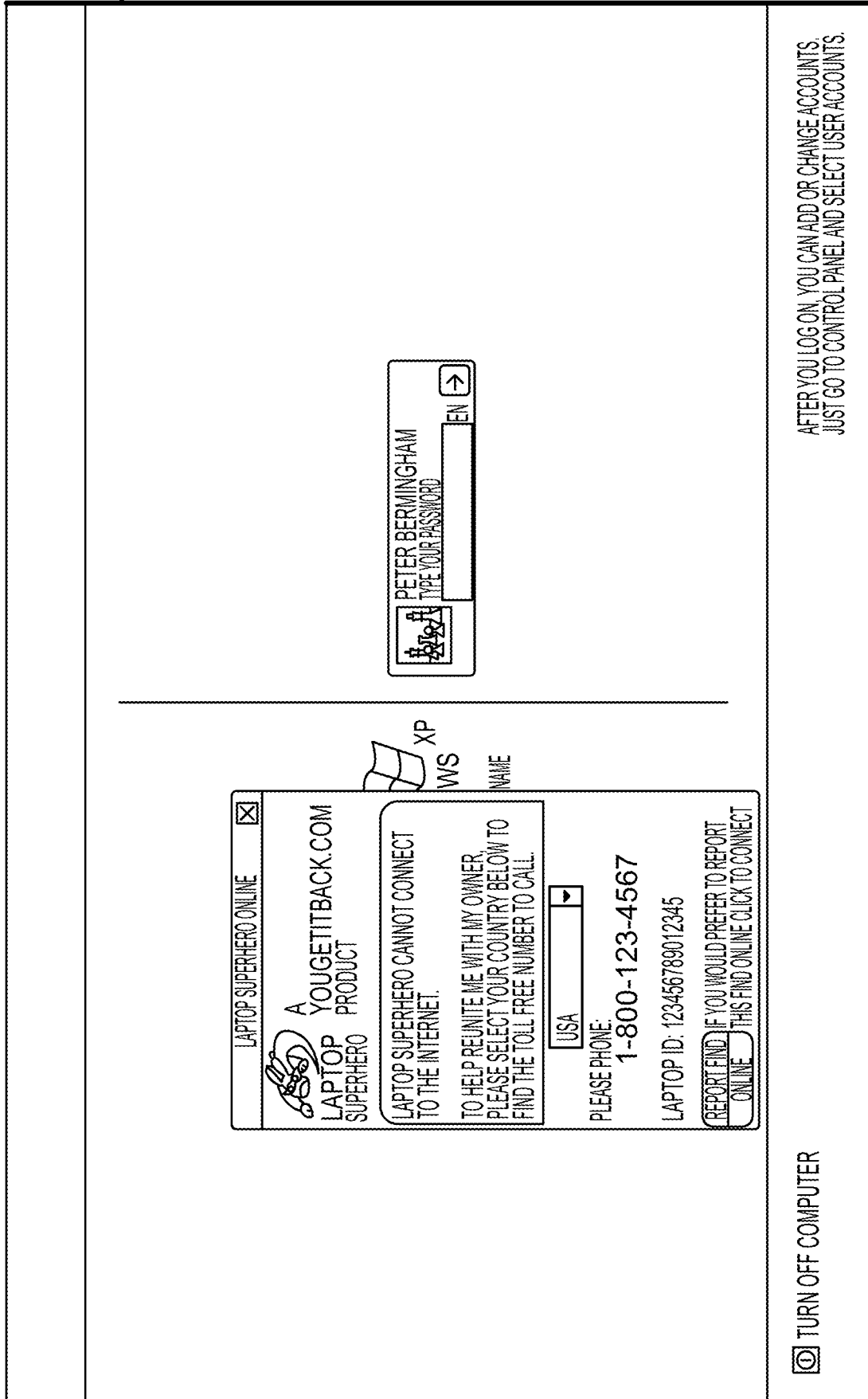
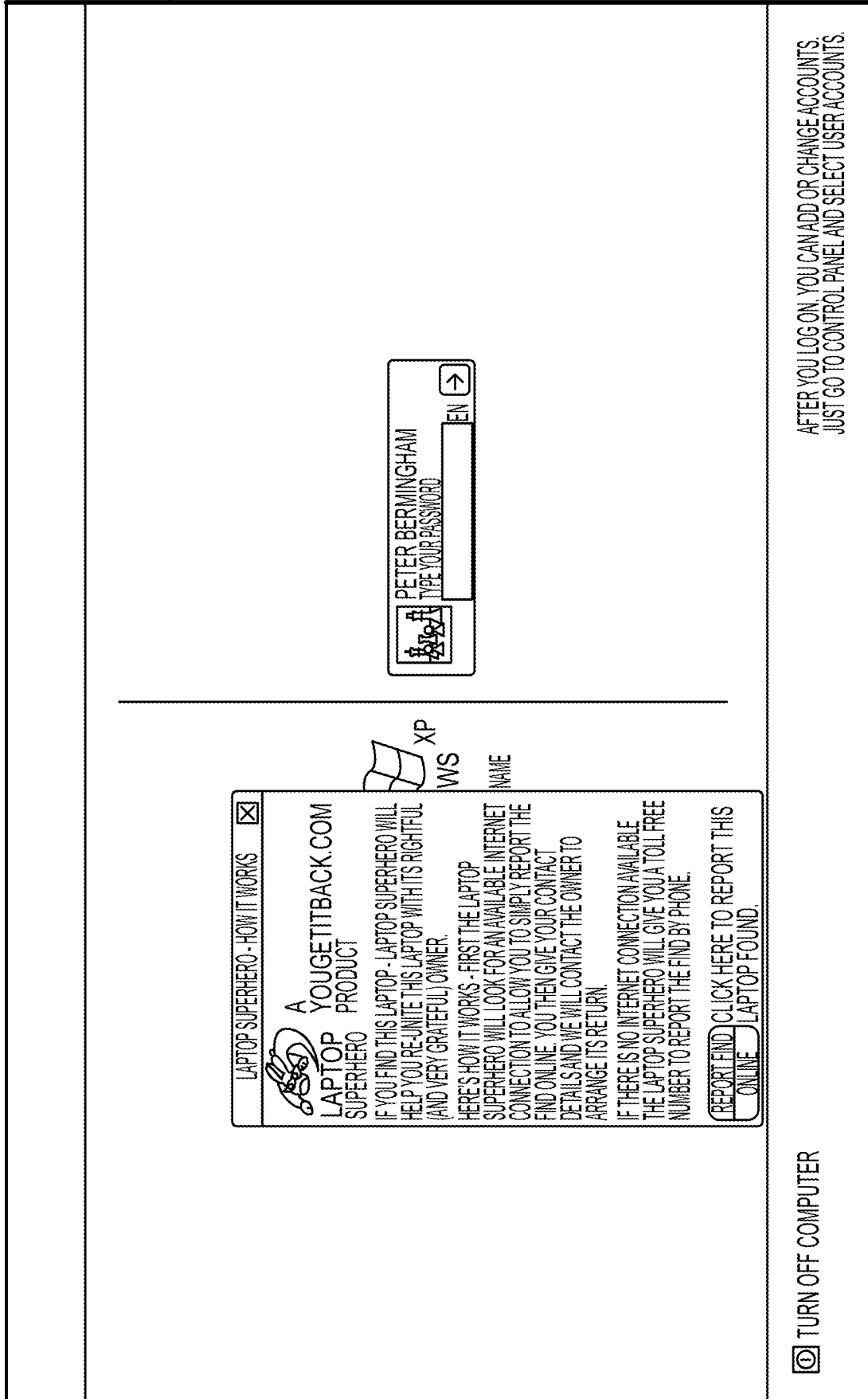


FIGURE 15

1600

16/64



AFTER YOU LOG ON, YOU CAN ADD OR CHANGE ACCOUNTS. JUST GO TO CONTROL PANEL AND SELECT USER ACCOUNTS.

FIGURE 16

17/64

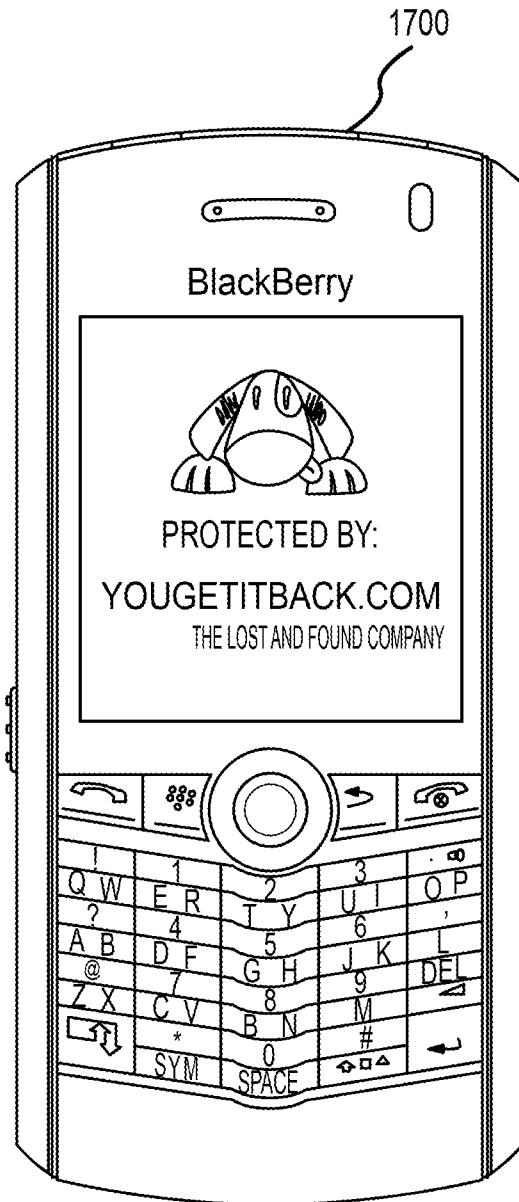


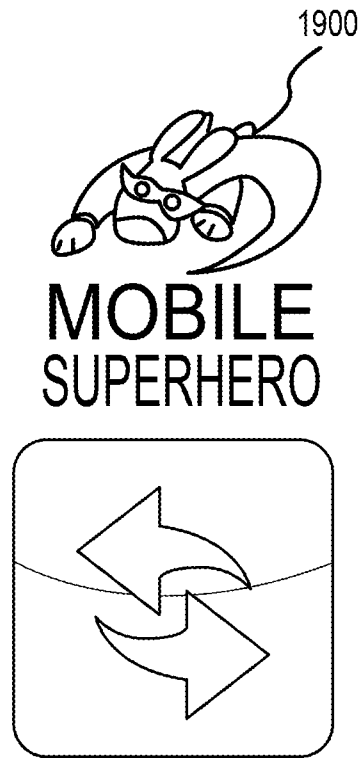
FIGURE 17

18/64



FIGURE 18

19/64



**CONNECTED**

TO END THIS CALL, JUST HOLD  
DOWN THE RED BUTTON

YOUGETITBACK.COM

**FIGURE 19**

20/64



**MOBILE  
SUPERHERO**

**EMERGENCY...**

TO END THIS CALL, JUST PRESS  
ALT + END

YOUGETITBACK.COM

**FIGURE 20**



21/64

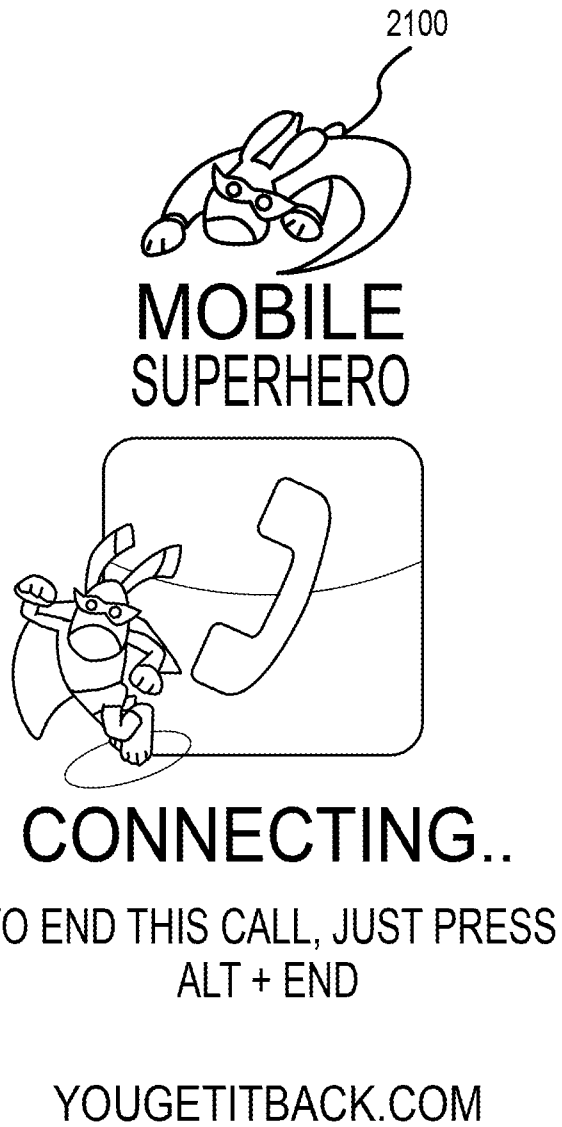
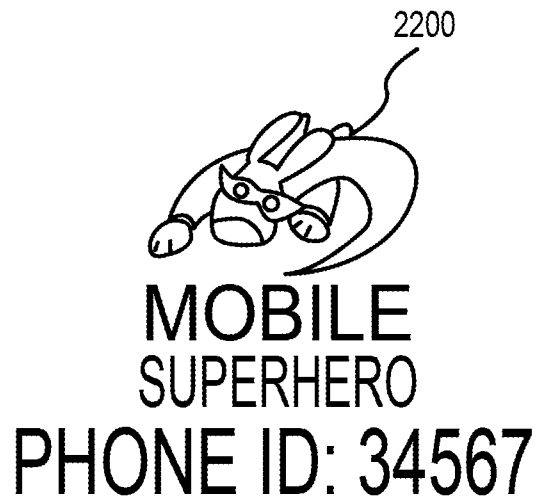


FIGURE 21

22/64



**REPORT FOUND**

**EMERGENCY CALL**

**HELP**

**ABOUT**

**YOUGETITBACK.COM**

**FIGURE 22**

23/64



FIGURE 23

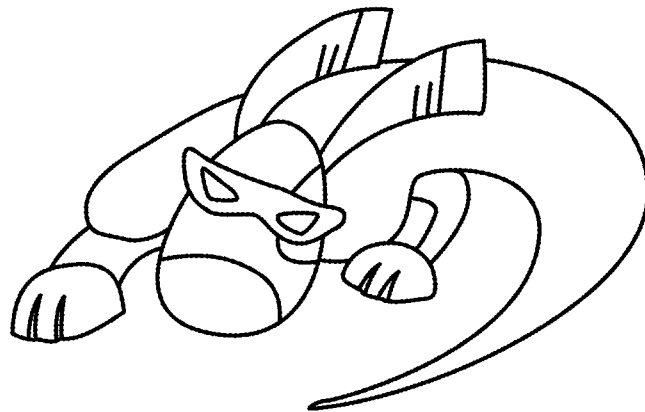
24/64



FIGURE 24

25/64

2500  
PROTECTED BY  
YOUGETITBACK.COM



**MOBILE  
SUPERHERO**

FIGURE 25

2600

WITH YOU GET IT BACK.COM, UP TO 75% OF ALL LOST ITEMS GET RETURNED.

SIGN UP FOR THE BETA  
OF OUR NEW PRODUCT!

SIGN UP NOW AND WE'LL GET IN TOUCH TO SET YOU  
UP WITH THIS EXCITING NEW PRODUCT. [SEE HERE FOR  
MORE INFO AND OUR PRIVACY POLICY.](#)

NAME:

EMAIL ADDRESS:

SUBMIT


[RETURNS POLICY](#) | [TERMS OF USE](#) | [PRIVACY POLICY](#) | [CORPORATE SERVICES](#)

FIGURE 26

27/64

2700

YOU ARE NOT SIGNED IN >> SIGN IN IRELAND << CHANGE



**YOUGETITBACK.COM**

THE LOST AND FOUND COMPANY

I FOUND SOMETHING...

I LOST SOMETHING...


BUY A TAG...

ACTIVATE A TAG...


MY VAULT | STORE | SUPPORT | ABOUT US | NEWS | HOME

---

WITH YOUGETITBACK.COM, UP TO 75% OF ALL LOST ITEMS GET RETURNED.




**FREE PRODUCT DOWNLOADS!**



**LAPTOP SUPERHERO**

DOWNLOAD NOW!



**MOBILE SUPERHERO**

DOWNLOAD NOW!

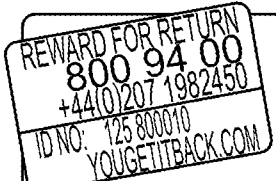
**SECURE YOUR LAPTOP AND MOBILE PHONE**

THESE EXCITING NEW PRODUCTS WILL HELP TO GET YOUR LAPTOP & MOBILE RETURNED TO YOU IN THE EVENT OF LOSS OR THEFT.


[MORE INFO ON LAPTOP SUPERHERO >>](#)

[MORE INFO ON MOBILE SUPERHERO >>](#)

---



**PROTECT YOUR STUFF!**



**YOUGETITBACK.COM**

LOST ITEMS WHICH ARE TAGGED WITH A YOUGETITBACK TAG ARE MUCH MORE LIKELY TO BE RETURNED TO YOU!

REGISTERED USERS ARE ALERTED IMMEDIATELY WHEN THEIR STUFF IS FOUND.

TAG YOUR STUFF NOW FOR PEACE OF MIND!

BUY TAGS

MORE INFO...

SIGN UP FOR FREE AND START USING THE YOUGETITBACK VAULT!

FIND IT HARD TO REMEMBER IMPORTANT DETAILS ABOUT YOUR BELONGINGS? MOBILE - PUK CODES AND PIN NUMBERS. CAR KEYS, SERIAL NUMBERS, WARRANTY INFO...

USE THE VAULT TO STORE THESE DETAILS AND MANAGE ALL YOUR TAGGED ITEMS ALL IN ONE PLACE.

SIGN UP

MORE INFO...


---

COPYRIGHT 2007 | YOUGETITBACK.COM ALL RIGHTS RESERVED

[RETURNS POLICY](#) | [TERMS OF USE](#) | [PRIVACY POLICY](#) | [CORPORATE SERVICES](#)

FIGURE 27

LOG IN
IRELAND << CHANGE



## YOUGETITBACK.COM

THE LOST AND FOUND COMPANY

I FOUND SOMETHING...

I LOST SOMETHING...


BUY A TAG...

ACTIVATE A TAG...


[MY VAULT](#) | [STORE](#) | [SUPPORT](#) | [ABOUT US](#) | [NEWS](#) | [BLOG](#) | [HOME](#)

---

WITH YOUGETITBACK.COM, UP TO 75% OF ALL LOST ITEMS GET RETURNED.




FREE PRODUCT DOWNLOADS!



LAPTOP  
SUPERHERO

DOWNLOAD  
NOW!



MOBILE  
SUPERHERO

DOWNLOAD  
NOW!

SECURE YOUR LAPTOP  
AND MOBILE PHONE

THESE EXCITING NEW PRODUCTS WILL HELP TO  
GET YOUR LAPTOP & MOBILE RETURNED TO  
YOU IN THE EVENT OF LOSS OR THEFT.

[MORE INFO ON LAPTOP SUPERHERO >>](#)

[MORE INFO ON MOBILE SUPERHERO >>](#)

---

ACTIVATE YOUR LOST & FOUND SERVICE...  
BE INSTANTLY NOTIFIED WHEN SOMEONE FINDS YOUR STUFF!

\* TAG ID:

\* EMAIL:

\* I AM A:

NEW CUSTOMER  
 EXISTING CUSTOMER

\* PASSWORD:


\* [TERMS & CONDITIONS](#)  I HAVE REVIEWED  
AND ACCEPT THESE  
TERMS & CONDITIONS

PROTECT YOUR STUFF

REWARD FOR RETURN

1800 238 0695

ID NO: T000E0001

YOUGETITBACK.COM 

LOST ITEMS WHICH ARE TAGGED WITH A YOUGETITBACK  
TAG ARE MUCH MORE LIKELY TO BE RETURNED TO YOU!  
TAG YOUR STUFF NOW FOR PEACE OF MIND!

USE THE VAULT TO STORE THESE DETAILS AND MANAGE  
ALL YOUR TAGGED ITEMS ALL IN ONE PLACE.

[SIGN UP FOR FREE AND START USING THE VAULT >>](#)

---

LATEST FROM THE BLOG...

THE PHONE CONDOM

SPOTTED ON THE LOIC LeMour BLOG A NIFTY WAY TO PROTECT YOUR PHONE  
WHEN EATING OUT. RESTAURANTS IN BEIJING ARE GIVING OUT PHONE  
CONDOMS (LITTLE PLASTIC BAGS) SO THEY CAN CHECK THEIR PHONE WHEN  
EATING WITHOUT SPILLING ANYTHING ON IT. CONTINUE READING...

[I HOPE SHE FINDS MY LOST STUFF >>](#)

[BLACKBERRY MAY BE SHUT DOWN IN INDIA >>](#)

[MORE >>](#)

SUBSCRIBE

[SUBSCRIBE IN A READER](#)

SUBSCRIBE VIA EMAIL:

ENTER YOUR EMAIL ADDRESS:

DELIVERED BY [FeedBurner](#)

---

COPYRIGHT 2007 | YOUGETITBACK.COM ALL RIGHTS RESERVED

[RETURNS POLICY](#) | [TERMS OF USE](#) | [PRIVACY POLICY](#) | [CORPORATE SERVICES](#)

FIGURE 28



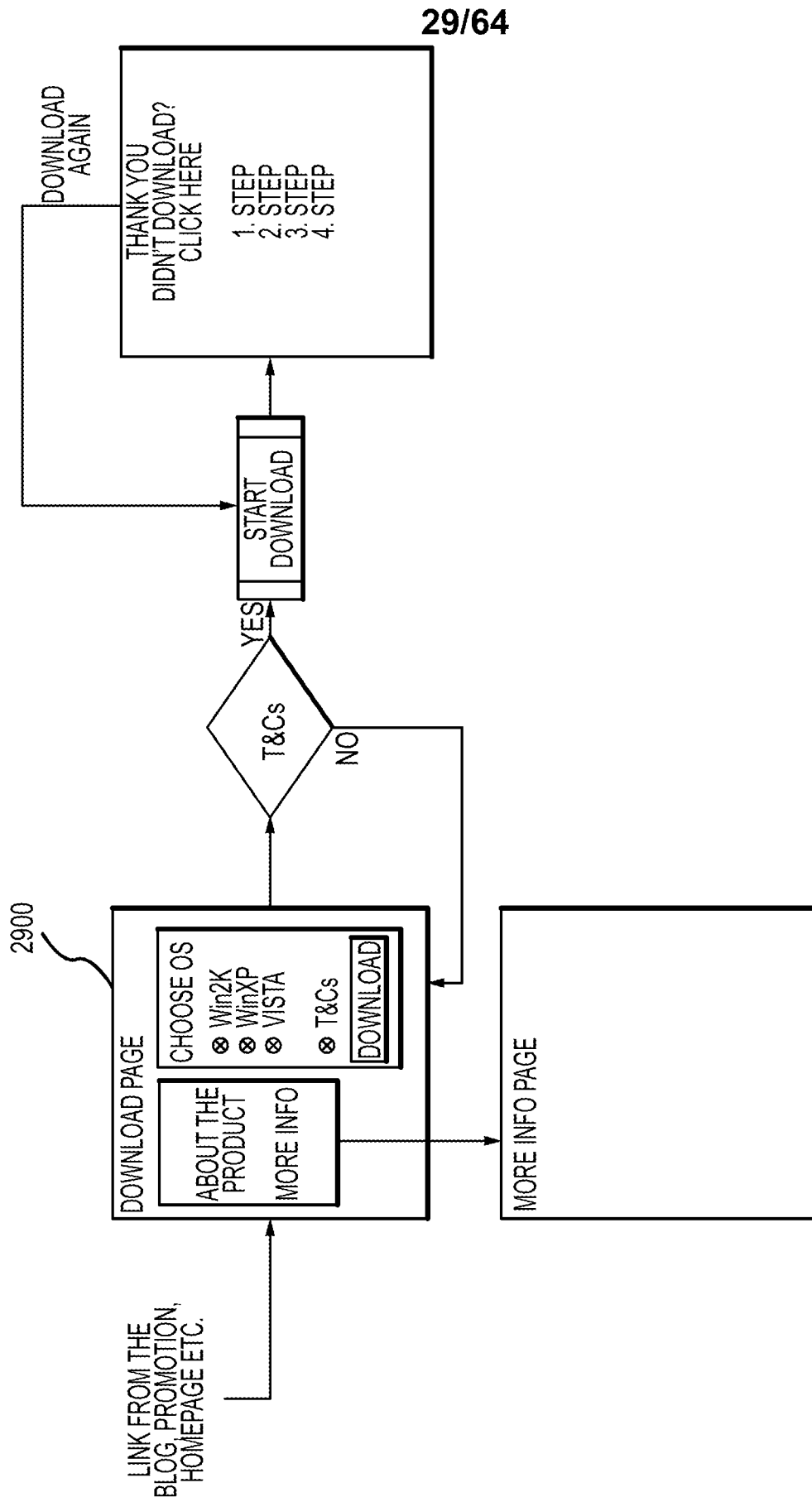



FIGURE 29

3000

LOG IN IRELAND << CHANGE



**YOUGETITBACK.COM**

THE LOST AND FOUND COMPANY

I FOUND SOMETHING...


I LOST SOMETHING...

BUY A TAG...

ACTIVATE A TAG...

---

[MY VAULT](#) | [STORE](#) | [SUPPORT](#) | [ABOUT US](#) | [NEWS](#) | [BLOG](#) | [HOME](#)




## LAPTOP SUPERHERO

LAPTOP SUPERHERO IS A NEW, FREE AND EXCITING LAPTOP SECURITY PRODUCT FROM YOUGETITBACK.COM. DOWNLOAD YOUR FREE COPY OF LAPTOP SUPERHERO. FREE FOR LIFE FOR FIRST 1000 PEOPLE TO SIGN UP TO THE BETA RELEASE. YOU WILL ALSO BE ENTITLED TO FREE UPGRADES AS THEY ARE RELEASED.

LAPTOP SUPERHERO IS A CLEVER PIECE OF SOFTWARE THAT HELPS GET YOUR LAPTOP BACK TO YOU IN THE EVENT OF A LOSS OR THEFT.

HOW DOES IT WORK?

1. DOWNLOAD LAPTOP SUPERHERO SOFTWARE
2. INSTALL ON YOUR LAPTOP
3. REGISTER YOUR LAPTOP SUPERHERO IN OUR SECURE VAULT
4. WE ALERT THE FINDER THAT THIS LAPTOP IS LOST
5. WE HELP GET YOUR LAPTOP BACK TO YOU



## LAPTOP SUPERHERO

SELECT YOUR OPERATING SYSTEM:

I HAVE READ, AND AGREE TO, THE TERMS AND CONDITIONS

DOWNLOAD

---

COPYRIGHT 2007 | YOUGETITBACK.COM ALL RIGHTS RESERVED

[RETURNS POLICY](#) | [TERMS OF USE](#) | [PRIVACY POLICY](#) | [CORPORATE SERVICES](#)

FIGURE 30

3100

AFTER THE USER HAS  
DOWNLOADED AND INSTALLED  
THE PRODUCT AND A RESTART  
HAS TAKEN PLACE AND A  
NETWORK CONNECTION IS  
AVAILABLE THE APPLICATION  
WILL LAUNCH THE BROWSER  
TO THE FOLLOWING PAGE  
WITH A UNIQUE YGIB TAG ID  
PREVIOUSLY RETRIEVED  
FROM THE YGIB SERVER

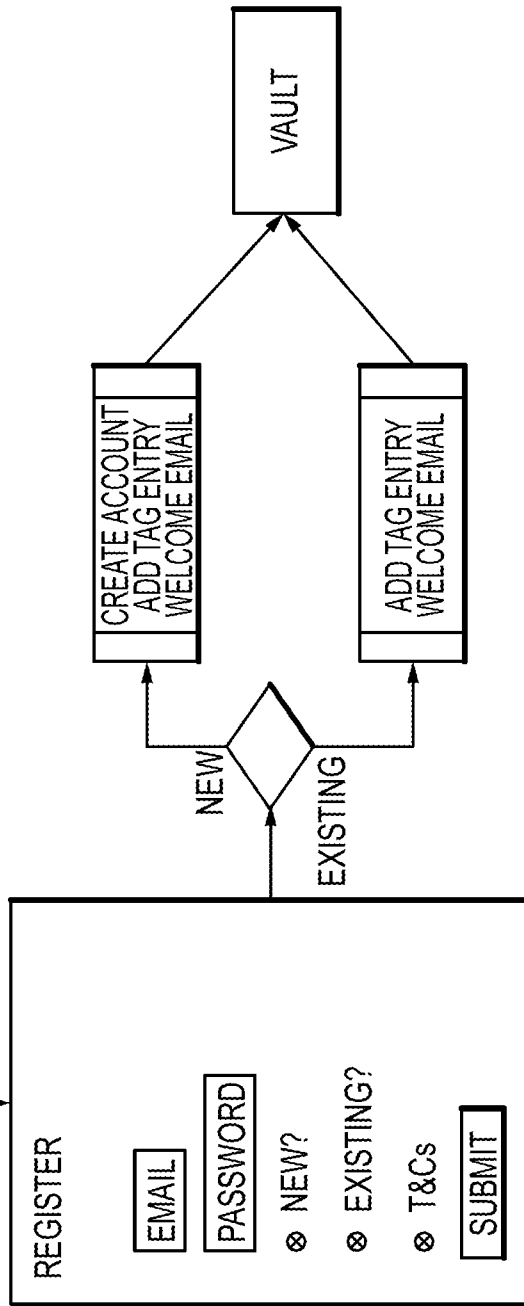


FIGURE 31

32/64

3200

YOU ARE LOGGED IN AS ROBERT SMITH | LOGOUT << CHANGE

**YOU GET IT BACK.COM**  
THE LOST AND FOUND COMPANY

I FOUND SOMETHING... I LOST SOMETHING...  
BUY A TAG... ACTIVATE A TAG...

MY VAULT | STORE | SUPPORT | ABOUT US | NEWS | BLOG | HOME

NULL  
NULL  
NULL  
NULL

**MY VAULT:**

(CREATE NEW ITEM >>)

	DESCRIPTION ▾	TAG ID ▾	SubCategory	
<input checked="" type="checkbox"/>	DIGITAL CAMERA	ABC000001	OTHER	<input type="button" value="MORE &gt;&gt;"/>
<input checked="" type="checkbox"/>	MOBILE PHONE	WWW188888	OTHER	<input type="button" value="MORE &gt;&gt;"/>
<input checked="" type="checkbox"/>	UMBRELLA	RYL593895	OTHER	<input type="button" value="MORE &gt;&gt;"/>

**MOBILE ETAGS**

TagCode	OS			
971131973376036	SYMBIAN_V2	<input type="button" value="LOCK"/>	<input type="button" value="UNLOCK"/>	VIEW CONTACTS
971131973376098	BB	<input type="button" value="LOCK"/>	<input type="button" value="UNLOCK"/>	VIEW CONTACTS

**LAPTOP ETAGS**

TagCode	OS	USERNAME		
55555	WINDOW		<input type="button" value="LOCK"/>	<input type="button" value="UNLOCK"/>


COPYRIGHT 2007 | YOUGETITBACK.COM ALL RIGHTS RESERVED  
RETURNS POLICY | TERMS OF USE | PRIVACY POLICY | CORPORATE SERVICES

FIGURE 32

33/64

3300

YOU ARE LOGGED IN AS JOHN PRENDERGAST | LOGOUT IRELAND << CHANGE

 **YOU GET IT BACK.COM** I FOUND SOMETHING... I LOST SOMETHING...  
THE LOST AND FOUND COMPANY BUY A TAG... ACTIVATE A TAG...

[MY VAULT](#) | [STORE](#) | [SUPPORT](#) | [ABOUT US](#) | [NEWS](#) | [BLOG](#) | [HOME](#)

MY VAULT

ACTIVATE A TAG

MY PROFILE

EMAIL TAG LIST

### MY VAULT:

[\(CREATE NEW ITEM >>\)](#)

	DESCRIPTION ▾	TAG ID ▾	SubCategory	
⊗		<a href="#">TTT111006</a>	2 WAY RADIOS	<a href="#">(MORE &gt;&gt;)</a>
Ⓢ	TESTD	<a href="#">TTT111005</a>	2 WAY RADIOS	<a href="#">(MORE &gt;&gt;)</a>

COPYRIGHT 2007 | YOU GET IT BACK.COM ALL RIGHTS RESERVED  
[RETURNS POLICY](#) | [TERMS OF USE](#) | [PRIVACY POLICY](#) | [CORPORATE SERVICES](#)

FIGURE 33

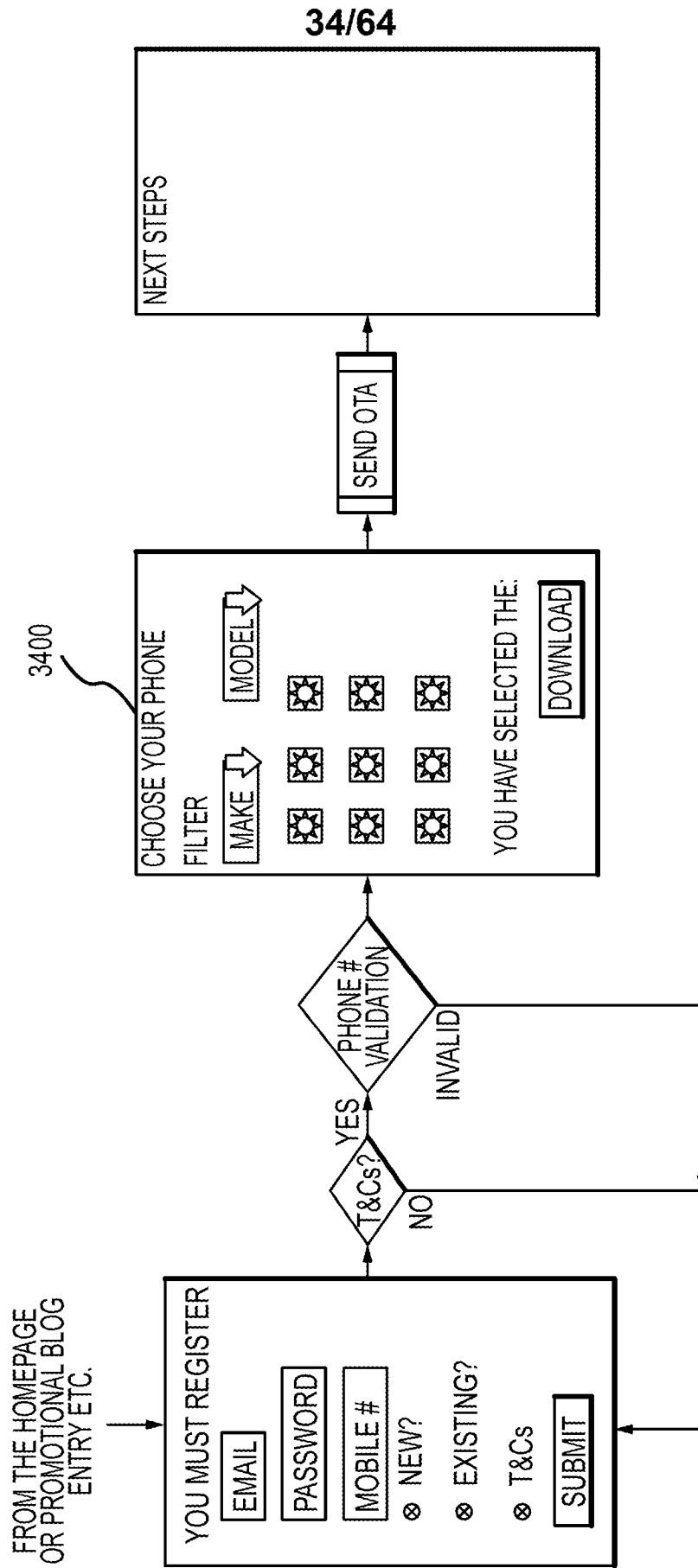



FIGURE 34

3500

YOU ARE NOT SIGNED IN >> SIGN IN IRELAND << CHANGE



# YOUGETITBACK.COM

THE LOST AND FOUND COMPANY

I FOUND SOMETHING...

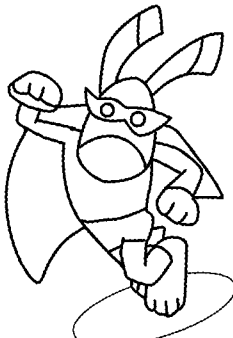
I LOST SOMETHING...

BUY A TAG...

ACTIVATE A TAG...

---

MY VAULT | STORE | SUPPORT | ABOUT US | NEWS | HOME



**MOBILE SUPERHERO**  
BETA

**GET MOBILE SUPERHERO FREE!**

NAME:


CHOOSE A PASSWORD:

MOBILE NUMBER:

I AM A:  NEW CUSTOMER  
 EXISTING CUSTOMER

TERMS & CONDITIONS:  I HAVE READ, AND AGREE TO THE TERMS & CONDITIONS

NEXT STEP



**MOBILE SUPERHERO**  
BETA

## MOBILE SUPERHERO

MOBILE SUPERHERO IS A NEW, FREE AND EXCITING MOBILE SECURITY PRODUCT FROM YOUGETITBACK.COM.

DOWNLOAD YOUR FREE COPY OF MOBILE SUPERHERO. FREE FOR LIFE FOR A LIMITED NUMBER OF EARLY SIGN-UPS TO THE BETA RELEASE. LIMITED EARLY SIGN UPS WILL ALSO BE ENTITLED TO FREE UPGRADES AS THEY ARE RELEASED.


MOBILE SUPERHERO IS A CLEVER PIECE OF SOFTWARE THAT ALLOWS YOU TO LOCK YOUR PHONE REMOTELY IF YOU LOSE IT AND ALSO ALLOWS YOU TO BACK-UP YOUR CONTACTS AND STORE THEM SECURELY IN YOUR OWN PRIVATE ONLINE VAULT. IN THE EVENT THAT YOUR PHONE IS LOST OR STOLEN OUR MOBILE SUPERHERO WILL HELP TO RE-UNITE YOU WITH THE FINDER.

1. REGISTER FOR THE PRODUCT
2. DOWNLOAD MOBILE SUPERHERO SOFTWARE TO YOUR PHONE
3. INSTALL ON YOUR MOBILE
4. BACKUP YOUR CONTACTS TO YOUR SECURE VAULT

FIGURE 35

3600

YOU ARE NOT SIGNED IN >> SIGN IN IRELAND << CHANGE



**YOUGETITBACK.COM**

THE LOST AND FOUND COMPANY

I FOUND SOMETHING...

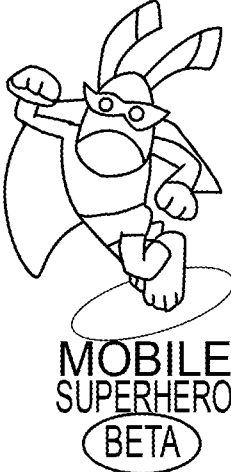
I LOST SOMETHING...

BUY A TAG...

ACTIVATE A TAG...

---

MY VAULT | STORE | SUPPORT | ABOUT US | NEWS | HOME

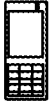

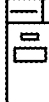





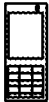

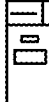







**MOBILE  
SUPERHERO  
BETA**

**NEARLY FINISHED... JUST CHOOSE YOUR PHONE MODEL!**

SELECT THE MAKE AND MODEL OF YOUR PHONE IN THE DROP DOWNS BELOW. OR CLICK THE PICTURE OF YOUR PHONE IF YOU SEE IT BELOW. CLICK THE SUBMIT BUTTON WHEN YOU HAVE SELECTED YOUR PHONE.

SELECT YOUR PHONE MAKE | v
SELECT YOUR PHONE MODEL | v
SUBMIT

 NOKIA N73	 NOKIA N72	 NOKIA N93	 NOKIA N92
 NOKIA N92	 NOKIA N93	 NOKIA N72	 NOKIA N73
 NOKIA N73	 NOKIA N72	 NOKIA N93	 NOKIA N92
 NOKIA N92	 NOKIA N93	 NOKIA N72	 NOKIA N73

COPYRIGHT 2007 | YOUGETITBACK.COM ALL RIGHTS RESERVED

[RETURNS POLICY](#) | [TERMS OF USE](#) | [PRIVACY POLICY](#) | [CORPORATE SERVICES](#)


FIGURE 36



37/64

3700

YOU ARE NOT SIGNED IN >> SIGN IN IRELAND << CHANGE



# YOUGETITBACK.COM

THE LOST AND FOUND COMPANY

I FOUND SOMETHING...


I LOST SOMETHING...

BUY A TAG...

ACTIVATE A TAG...

---

[MY VAULT](#) | [STORE](#) | [SUPPORT](#) | [ABOUT US](#) | [NEWS](#) | [HOME](#)



## MOBILE SUPERHERO

BETA

### CONGRATULATIONS!

YOU SHOULD RECEIVE A TEXT MESSAGE FROM US SHORTLY. PLEASE FOLLOW THE INSTRUCTIONS IN THE TEXT TO COMPLETE YOUR INSTALLATION OF MOBILE SUPERHERO.

## MOBILE SUPERHERO

VUgue dolesto cons nostrud dolore veliquat, sum volenibh el do deliquissim vel eugait, sissequat ilit doluptation henissis ad tat, quis accum in ex enit luptatin utpatem er sim nim ad dolorpe rcipsum ad dignibh estrud exero eliqui bia augue essequis at, consenis autpat. Dui tincinim ip et atem esed tat. Sim dunt acilit at nonullu msandia mcommy nulla commy num niscidunt fute eugue ver sim er se dit nullupt atumsan dipisi del ing et niscidunt ut aut diamet landrer accumsan eum elenim nullan ut ad te con venim dit velendi onsecte dunt nons eratem quam irit volor sum doloreet illute consendre tin hendrem nis num dipsuscing etue dipit irillaor ilit inil ing exenus cillutpat.

Lore ercil dolutet wisit iliquat ut atio corero delit, qui blaor sum zzrit venismo dolorem zzriliquisit nostrud tem duipsuscilis nulputet lam, velis accum alis elit wis delisit velent niscipis ea consectet lobore commy nit, vel essecte tat. Ut del delis ad tem zzrillut iure magna con ulput wis adip ea corem exeristrud mod tet lorper augiamet incilisit nulla faccumy nis dio od ea con ut vercil dio con venisim iustie vulput augait, commodo lorperci tie magna facilla aliscidunt enis non vent in heniliquam, quat.

COPYRIGHT 2007 | YOUGETITBACK.COM ALL RIGHTS RESERVED  
[RETURNS POLICY](#) | [TERMS OF USE](#) | [PRIVACY POLICY](#) | [CORPORATE SERVICES](#)

FIGURE 37

3800

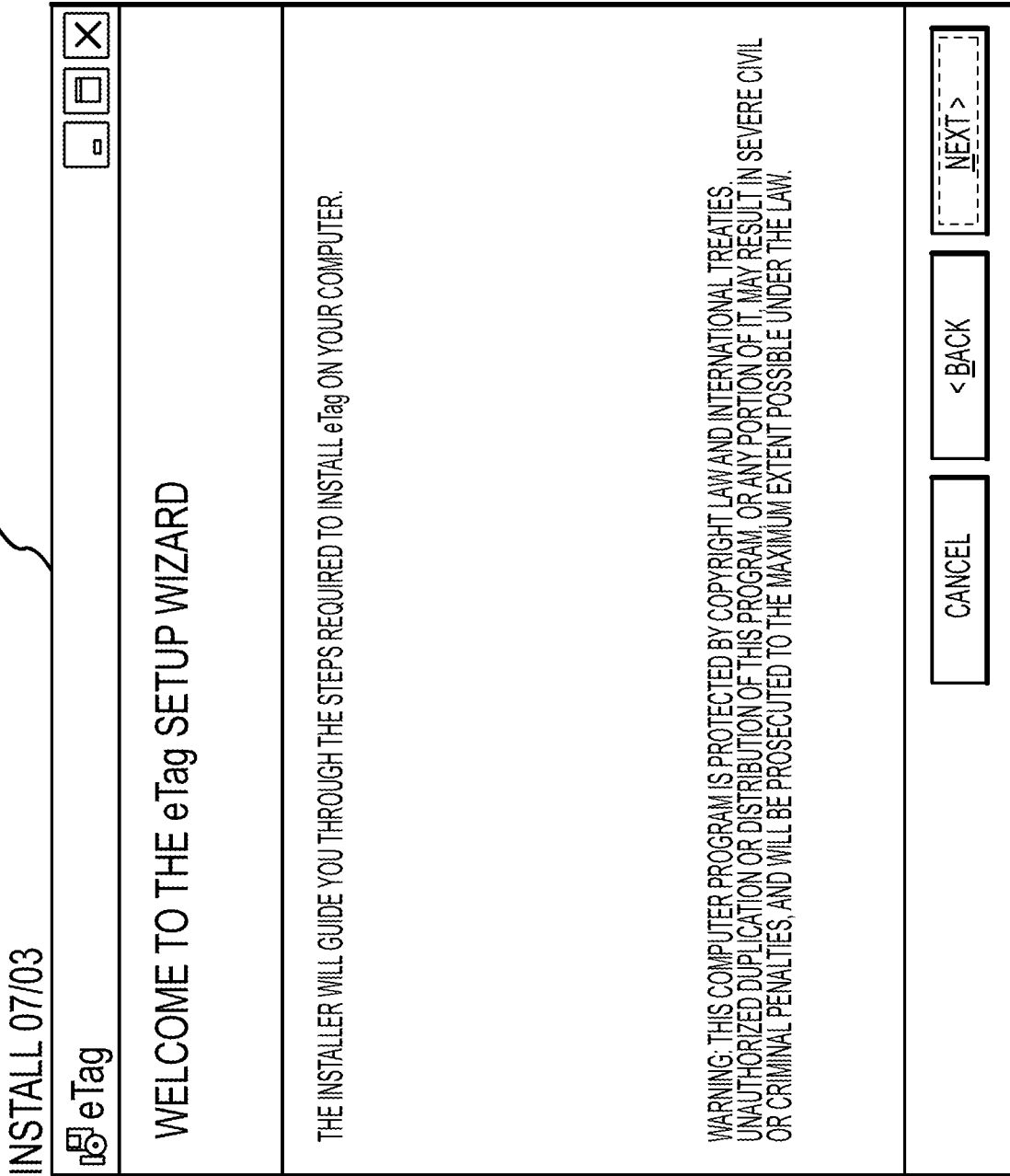


FIGURE 38

3900

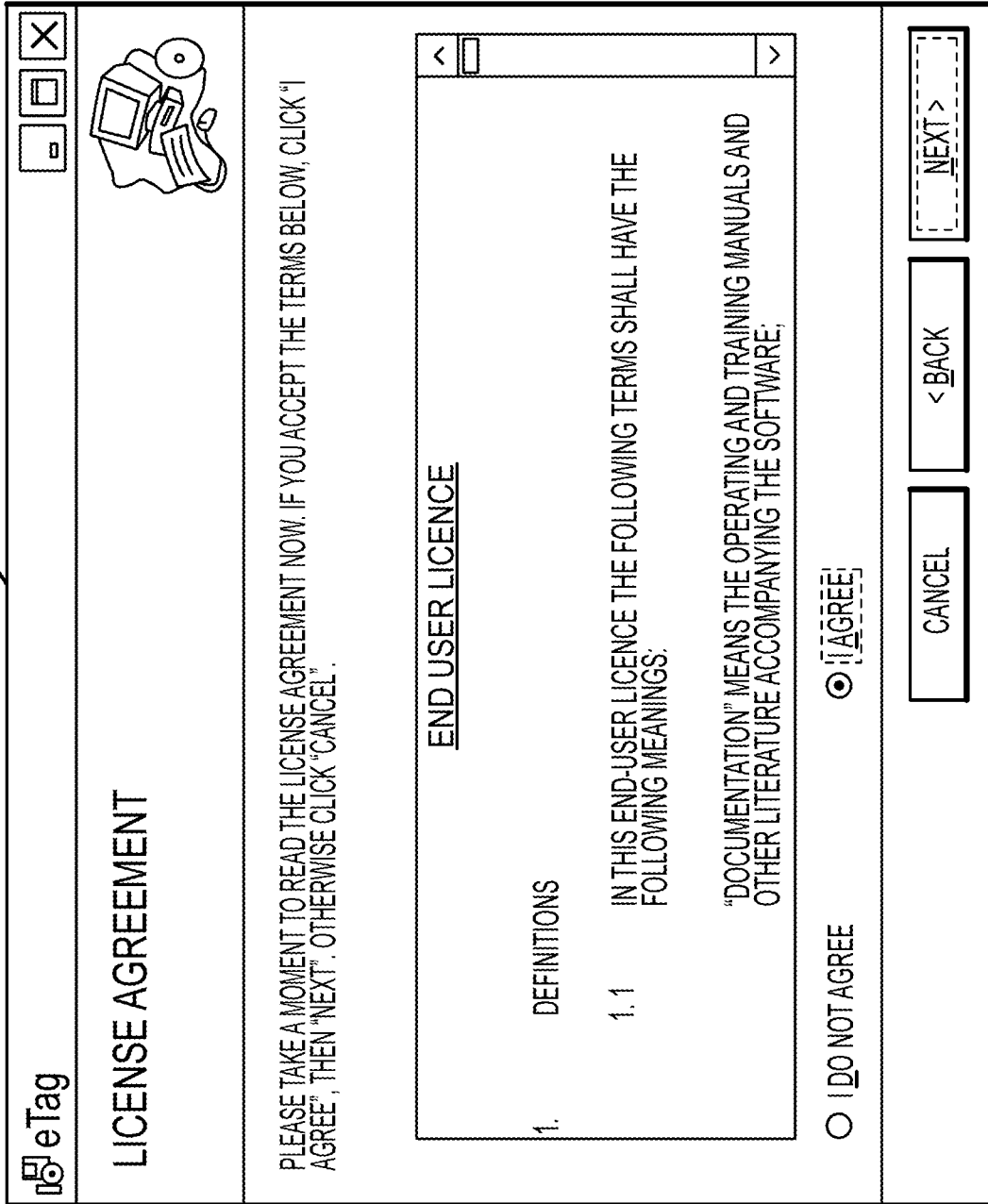


FIGURE 39

4000

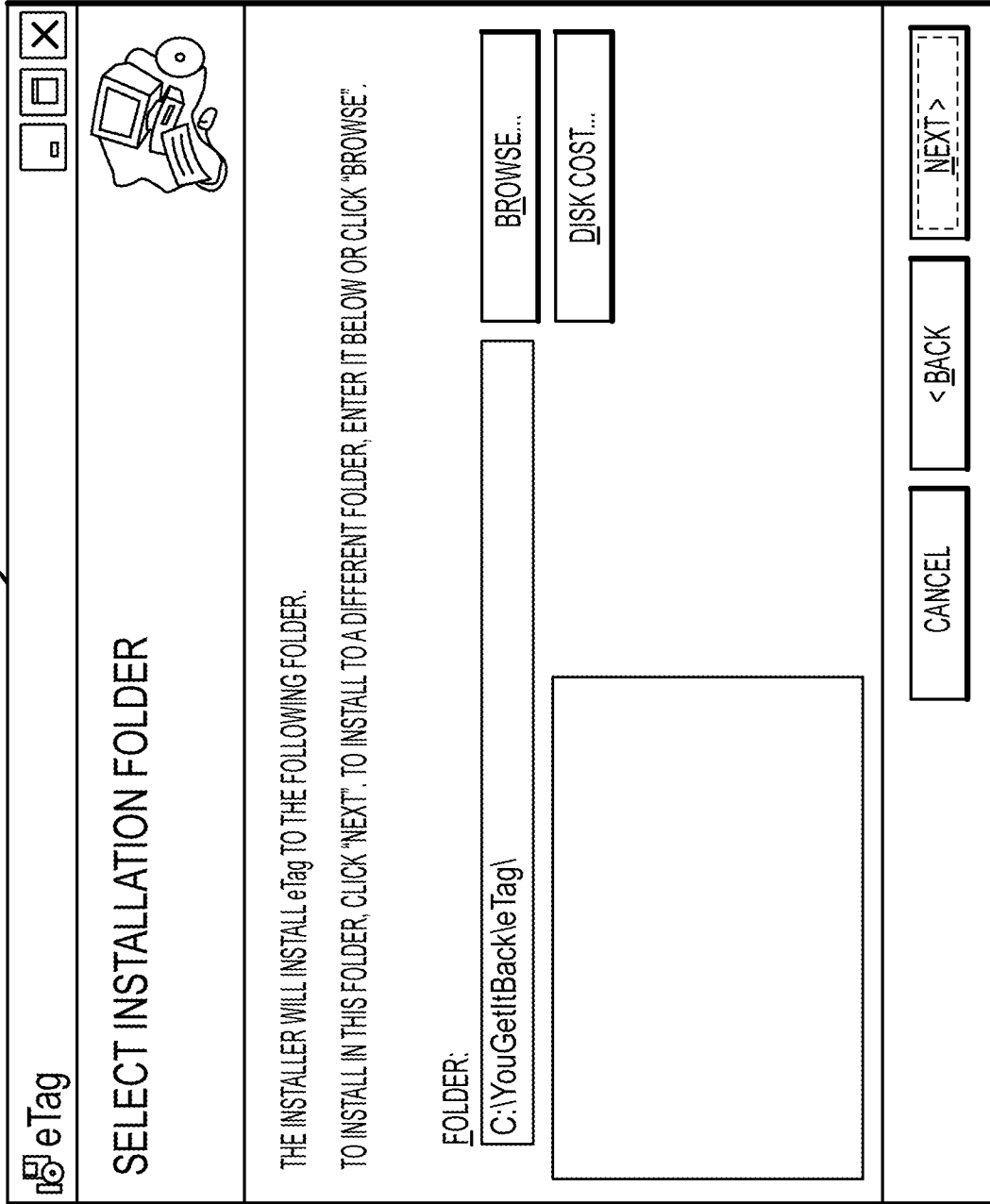


FIGURE 40

4100

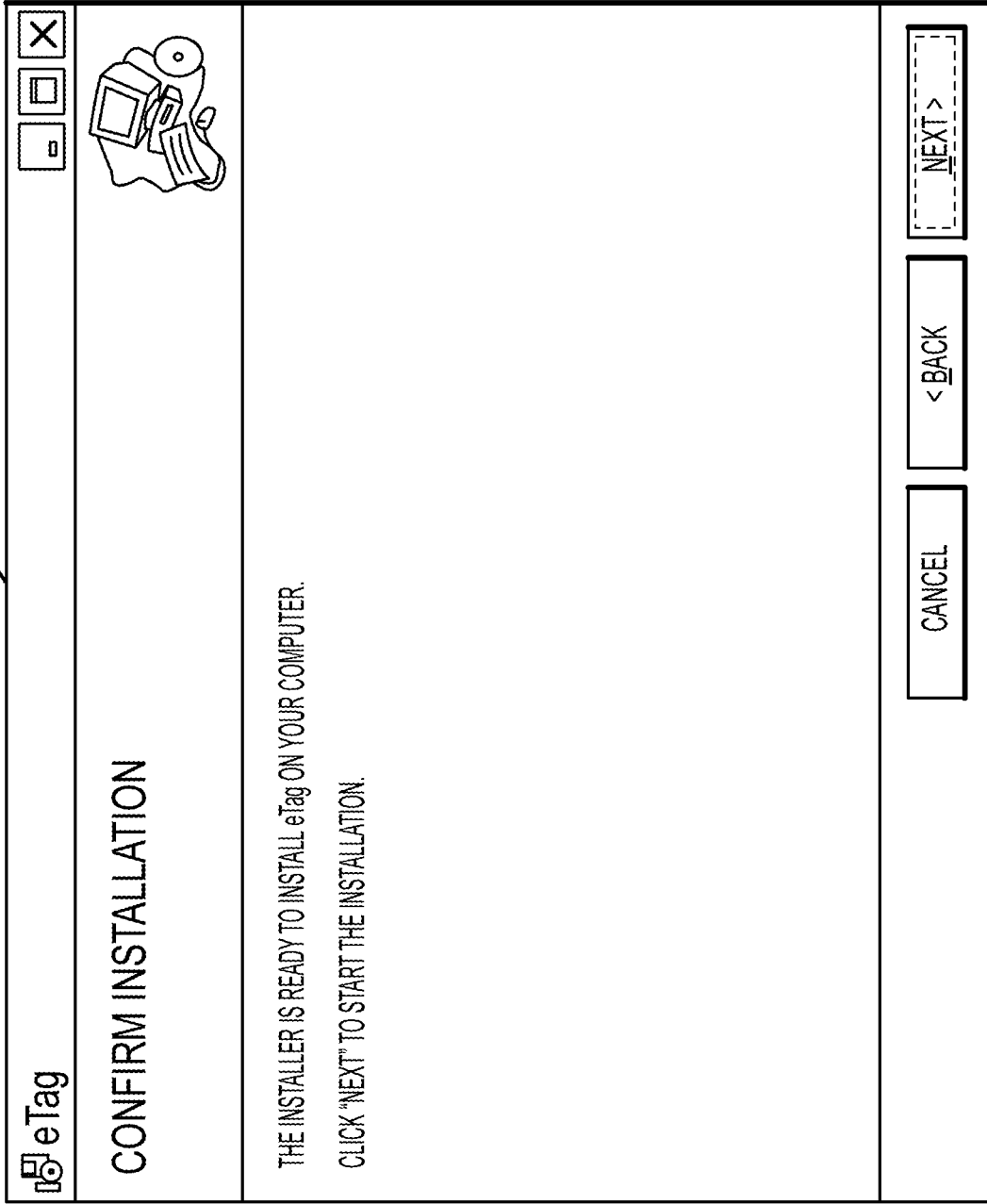


FIGURE 41

4200

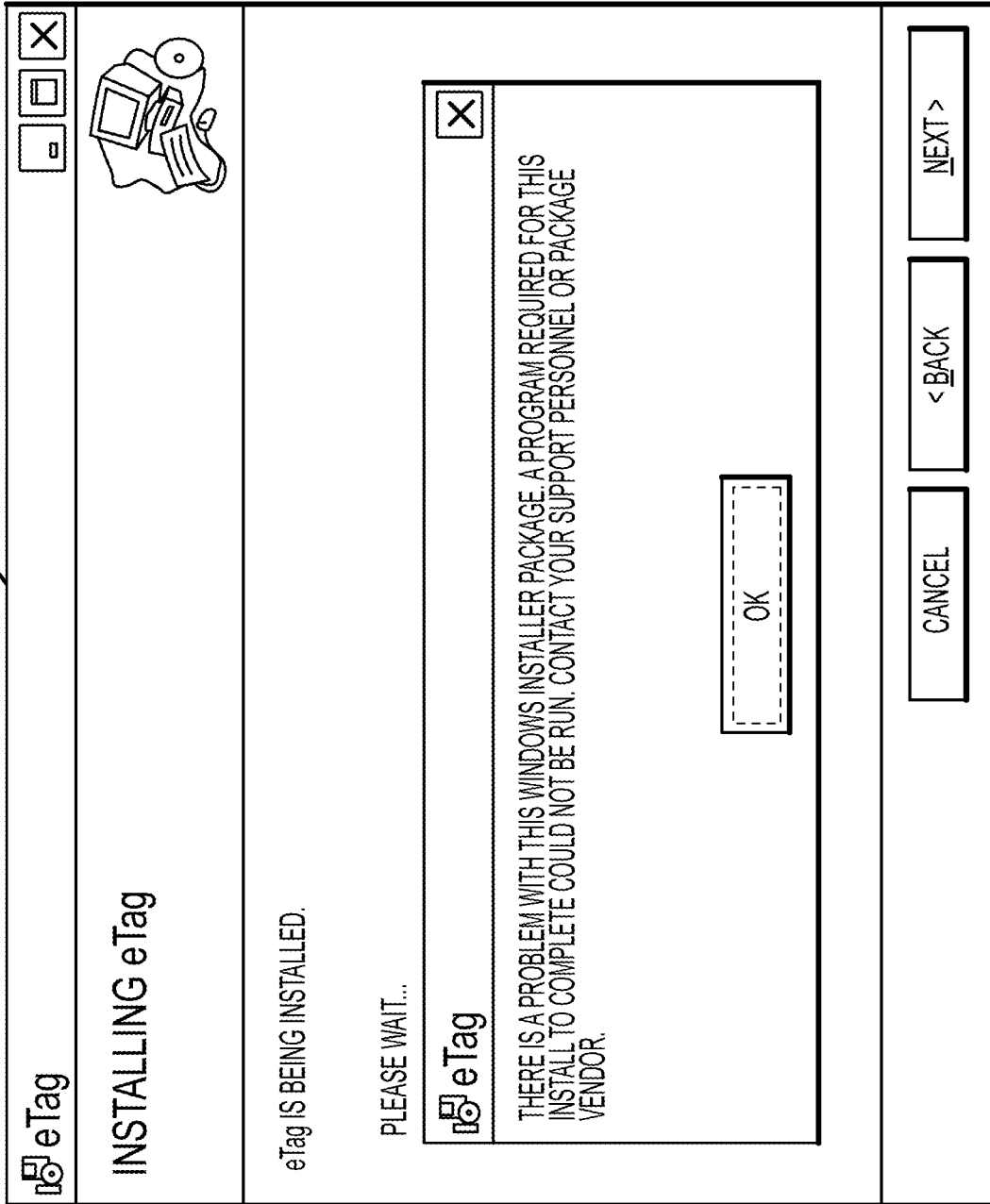


FIGURE 42

4300

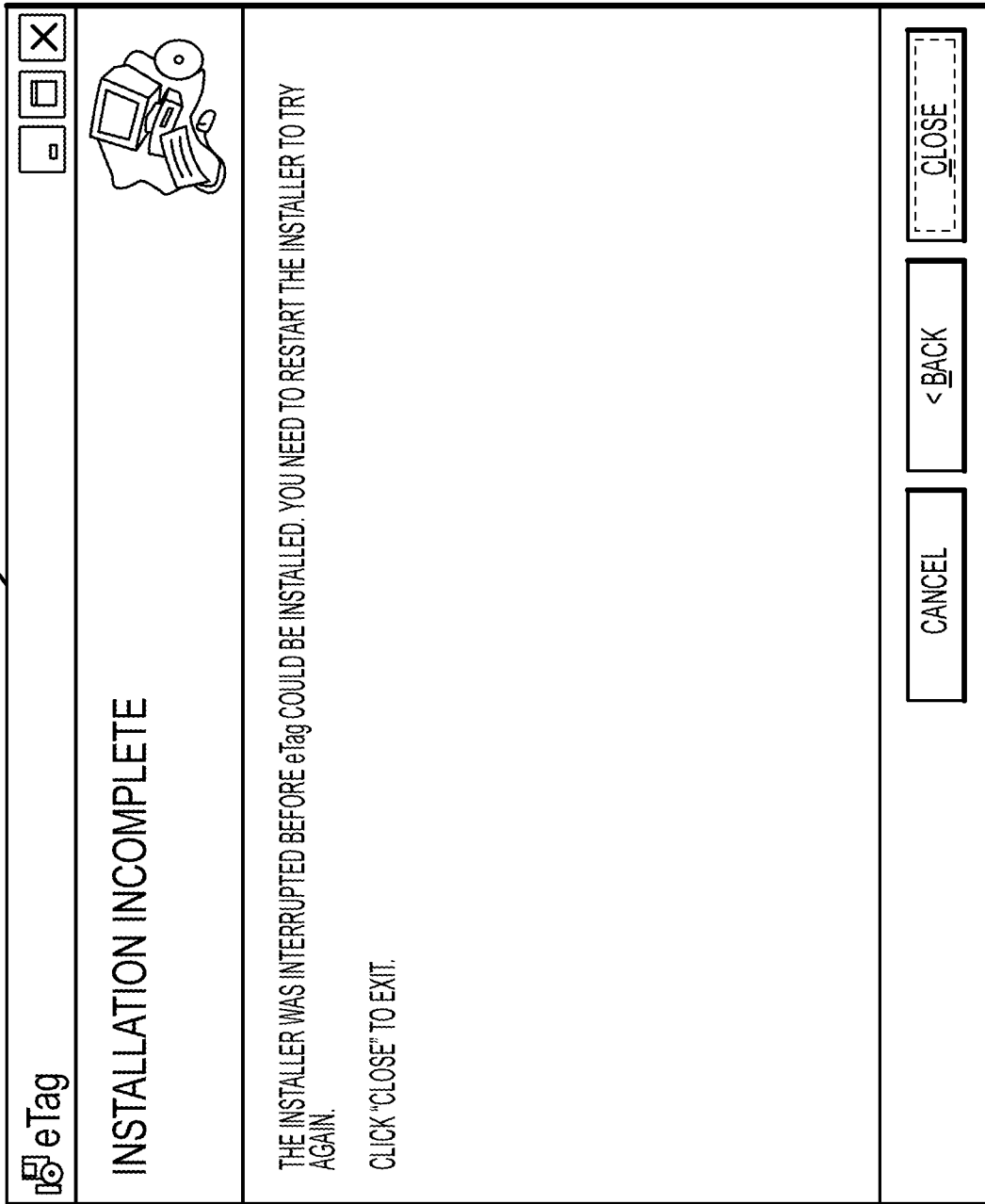


FIGURE 43

4400

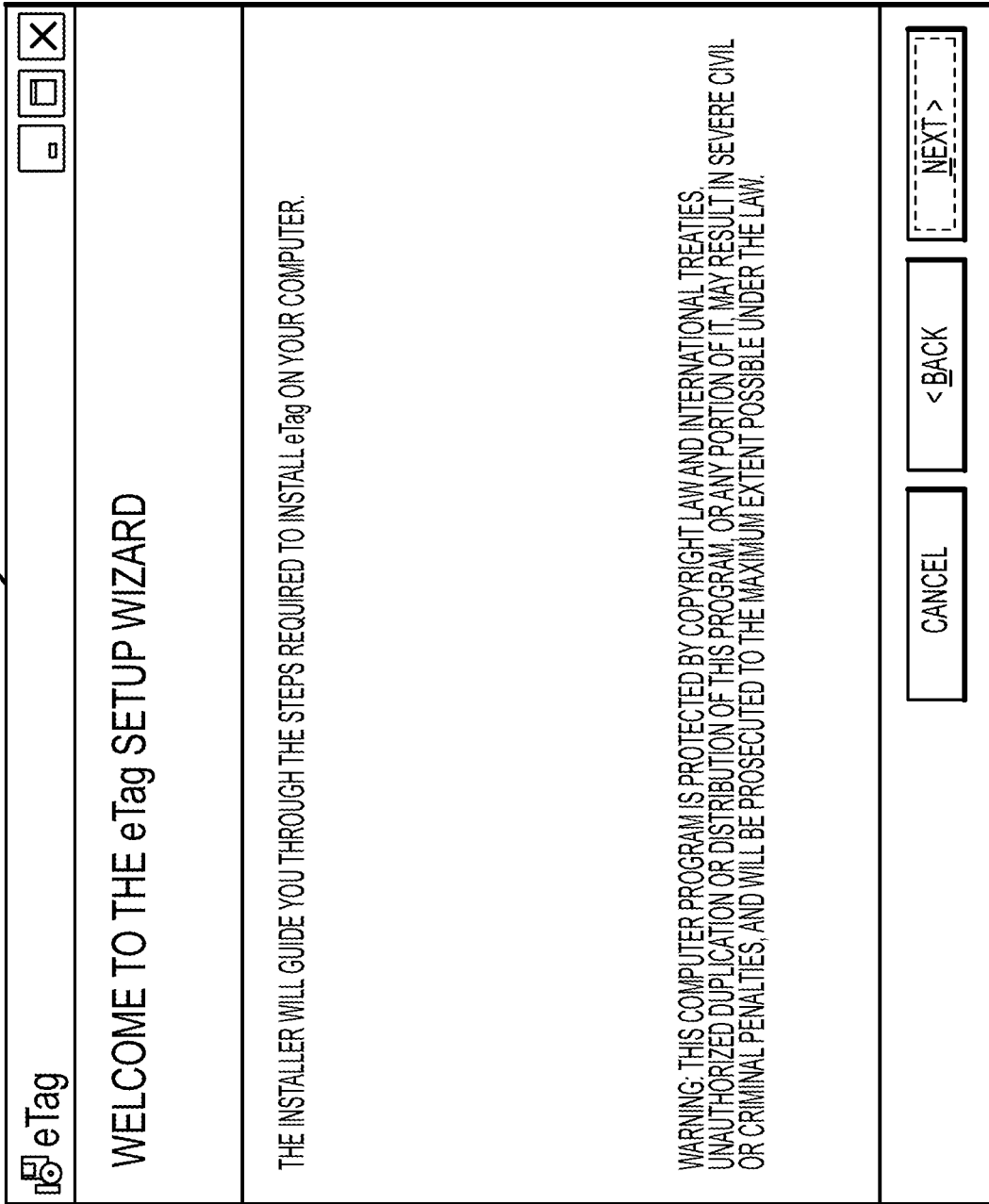


FIGURE 44



4500

**eTag**

**LICENSE AGREEMENT**

PLEASE TAKE A MOMENT TO READ THE LICENSE AGREEMENT NOW. IF YOU ACCEPT THE TERMS BELOW, CLICK "I AGREE", THEN "NEXT". OTHERWISE CLICK "CANCEL".

WHICH IS THE PRINCIPAL PLACE OF BUSINESS OF THE END-USER AND WHERE THE SOFTWARE WILL BE INSTALLED AND USED;

"TERM" MEANS THE PERIOD OF DURATION OF THIS END-USER LICENCE AS SPECIFIED IN THE SALES ORDER FORM;

"SALES ORDER FORM" MEANS THE STANDARD YOUGETITBACK LIMITED END-USER ORDER FORM AS COMPLETED BY THE YOUGETITBACK LIMITED CERTIFIED RESELLER;

I DO NOT AGREE       I AGREE

FIGURE 45

4600

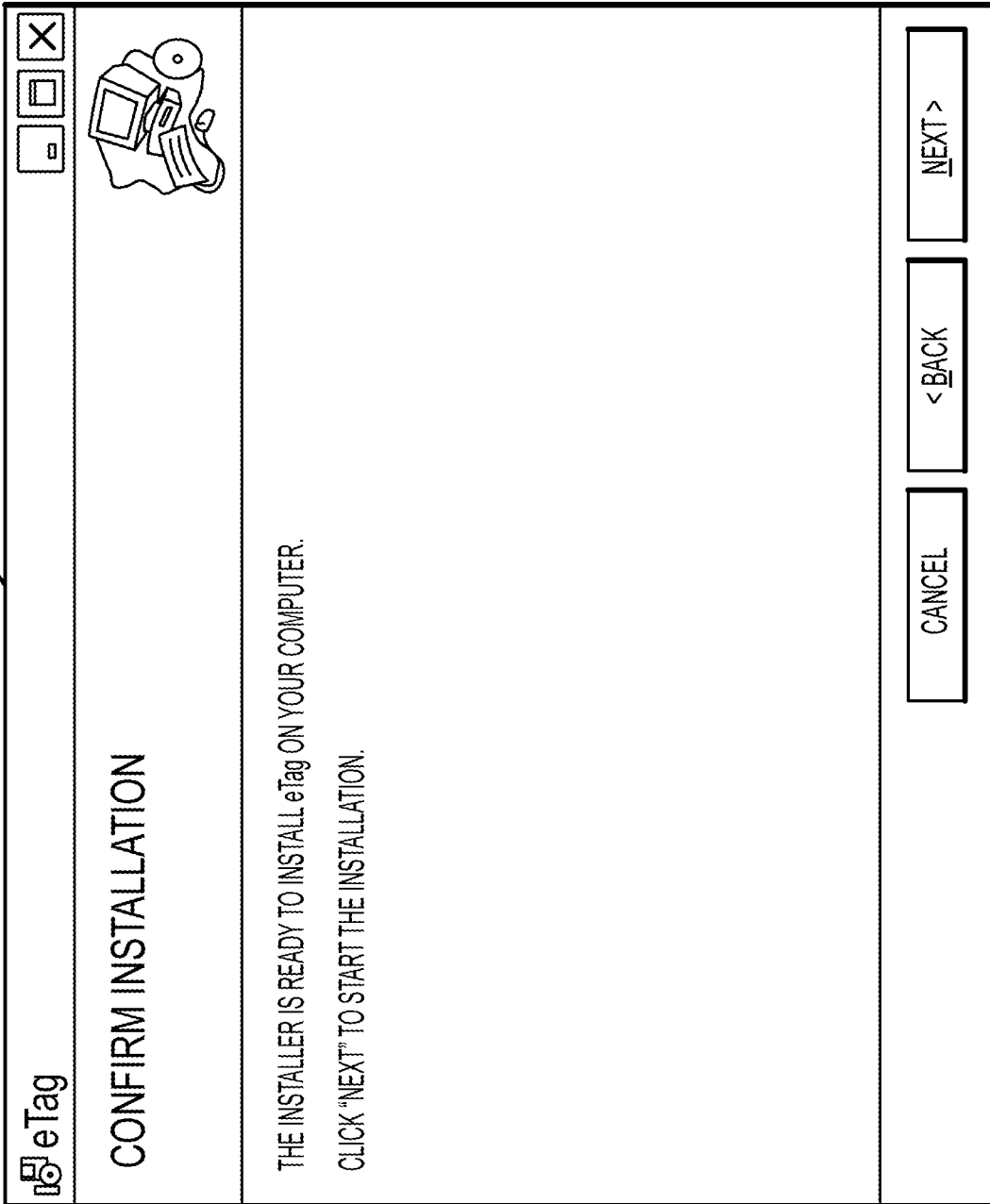


FIGURE 46

47/64

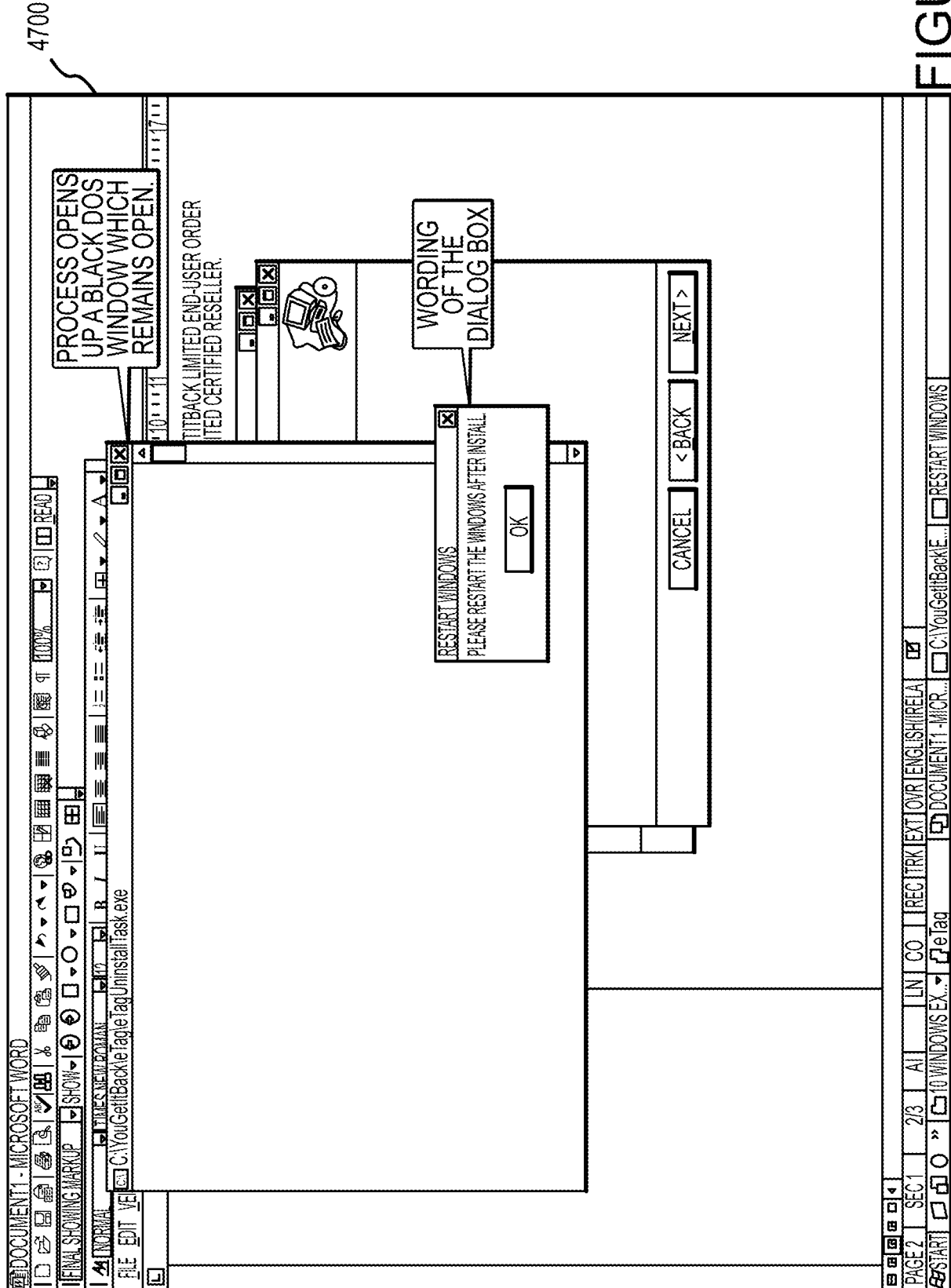


FIGURE 47

4800

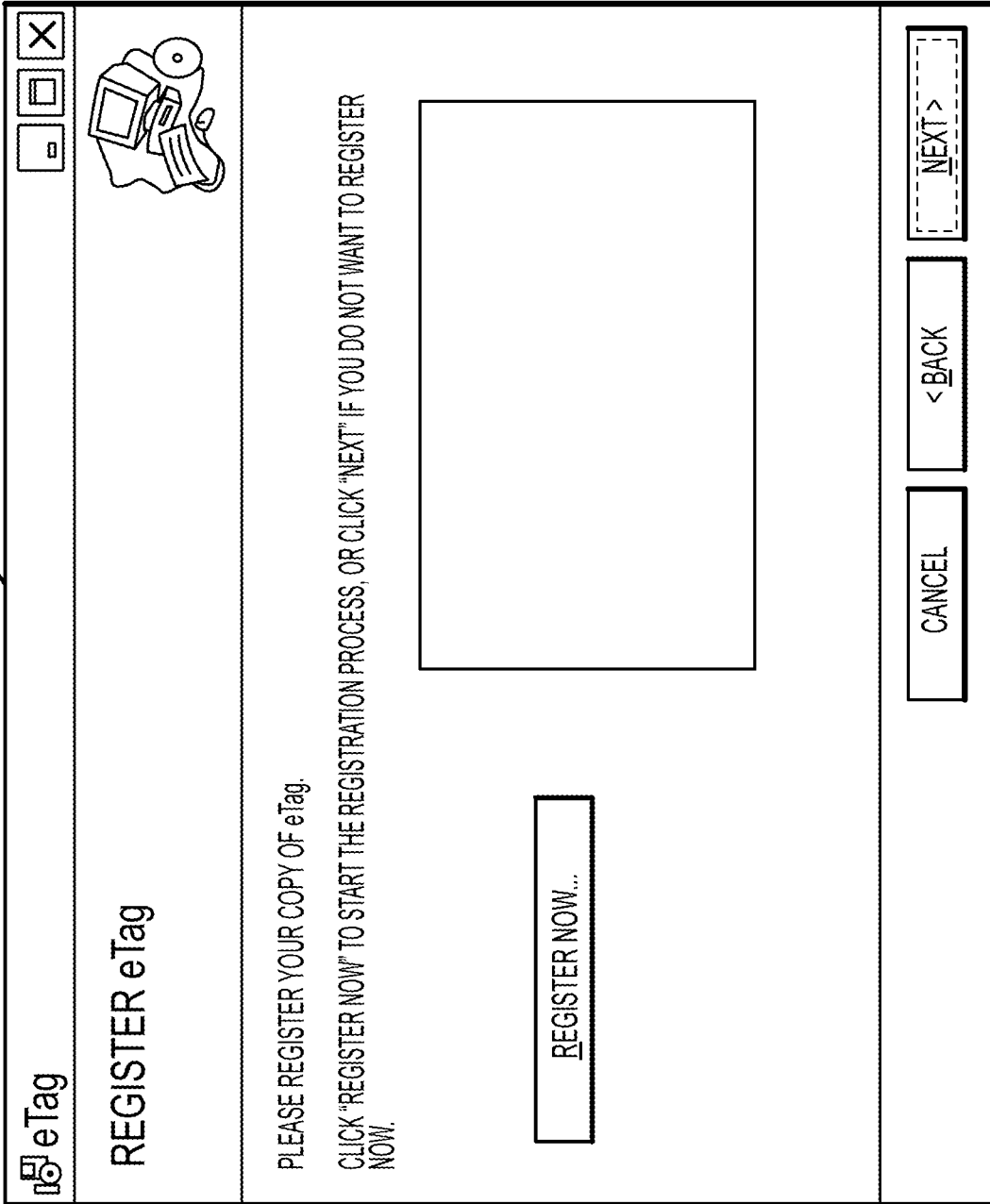
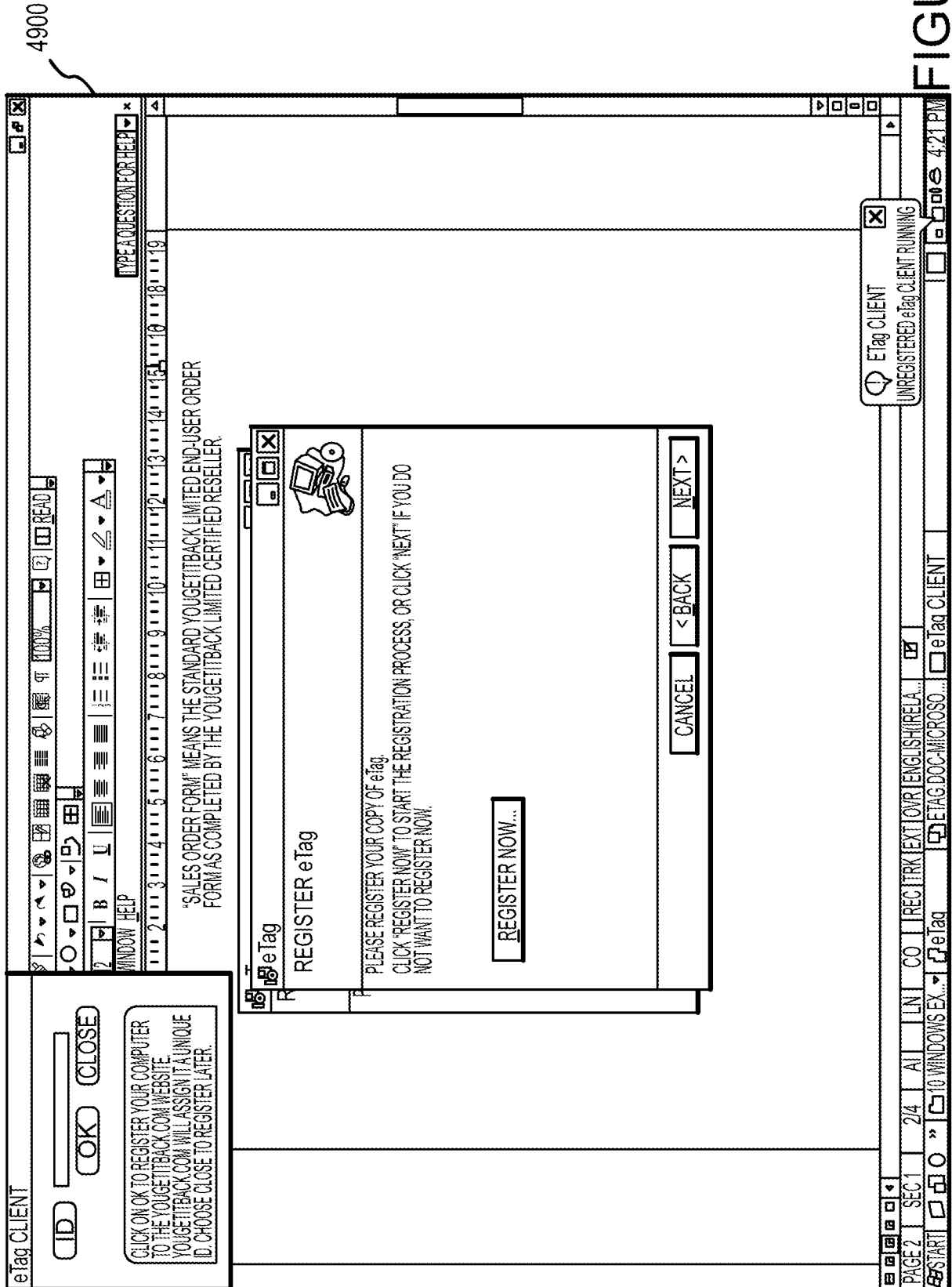


FIGURE 48



4900

FIGURE 49

50/64

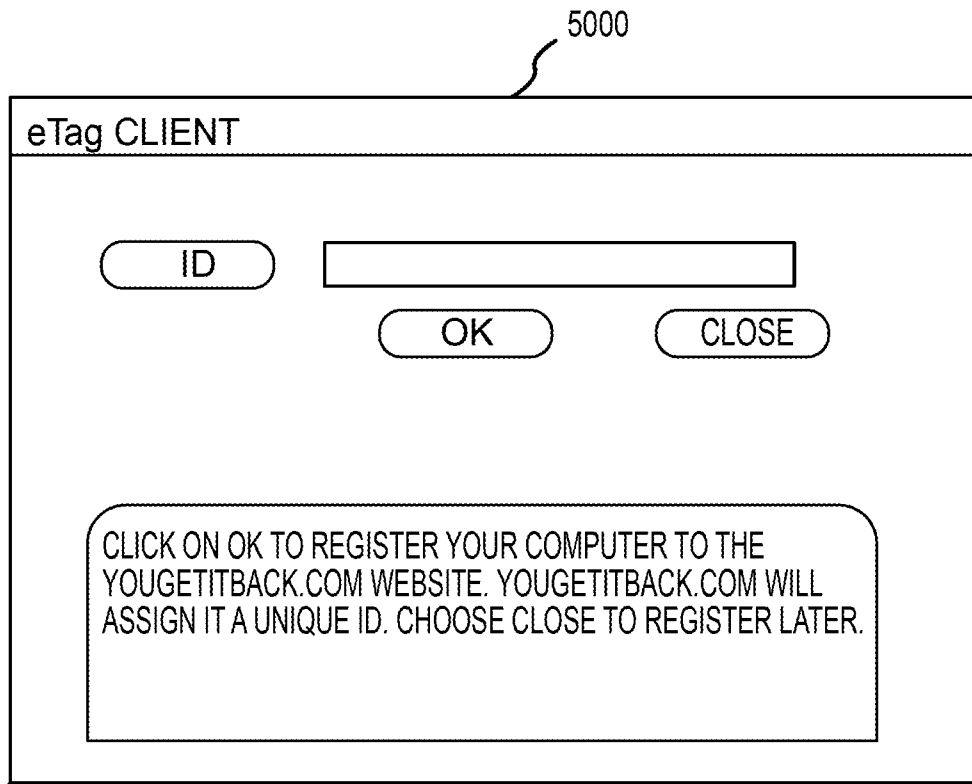


FIGURE 50

51/64

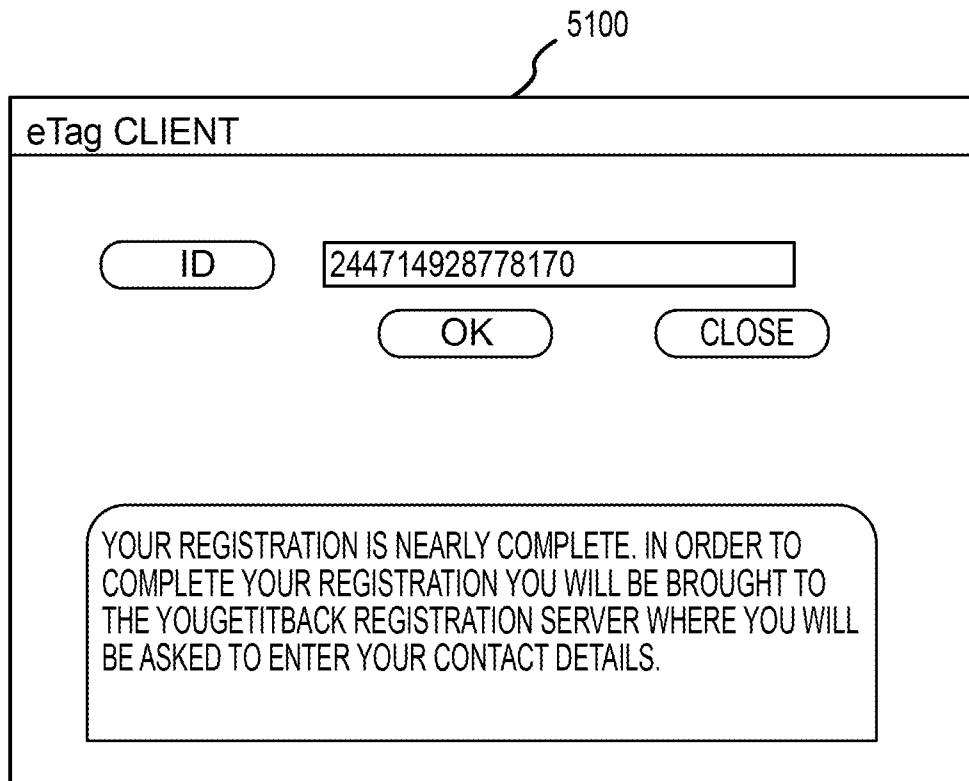


FIGURE 51

52/64

5200

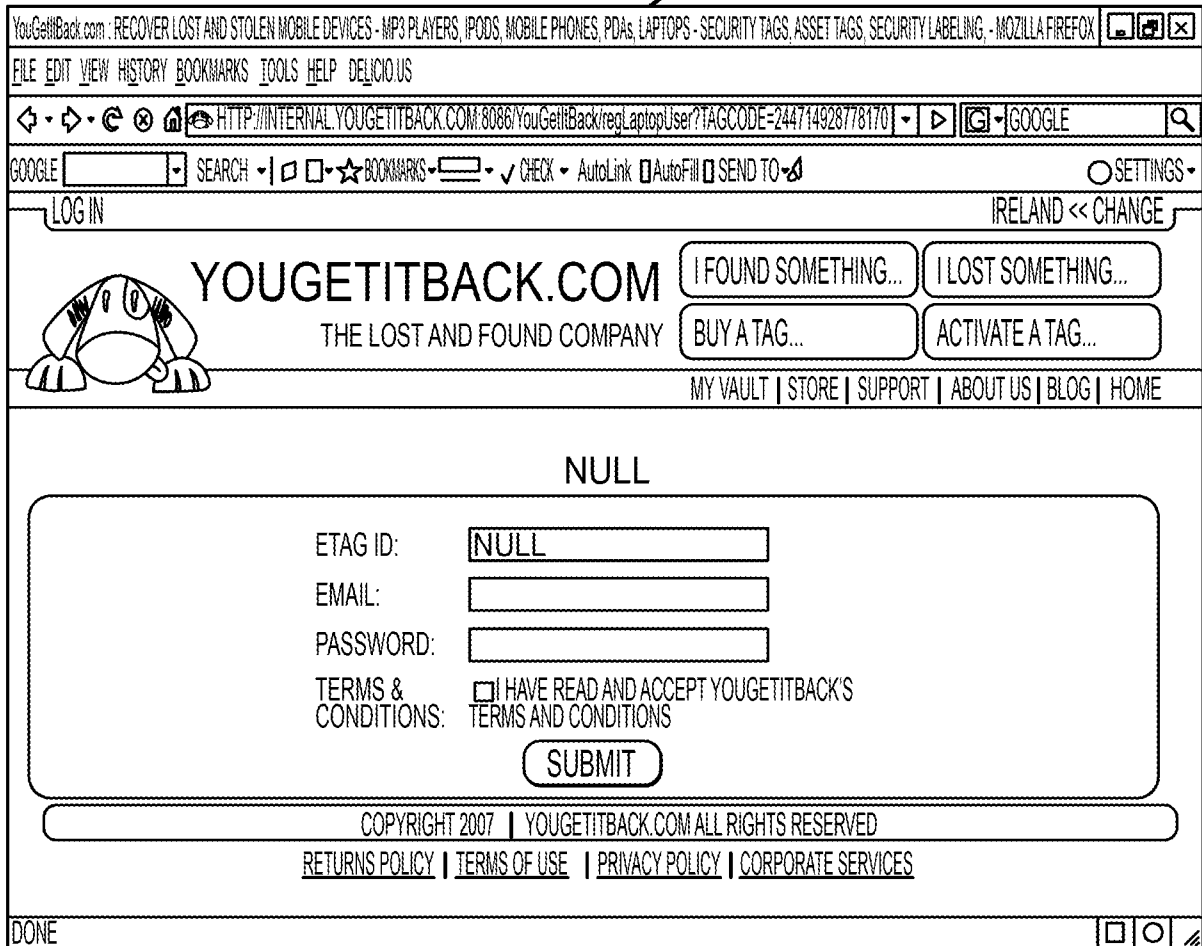


FIGURE 52



53/64

5300

The screenshot displays the YouGetItBack.com website within a Mozilla Firefox browser window. The browser's address bar shows the URL: <http://internal.yougetitback.com:8086/YouGetItBack/regLaptopUser.jsessionid=CD23AB1C8458882E08277AA171BFD381>. The page header includes the site name and navigation links like 'FILE', 'EDIT', 'VIEW', 'HISTORY', 'BOOKMARKS', 'TOOLS', 'HELP', and 'DELICIOUS'. A user is logged in as 'JOHNP@SOMCH.COM USER' with a 'LOGOUT' option. The main navigation menu includes 'I FOUND SOMETHING...', 'I LOST SOMETHING...', 'BUY A TAG...', and 'ACTIVATE A TAG...'. A central banner reads 'WITH YOUGETITBACK.COM, UP TO 75% OF ALL LOST ITEMS GET RETURNED.' Below this is a form to 'ACTIVATE YOUR LOST & FOUND SERVICE!' with a 'SUBMIT' button and the text 'BE INSTANTLY NOTIFIED WHEN SOMEONE FINDS YOUR STUFF!'. A second banner features a 'REWARD FOR RETURN' tag with ID number '1000000001' and the slogan 'PROTECT YOUR STUFF!' with icons for a mobile phone, laptop, CD player, and camera. This section promotes the 'YOUGETITBACK VAULT' for storing important details like PUK codes and warranty info, with 'SIGN UP' and 'MORE INFO...' buttons. The footer contains copyright information for 2007 and links to 'RETURNS POLICY', 'TERMS OF USE', 'PRIVACY POLICY', and 'CORPORATE SERVICES'. The browser status bar at the bottom shows 'DONE'.

FIGURE 53

54/64

5400

YouGetItBack.com: RECOVER LOST AND STOLEN MOBILE DEVICES - MP3 PLAYERS, IPODS, MOBILE PHONES, PDAs, LAPTOPS - SECURITY TAGS, ASSET TAGS, SECURITY LABELING - MOZILLA FIREFOX

FILE EDIT VIEW HISTORY BOOKMARKS TOOLS HELP DELICIOUS

HTTP://INTERNAL.YOUGETITBACK.COM:30986/YouGetItBack/res/LaptopUser.js?SESSIONID=CD23AB1C8458882E08277A4171BF0381

GOOGLE SEARCH BOOKMARKS CHECK AutoLink AutoFill SEND TO SETTINGS

YOU ARE LOGGED IN AS JOHN@SOMCH.COM USER | LOGOUT IRELAND << CHANGE

**YOUGETITBACK.COM** THE LOST AND FOUND COMPANY

I FOUND SOMETHING... I LOST SOMETHING...  
BUY A TAG... ACTIVATE A TAG...


MY VAULT | STORE | SUPPORT | ABOUT US | BLOG | HOME

WITH YOUGETITBACK.COM, UP TO 75% OF ALL LOST ITEMS GET RETURNED.

\* TAG ID:   **ACTIVATE YOUR LOST & FOUND SERVICE!**  
BE INSTANTLY NOTIFIED WHEN SOMEONE FINDS YOUR STUFF!

REWARD FOR RETURN 1800 238 0695  
ID NO: 1000000001  
YOUGETITBACK.COM

PROTECT YOUR STUFF!



**YOUGETITBACK.COM**  
LOST ITEMS WHICH ARE TAGGED WITH A YOUGETITBACK TAG ARE MUCH MORE LIKELY TO BE RETURNED TO YOU!  
REGISTERED USERS ARE ALERTED IMMEDIATELY WHEN THEIR STUFF IS FOUND.  
TAG YOUR STUFF NOW FOR PEACE OF MIND!  
 

**SIGN UP FOR FREE AND START USING THE YOUGETITBACK VAULT!**  
FIND IT HARD TO REMEMBER IMPORTANT DETAILS ABOUT YOUR BELONGINGS? MOBILE - PUK CODES AND PIN NUMBERS. CAR KEYS, SERIAL NUMBERS, WARRANTY INFO!  
USE THE VAULT TO STORE THESE DETAILS AND MANAGE ALL YOUR TAGGED ITEMS ALL IN ONE PLACE.  
 

COPYRIGHT 2007 | YOUGETITBACK.COM ALL RIGHTS RESERVED  
RETURNS POLICY | TERMS OF USE | PRIVACY POLICY | CORPORATE SERVICES

DONE

FIGURE 54

55/64

5500

YOU ARE LOGGED IN AS JOHN.P@SOMCH.COM USER | LOGOUT IRELAND << CHANGE



**YOUGETITBACK.COM**

THE LOST AND FOUND COMPANY

I FOUND SOMETHING...

I LOST SOMETHING...

BUY A TAG...

ACTIVATE A TAG...

[MY VAULT](#) | [STORE](#) | [SUPPORT](#) | [ABOUT US](#) | [BLOG](#) | [HOME](#)

---

WITH YOUGETITBACK.COM, UP TO 75% OF ALL LOST ITEMS GET RETURNED.

\* TAG ID:

DID NOT ACCEPT THE TAG ID

Ⓛ THE LABEL ID MUST BE 9, 11 OR 12 CHARACTERS LONG

SUBMIT

ACTIVATE YOUR LOST & FOUND SERVICE!

BE INSTANTLY NOTIFIED WHEN SOMEONE FINDS YOUR STUFF!

REWARD FOR RETURN  
1800 238 0695

ID NO: 1000000001  
YOUGETITBACK.COM

PROTECT YOUR STUFF!

**YOUGETITBACK.COM**

LOST ITEMS WHICH ARE TAGGED WITH A YOUGETITBACK TAG ARE MUCH MORE LIKELY TO BE RETURNED TO YOU!

REGISTERED USERS ARE ALERTED IMMEDIATELY WHEN THEIR STUFF IS FOUND.

TAG YOUR STUFF NOW FOR PEACE OF MIND!

BUY TAGS

MORE INFO...

SIGN UP FOR FREE AND START USING THE YOUGETITBACK VAULT!

FIND IT HARD TO REMEMBER IMPORTANT DETAILS ABOUT YOUR BELONGINGS? MOBILE - PUK CODES AND PIN NUMBERS, CAR KEYS, SERIAL NUMBERS, WARRANTY INFO!

USE THE VAULT TO STORE THESE DETAILS AND MANAGE ALL YOUR TAGGED ITEMS ALL IN ONE PLACE.

SIGN UP

MORE INFO...


---

COPYRIGHT 2007 | YOUGETITBACK.COM ALL RIGHTS RESERVED

[RETURNS POLICY](#) | [TERMS OF USE](#) | [PRIVACY POLICY](#) | [CORPORATE SERVICES](#)

FIGURE 55

YOU ARE LOGGED IN AS JOHN PRENDERGAST | LOGOUT IRELAND << CHANGE



# YOU GET IT BACK.COM

THE LOST AND FOUND COMPANY

I FOUND SOMETHING...

I LOST SOMETHING...

BUY A TAG...

ACTIVATE A TAG...

MY VAULT | STORE | SUPPORT | ABOUT US | NEWS | BLOG | HOME

MY VAULT

ACTIVATE A TAG

MY PROFILE

EMAIL TAG LIST

## MY VAULT:

CREATE NEW ITEM >>

	DESCRIPTION	TAG ID	SubCategory	
①	PASSPORT	MCP001662	PASSPORTS	<span style="border: 1px solid black; padding: 2px 5px; border-radius: 5px;">MORE &gt;&gt;</span>

PASSPORT 9

REPORT ITEM LOST
DELETE ITEM

STATUS:

DESCRIPTION:

TAG ID:

ACTIVATED:

EXPIRES:

CATEGORY:  ▼

MAKE:

MODEL:

SERIAL NUMBER:

COMMENTS:

REWARD:  ▼

SUBMIT

	DESCRIPTION ▼	TAG ID ▼	SubCategory	
⊗		TTT111006	2 WAY RADIOS	<span style="border: 1px solid black; padding: 2px 5px; border-radius: 5px;">MORE &gt;&gt;</span>
⊙	LAPTOP	MCP001766	LAPTOPS	<span style="border: 1px solid black; padding: 2px 5px; border-radius: 5px;">MORE &gt;&gt;</span>
①	TESTD	TTT111005	2 WAY RADIOS	<span style="border: 1px solid black; padding: 2px 5px; border-radius: 5px;">MORE &gt;&gt;</span>
⊙	TEST FREE TAG	NOT ACTIVATED	2 WAY RADIOS	<span style="border: 1px solid black; padding: 2px 5px; border-radius: 5px;">MORE &gt;&gt;</span>

COPYRIGHT 2007 | YOU GET IT BACK.COM ALL RIGHTS RESERVED

[RETURNS POLICY](#) | 
 [TERMS OF USE](#) | 
 [PRIVACY POLICY](#) | 
 [CORPORATE SERVICES](#)


FIGURE 56

57/64

5700

YOU ARE LOGGED IN AS JOHN PRENDERGAST | LOGOUT IRELAND << CHANGE

---



## YOUGETITBACK.COM

THE LOST AND FOUND COMPANY

---

[MY VAULT](#) | [STORE](#) | [SUPPORT](#) | [ABOUT US](#) | [NEWS](#) | [BLOG](#) | [HOME](#)

MY VAULT

ACTIVATE A TAG

MY PROFILE

EMAIL TAG LIST

### REPORT LOST TAG

ITEM LOST/FOUND

LABEL NUMBER

CATEGORY

DESCRIPTION

MAKE

MODEL

SERIAL NUMBER

OPTIONAL REWARD

COMMENTS

STATUS

---


COPYRIGHT 2007 | YOUGETITBACK.COM ALL RIGHTS RESERVED  
[RETURNS POLICY](#) | [TERMS OF USE](#) | [PRIVACY POLICY](#) | [CORPORATE SERVICES](#)

FIGURE 57

58/64

5800

LOG IN IRELAND << CHANGE

 **YOUGETITBACK.COM** I FOUND SOMETHING... I LOST SOMETHING...  
THE LOST AND FOUND COMPANY BUY A TAG... ACTIVATE A TAG...

MY VAULT | STORE | SUPPORT | ABOUT US | NEWS | BLOG | HOME

### REPORT FOUND ITEM

- THIS LABEL HAS BEEN REPORTED FOUND. YOU WILL BE CONTACTED BY OUR STAFF TO ARRANGE RETURN OF THE ITEM, AND DELIVERY OF YOUR REWARD.

-----

TYPE YOUR LABEL ID HERE!  (REPORT THIS ITEM AS FOUND!)

COPYRIGHT 2007 | YOUGETITBACK.COM ALL RIGHTS RESERVED  
[RETURNS POLICY](#) | [TERMS OF USE](#) | [PRIVACY POLICY](#) | [CORPORATE SERVICES](#)

FIGURE 58

5900

**ADD OR REMOVE PROGRAMS**

**CURRENTLY INSTALLED PROGRAMS:**

SHOW UPDATES    SORT BY: NAME

PROGRAM NAME	SIZE	USED
DELL 9000 PLOTTER	100.00MB	
DIA (REMOVE ONLY)	48.11MB	
DIGITAL LINE DETECT	0.24MB	
EPSON ADVANCED PRINTER DRIVER 3	24.07MB	
eTag	0.66MB	
CLICK HERE FOR SUPPORT INFORMATION.		
TO CHANGE THIS PROGRAM OR REMOVE IT FROM YOUR COMPUTER, CLICK CHANGE OR REMOVE.		
FileMaker PRO 8 ADVANCED	377.00MB	
FogBugz SCREENSHOT	0.41MB	
GOOGLE AdWords EDITOR	40.62MB	
GOOGLE SketchUp 6	49.71MB	
GOOGLE TALK (REMOVE ONLY)	5.08MB	
GOOGLE TOOLBAR FOR INTERNET EXPLORER	104.00MB	
IKEA HomePlanner KITCHEN	35.45MB	
INTEL(R) PROSet/WIRELESS SOFTWARE	8.74MB	
INTERNAL NETWORK CARD POWER MANAGEMENT	0.59MB	
IfanView (REMOVE ONLY)	1.34MB	
iTunes	72.59MB	
JAVA 2 RUNTIME ENVIRONMENT, SE V1.4.2_03	136.00MB	
MICROSOFT .NET FRAMEWORK 1.1		
MICROSOFT .NET FRAMEWORK 1.1 HOTFIX (KB928366)		

**CHANGE OR REMOVE PROGRAMS**

**ADD NEW PROGRAMS**

**ADD/REMOVE WINDOWS COMPONENTS**

**SET PROGRAM ACCESS AND DEFAULTS**

FIGURE 59

60/64

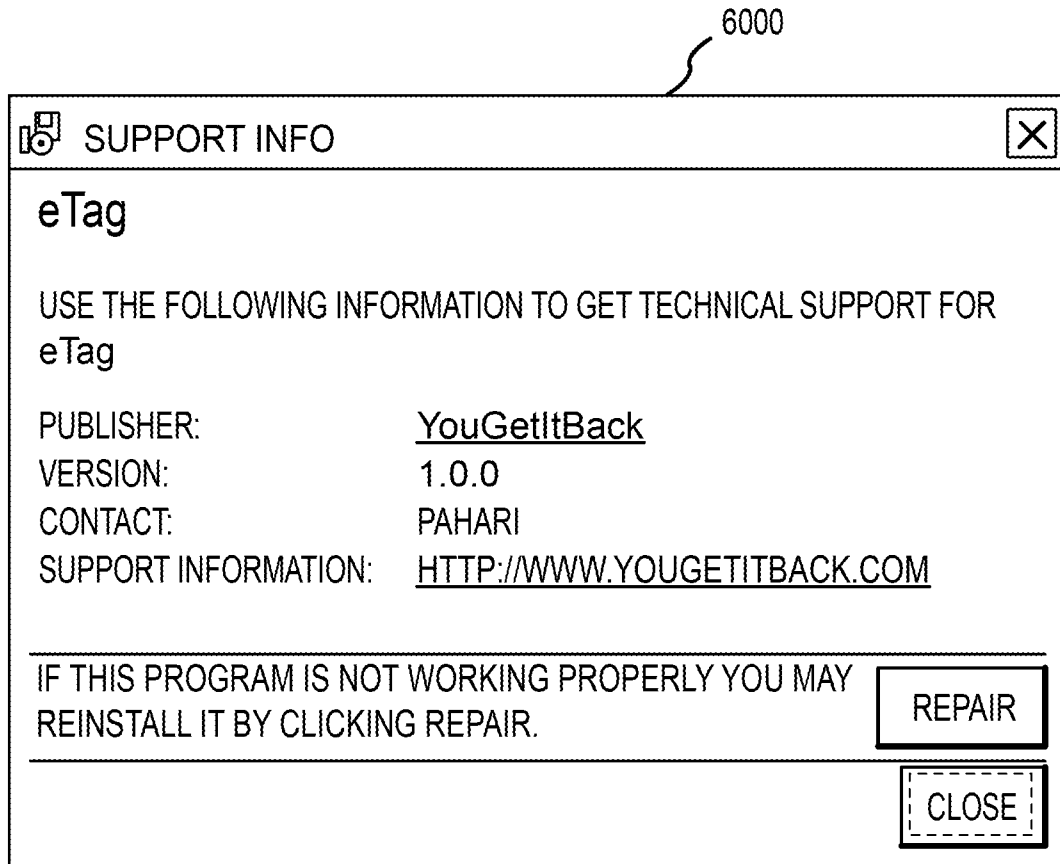


FIGURE 60



61/64

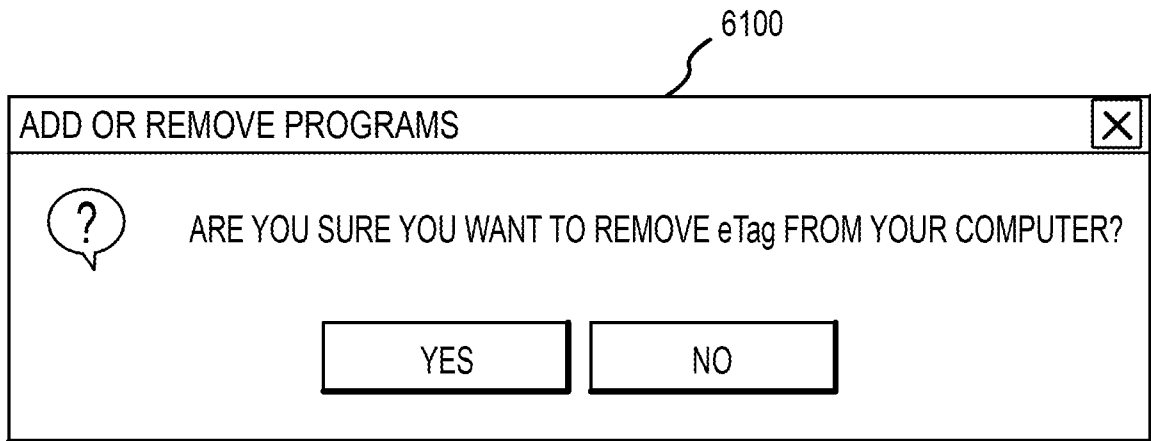


FIGURE 61

62/64

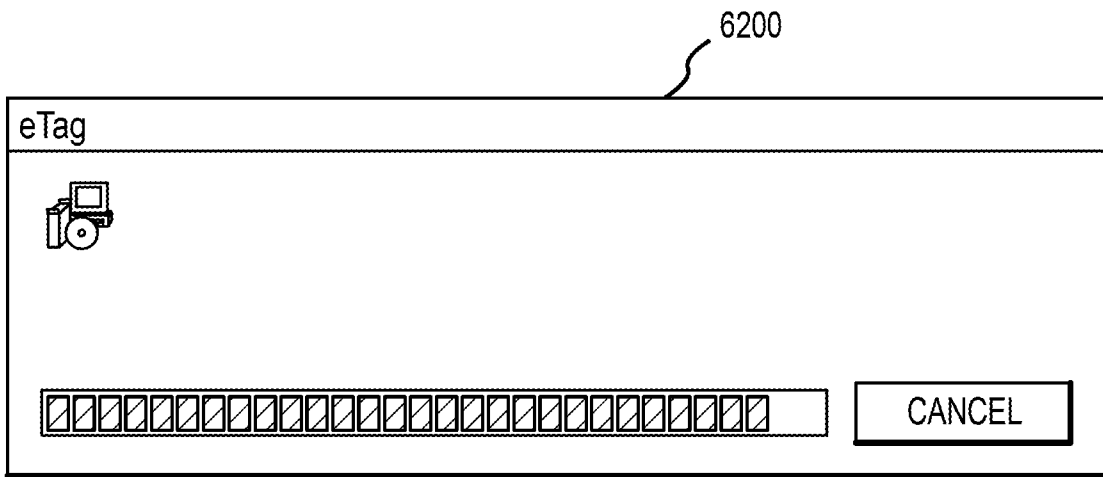


FIGURE 62

6300

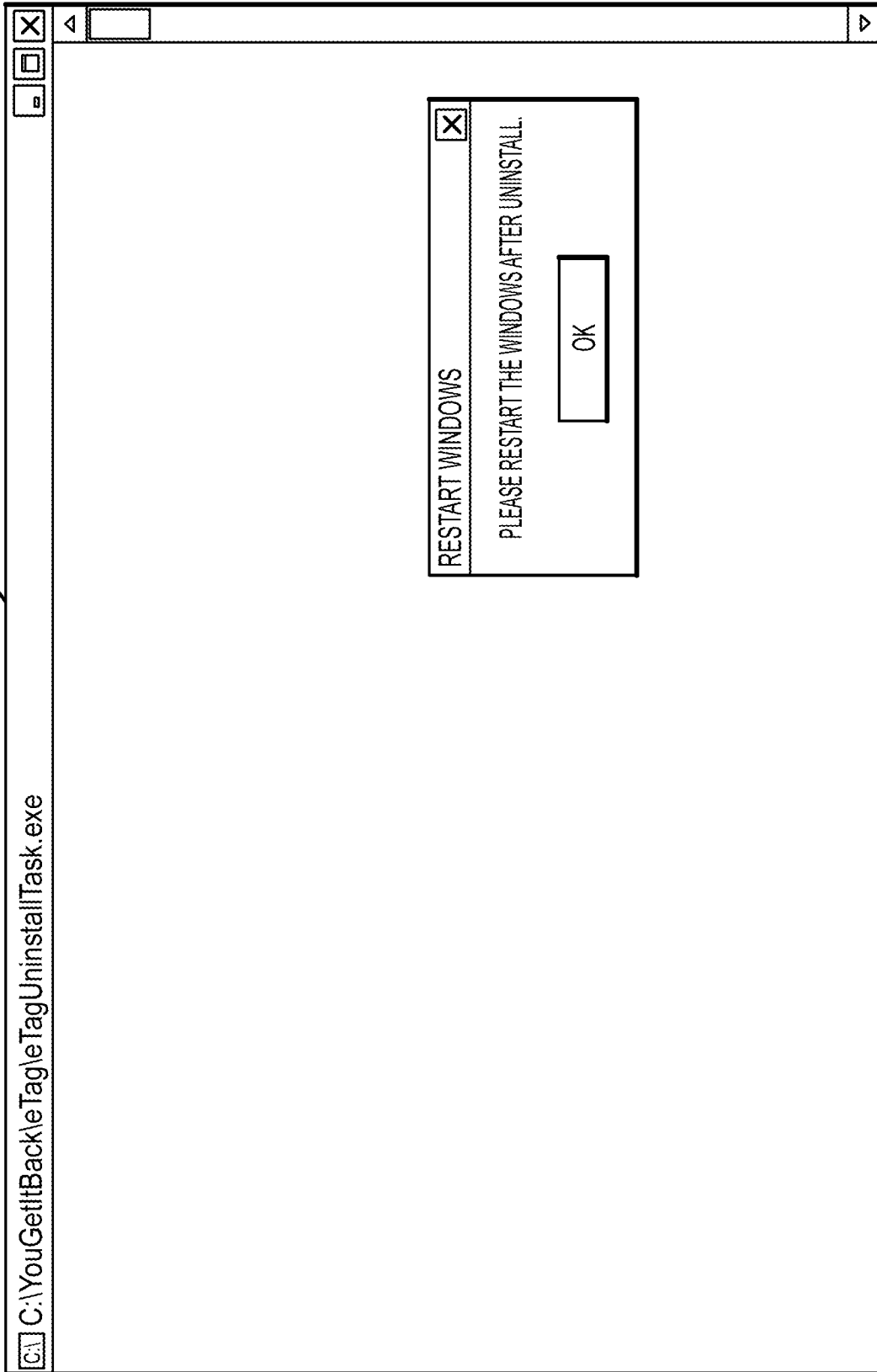


FIGURE 63

6400

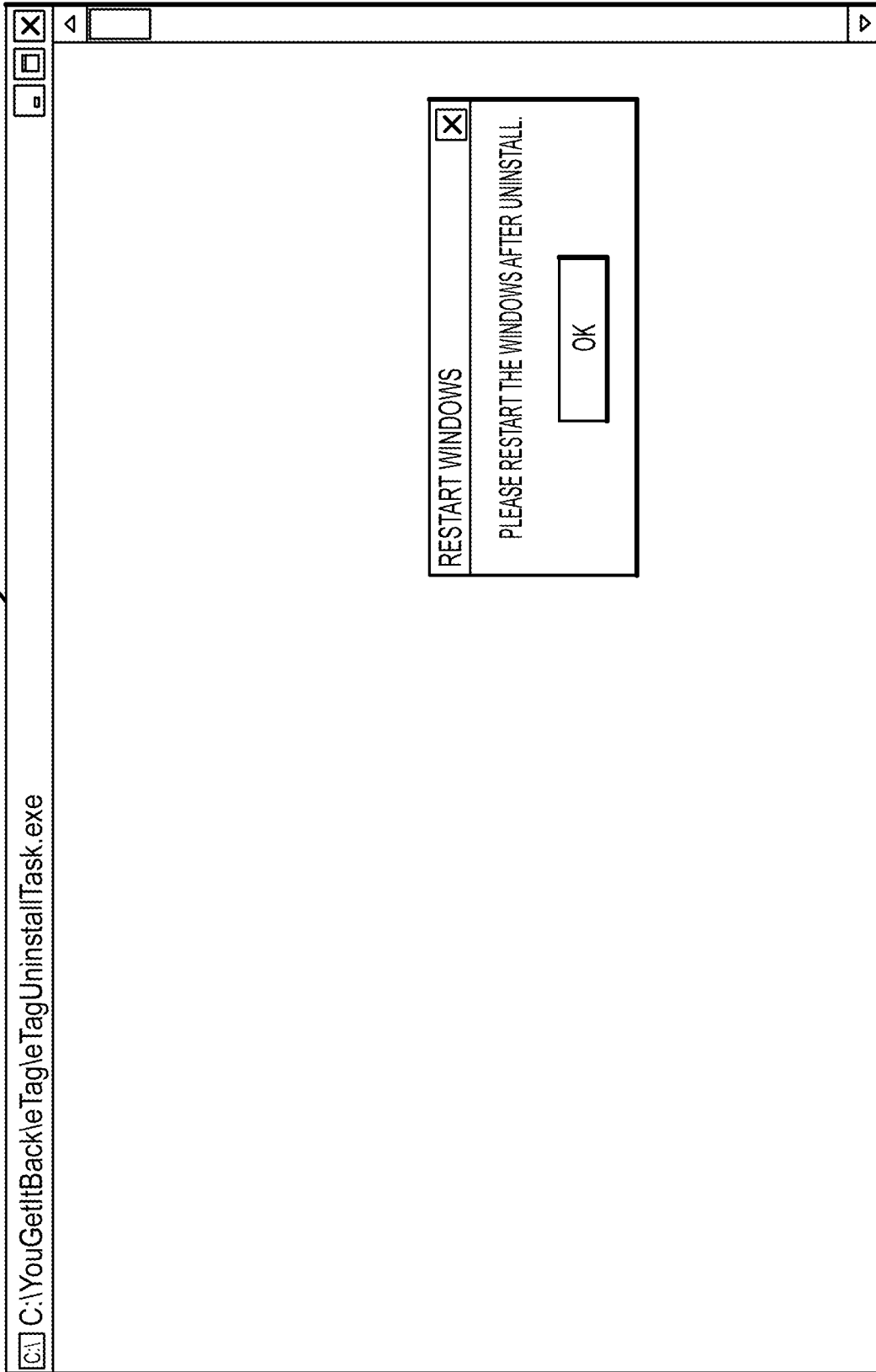


FIGURE 64