FILED

2012 MAY 16 PM 12: 15

CLERK U.S. DISTRICT COURT
CENTRAL DIST. OF CALIF.
LOS ANGELES

KRIS LE FAN, ESQ. (SBN 278611)
LAW OFFICE OF KRIS LE FAN
433 North Camden Drive, Sixth Floor
Beverly Hills, California 90210
Telephone: (213) 290-1091
krislefanesquire@gmail.com

Attorney for Plaintiff, WOLF RUN HOLLOW, LLC

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

LOS ANGELES DIVISION

WOLF RUN HOLLOW, LLC,

Plaintiff,

v.

CITY NATIONAL BANK,

Defendant.

CV12-4255-RSWL(E)

Case No.

COMPLAINT FOR PATENT INFRINGEMENT

Jury Trial Demanded

BY FAX

PLAINTIFF'S ORIGINAL COMPLAINT

Plaintiff Wolf Run Hollow, LLC ("Plaintiff"), by and through its undersigned counsel, files this Original Complaint against City National Bank ("Defendant") as follows:

NATURE OF THE ACTION

1. This is a patent infringement action to stop Defendant's infringement of Plaintiff's United States Patent No. 6,115,817 entitled "*Methods and Systems for Facilitating Transmission of Secure Messages Across Insecure Networks*" (the "'817 patent"; a copy of which is attached hereto as Exhibit A). Plaintiff is the exclusive licensee of the '817 patent with respect to the Defendant. Plaintiff seeks injunctive relief and monetary damages.

PARTIES

2. Plaintiff is a limited liability company organized and existing under the laws of the State of Delaware. Plaintiff maintains its principal place of business at 170 Kinnelon Road, Suite 13, Kinnelon, New Jersey 07405. Plaintiff is the exclusive licensee of the '817 patent with respect to the Defendants, and possesses the right to sue for infringement and recover past damages.

3. Upon information and belief, Defendant is a corporation organized and existing under the laws of the State of Delaware with its principal place of business located at 555 South Flower Street, Los Angeles, California 90071.

JURISDICTION AND VENUE

4. This action arises under the Patent Laws of the United States, 35 U.S.C. § 1 *et seq.*, including 35 U.S.C. §§ 271, 281, 283, 284, and 285. This Court has subject matter jurisdiction over this case for patent infringement under 28 U.S.C. §§ 1331 and 1338(a).

5. The Court has personal jurisdiction over Defendant because: Defendant is present within or has minimum contacts with the State of California and the Central District of California; Defendant has purposefully availed itself of the privileges of conducting business in the State of California and in the Central District of California; Defendant has sought protection and benefit from the laws of the State of California; Defendant regularly conducts business within the State of

California and within the Central District of California; and Plaintiff's causes of action arise directly from Defendants' business contacts and other activities in the State of California and in the Central District of California.

6. More specifically, Defendant, directly and/or through authorized intermediaries, ships, distributes, offers for sale, sells, and/or advertises (including the provision of an interactive web page) its products and services in the United States, the State of California, and the Central District of California. Upon information and belief, Defendant has committed patent infringement in the State of California and in the Central District of California, has contributed to patent infringement in the State of California and in the Central District of California, and/or has induced others to commit patent infringement in the State of California and in the Central District of California. Defendant solicits customers in the State of California and in the Central District of California. Defendant has many paying customers who are residents of the State of California and the Central District of California and who each use each of the respective Defendant's products and services in the State of California and in the Central District of California.

7. Venue is proper in the Central District of California pursuant to 28 U.S.C. §§ 1391 and 1400(b).

COUNT I – PATENT INFRINGEMENT

8. The '817 patent was duly and legally issued by the United States Patent and Trademark Office on September 5, 2000, after full and fair examination for systems and methods for secure messaging on an insecure network. Plaintiff is the exclusive licensee of the '817 patent with respect to the Defendants, and possesses all rights of recovery under the '817 patent with respect to the Defendants, including the right to sue for infringement and recover past damages.

9. Upon information and belief, Defendant has infringed and continues to infringe one or more claims of the '817 patent by making, using, providing, offering to sell, and selling (directly or through intermediaries), in this district and elsewhere in the United States, secure messaging systems and methods that embody the patented invention, including via the website

https://www.cnb.com. Upon information and belief, Defendant directs or requires users to request, utilize, transmit and/or receive secure messages via the secure online banking and/or messaging systems and methods on their website. Upon information and belief, Defendant has also contributed to the infringement of one or more claims of the '817 patent, and/or actively induced others to infringe one or more claims of the '817 patent via their website, in this district and elsewhere in the United States.

10. Defendant's aforesaid activities have been without authority and/or license from Plaintiff.

11. Plaintiff is entitled to recover from the Defendant the damages sustained by Plaintiff as a result of the Defendant's wrongful acts in an amount subject to proof at trial, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

12. Defendant's infringement of Plaintiff's exclusive rights under the '817 patent will continue to damage Plaintiff, causing irreparable harm for which there is no adequate remedy at law, unless enjoined by this Court.

JURY DEMAND

13. Plaintiff hereby requests a trial by jury pursuant to Rule 38 of the Federal Rules of Civil Procedure.

PRAYER FOR RELIEF

Plaintiff respectfully requests that the Court find in its favor and against Defendant, and that the Court grant Plaintiff the following relief:

A. An adjudication that one or more claims of the '817 patent have been infringed, either literally and/or under the doctrine of equivalents, by Defendant and/or by others to whose infringement Defendant has contributed and/or by others whose infringement has been induced by Defendant;

B. An award to Plaintiff of damages adequate to compensate Plaintiff for the Defendant's acts of infringement together with pre-judgment and post-judgment interest;

C. That, should Defendant's acts of infringement be found to be willful from the time that Defendant became aware of the infringing nature of its actions, which is the time of filing of Plaintiff's Original Complaint at the latest, that the Court award treble damages for the period of such willful infringement pursuant to 35 U.S.C. § 284;

D. A grant of permanent injunction pursuant to 35 U.S.C. § 283, enjoining the Defendant from further acts of (1) infringement, (2) contributory infringement, and (3) actively inducing infringement with respect to the claims of the '817 patent;

E. That this Court declare this to be an exceptional case and award Plaintiff its reasonable attorneys' fees and costs in accordance with 35 U.S.C. §285; and

F. Any further relief that this Court deems just and proper.

Respectfully submitted,
LAW OFFICE OF KRIS LE FAN

Dated: March 15, 2012

Kris Le Fan, Esq.
Attorney for Plaintiff
WOLF RUN HOLLOW, LLC

US006115817A

United States Patent [19]

Whitmire

[11] **Patent Number: 6,115,817**

[45] **Date of Patent: Sep. 5, 2000**

[54] **METHODS AND SYSTEMS FOR FACILITATING TRANSMISSION OF SECURE MESSAGES ACROSS INSECURE NETWORKS**

[76] Inventor: **David R. Whitmire**, P.O. Box 393, Watkinsville, Ga. 30677-0393

[21] Appl. No.: **09/072,986**

[22] Filed: **May 6, 1998**

[51] **Int. Cl.**^{7} **H04L 9/00**

[52] **U.S. Cl.** **713/171**; 713/155; 713/156; 713/158; 380/28; 380/30

[58] **Field of Search** 380/277, 278, 380/281, 28, 30; 713/155, 156, 168, 170, 171

[56] **References Cited**

PUBLICATIONS

"Applied Cryptography", Schneier, pp. 53, 54, 180, 181, 225.

Pretty Good Privacy™, PGP®Business Security, Version 5.5 Windows User's Guide, 1997, pp. 1–6 and 23–46.

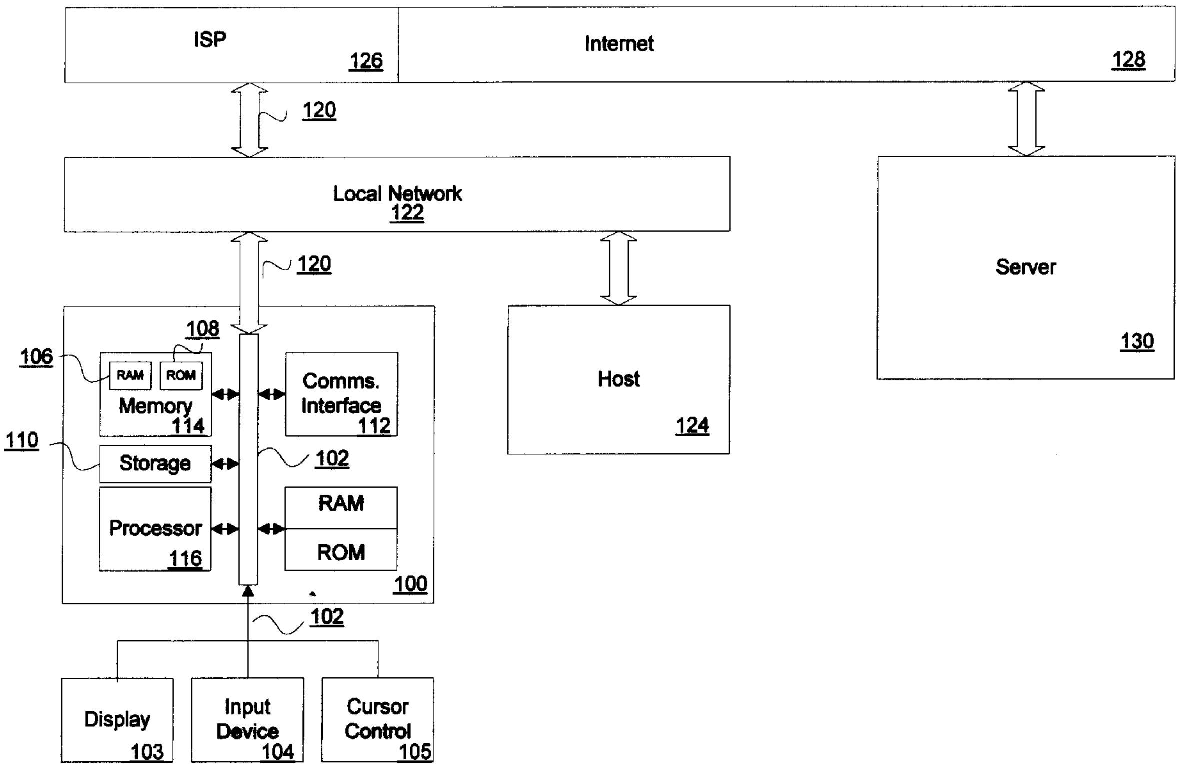
Schneier, Bruce, Applied Cryptography: Protocols, Algorithms, and Source Code in C (2nd Ed. 1996), 1996, pp. 31–34.

Primary Examiner—Thomas R. Peeso
Attorney, Agent, or Firm—Finnegan, Henderson, Farabow, Garrett & Dunner L.L.P.

[57] **ABSTRACT**

In accordance with the present invention, methods and systems consistent with the present invention facilitate the transmission of secure messages across an insecure network. The sender requests a recipient's security software object by, for example, clicking on a button or icon on the recipient's web page. A security software object with encapsulated security information and routing information is transmitted to the sender. The sender composes a message using the security software object. When sender indicates completion, the security software object secures the message according to the security procedure of the object and transmits the secured message to the recipient.

27 Claims, 4 Drawing Sheets



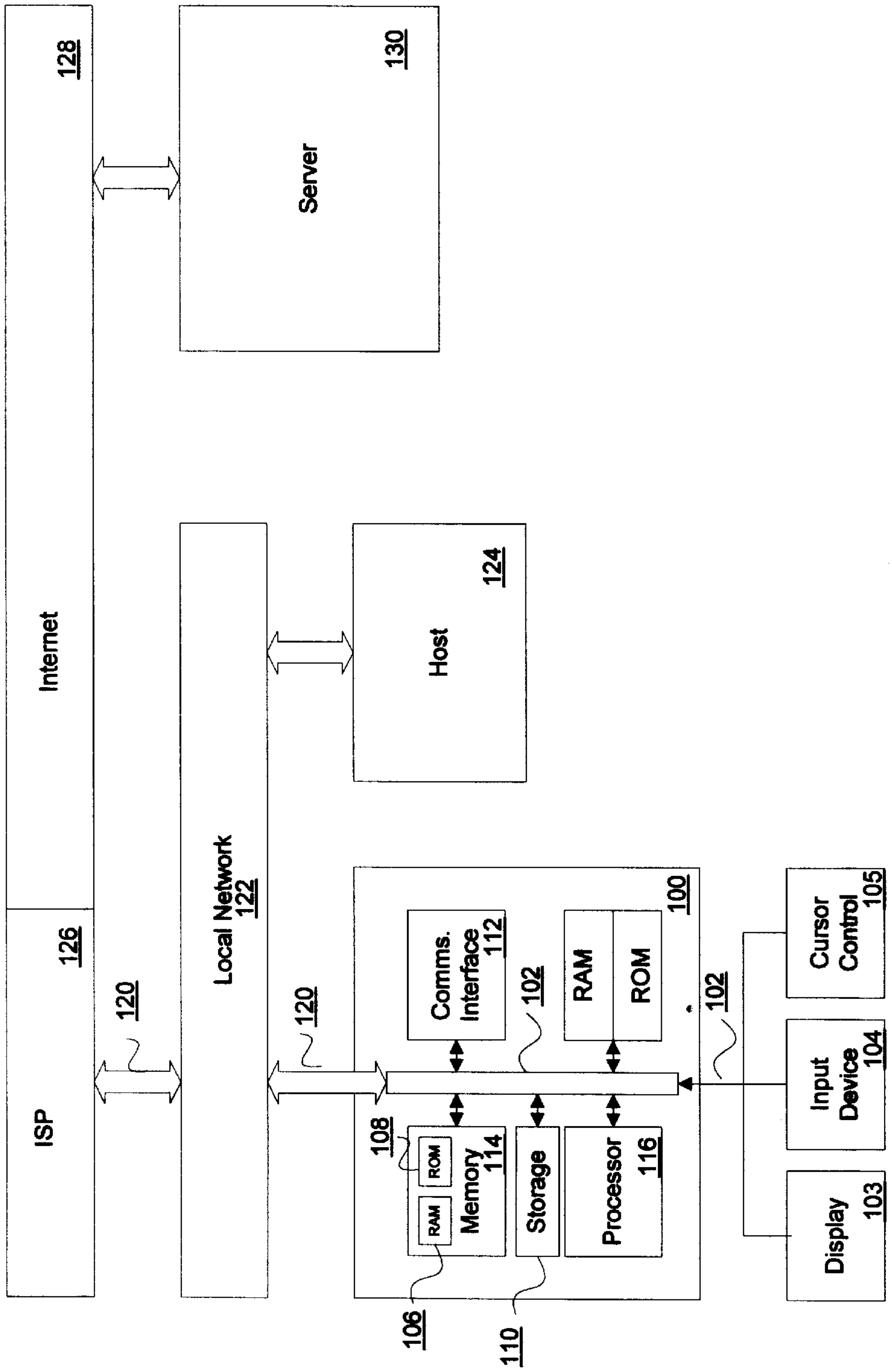

Internet
128
Server
130
ISP
126
120
Local Network
122
Host
124
120
Comms. Interface
112
102
RAM
ROM
100
102
Cursor Control
105
Input Device
104
Display
103
108
ROM
RAM
Memory
114
Storage
Processor
116
106
110

FIG. 1

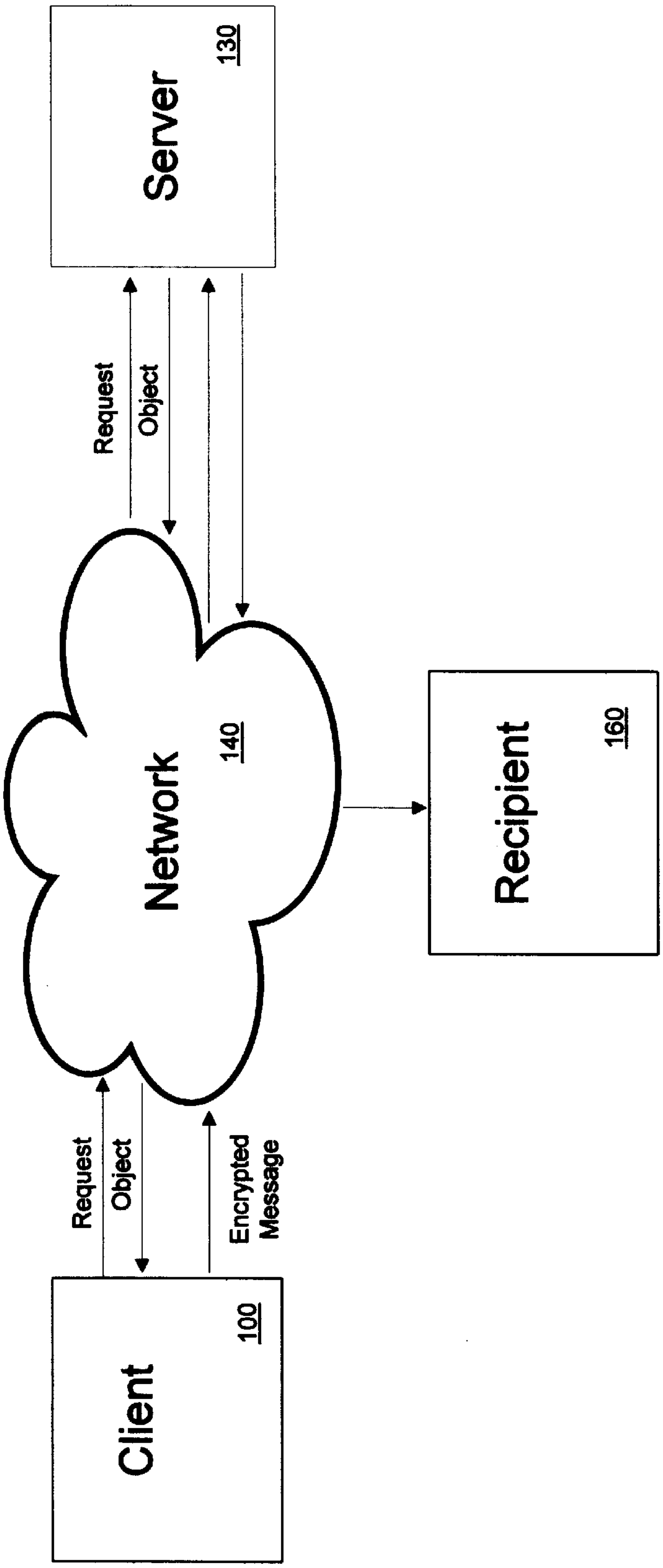

Server
130
Request
Object
Network
140
Recipient
160
Request
Object
Encrypted Message
Client
100

FIG. 2

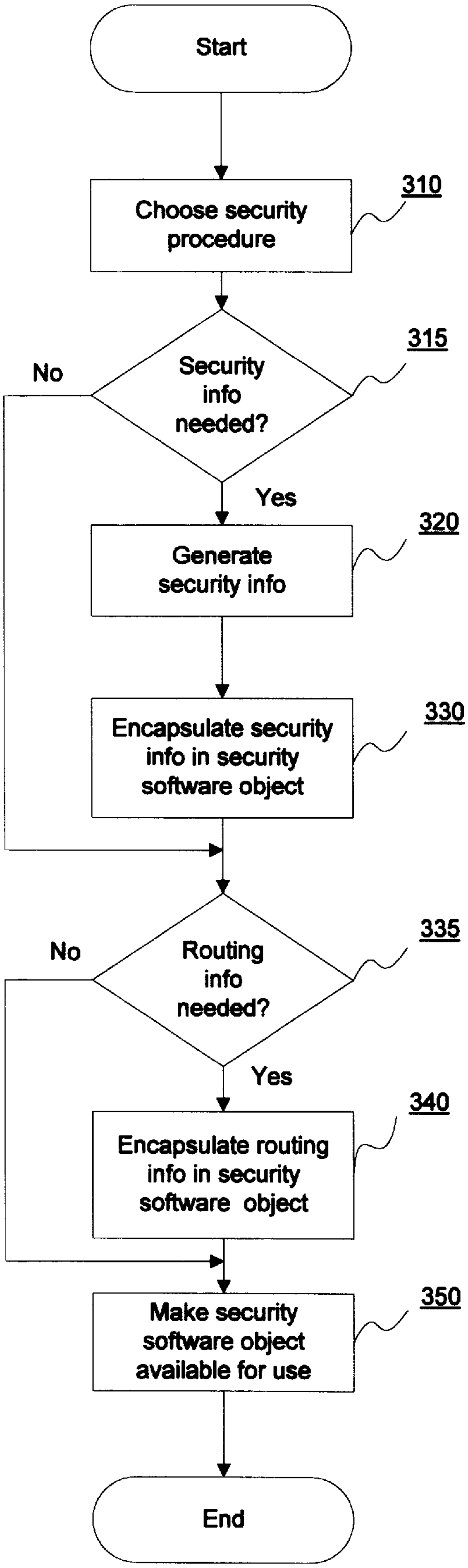

Start
Choose security procedure
310
Security info needed?
315
No
Yes
Generate security info
320
Encapsulate security info in security software object
330
Routing info needed?
335
No
Yes
Encapsulate routing info in security software object
340
Make security software object available for use
350
End

FIG. 3

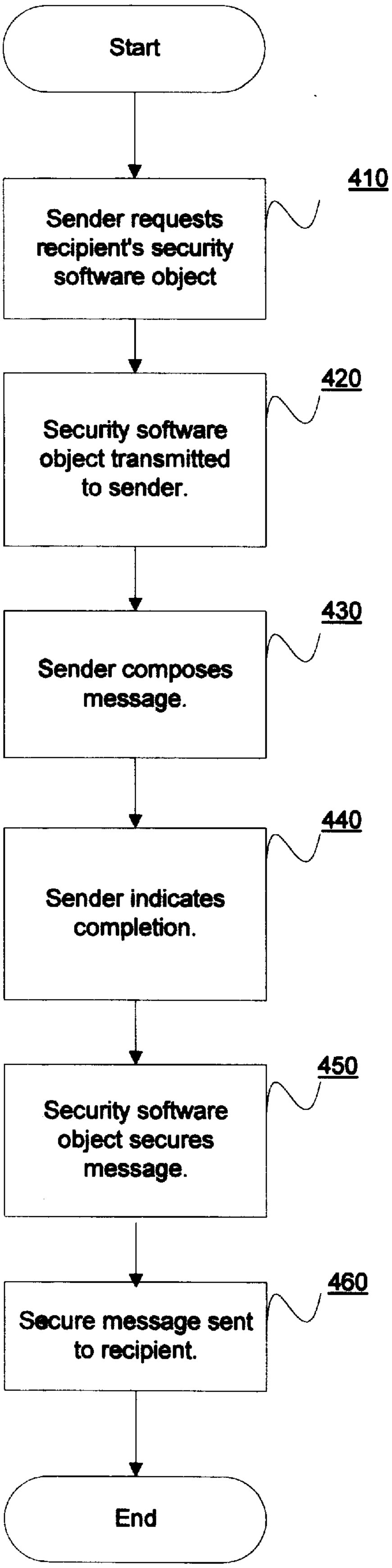

Start
Sender requests recipient's security software object
410
Security software object transmitted to sender.
420
Sender composes message.
430
Sender indicates completion.
440
Security software object secures message.
450
Secure message sent to recipient.
460
End

FIG. 4

METHODS AND SYSTEMS FOR FACILITATING TRANSMISSION OF SECURE MESSAGES ACROSS INSECURE NETWORKS

BACKGROUND OF THE INVENTION

The present invention relates generally to methods and systems for facilitating the transmission of secure messages over an insecure network and, in particular, is directed to methods and systems for encapsulating security procedures, a recipient's security procedure information, and electronic mail address information in a software object.

The Internet has quickly become a popular tool for communicating and conducting business. The Internet is a very large network of smaller interconnected local area networks (LANs) and wide area networks (WANs). By 1995, Internet access was available in 180 countries and there were more than 30 million users. Many expect that the number of worldwide users of the Internet will exceed 100 million by the year 2000.

People communicate with one another over the Internet using electronic mail, that is, e-mail. Using e-mail, a user on the Internet can transfer messages entered from the keyboard or attach and send large electronic files to another user on the Internet almost instantaneously. As used herein, the term "message" includes not only text messages but also files, documents, and any other data to be transmitted from a sender to a recipient, and any combination thereof unless the context indicates otherwise. The Internet is also used to conduct a broad range of commercial and financial transactions. Parties use the communication capabilities of the Internet to enter into contracts electronically and use electronic funds transfers (EFTs) to satisfy the resulting financial obligations. An EFT involves the movement of funds from one bank account to another in response to electronically-communicated payment instructions.

Although the Internet offers a fast, reliable, and efficient way to communicate and conduct business, information transmitted can be vulnerable to security breaches. Without adequate security controls, privileged and confidential communications, financial information, and other communications involving private data that are sent via e-mail could possibly enter the public domain with disastrous results. Professionals and their clients may be exposed to significant risks including financial liabilities or the career-ending loss of professional status.

Technologies currently exist that allow a user to protect private information transmitted over the Internet. Public-key cryptography, for example, is a process that allows users to secure communications with the use of a public-private key pair. Using public-key cryptography, a sender of confidential information uses a public-key algorithm and a public key specified by the intended recipient to encrypt the data. The encrypted data can then be transmitted via any public means, including the Internet, without loss of privacy. The intended recipient uses a private key known only to the recipient and a public-key algorithm to decrypt the data. For more details on public-key cryptography, see Bruce Schneier, Applied Cryptography (1996), pp. 31–34.

Many software providers have developed software products designed to make digital security and public-key cryptography more convenient for the user. One such software package is the Pretty Good Privacy ("PGP") software package offered by Pretty Good Privacy, Inc. Even using software like PGP, however, the process of sending an encrypted document may still be too difficult or time-consuming for many users. First, before sending an encrypted e-mail to a recipient, for example, the sender must first obtain the recipient's public key. Even if the key is posted on a public or corporate key server, the sender will have to spend some amount of time to find and access it. Second, the sender must import the recipient's key into his or her operating version of the encryption software by, for example, cutting and pasting the key text from the key server's page or typing in the key information directly. Both methods are prone to errors and, as a result, the encryption feature will not function properly. Lastly, even if the sender implements the encryption software correctly, the intended recipient may not be operating a compatible software package.

The present invention provides methods and systems for facilitating the transmission of a secure message across an insecure network by encapsulating a security procedure that is compatible with the recipient in a security software object that is transmitted to the sender. The present invention further provides methods and systems for facilitating transmission of a secure message across an insecure network by encapsulating security information used by the security procedure, such as the recipient's public key, in the security software object.

The present invention further provides methods and systems for transmission of a secure message across an insecure network by encapsulating the recipient's communications procedure and routing information to facilitate transmitting the encrypted data to an intended recipient.

SUMMARY OF THE INVENTION

Methods for facilitating transmission of a secure message across an insecure network consistent with this invention comprise the steps, performed by a processor, of receiving a request for a recipient's security software object from a sender; transmitting the software object in response to the user request, the software object comprising a security procedure and recipient information; receiving a secured message secured using the security procedure and the recipient information; and transmitting the secured message to the recipient based on the recipient information.

In accordance with another aspect of the present invention, a method for facilitating the transmission of a secure message from a sender to a recipient comprises the steps, performed by a processor, of receiving a request from a sender for recipient information encapsulated in a self-executable security procedure; transmitting the recipient information encapsulated in a self-executable security procedure in response to the request; receiving a secured message secured using the self-executable security procedure and the recipient information; and transmitting the secured message to the recipient based on the recipient information.

In accordance with still another aspect of the present invention, a method for creating and transmitting a secured message over an insecure network, comprises the steps, performed by a processor, of obtaining a software object comprising a security procedure and recipient information; generating a message; executing the software object to secure the message; and transmitting the secured message based on the recipient information.

A still further aspect of the present invention is a computer program product that comprises a computer-usable medium having computable-readable code embodied therein for transmitting a secure message across an insecure network between a client and a server, the computer program product comprising the steps, performed by a processor, of receiving a request from a sender; transmitting a software object in response to the user request, the software object comprising a security procedure and recipient information; receiving a secured message secured using the security procedure and the recipient information; and, transmitting the secured message to the recipient based on the recipient information.

Yet another aspect of the present invention is a system for facilitating the transmission of a secure message from a sender to a recipient comprising a first receiver for receiving a request from a sender; a first transmitter for transmitting a software object in response to the user request, the software object comprising a security procedure and recipient information; a second receiver for receiving a secured message secured using the security procedure and the recipient information; and a second transmitter for transmitting the secured message to the recipient based on the recipient information.

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings, which are incorporated in and constitute a part of this specification, illustrate the invention and, together with the description, serve to explain the principles of the invention.

FIG. **1** is a schematic block diagram illustrating a computer architecture suitable for use with the present invention;

FIG. **2** is a pictorial representation of a method consistent with the present invention;

FIG. **3** is a flowchart of the steps performed by a processor consistent with the present invention for generating a security software object; and

FIG. **4** is a flowchart of the steps performed by a processor consistent with the present invention for facilitating the transmission of a secure message across an insecure network.

DETAILED DESCRIPTION OF THE INVENTION

A. Overview

Systems and methods consistent with the present invention allow secure messages to be transmitted across a network connection. A sender obtains a security software object comprising a security procedure and other information, such as the recipient's public key and e-mail address. The sender then composes a message or attaches a file using the security software object. Upon indication from the sender, the software object secures the message and attached file by executing the security procedure using information encapsulated in the security software object. The secured message is then transmitted across the network connection to the recipient.

The present invention may be implemented using hardware, software, or a combination of hardware and software. Specifically, the invention may be implemented with both object-oriented programming languages, like Java® and C++, and nonobject-oriented programming languages. (Java® is a registered trademark of Sun Microsystems, Inc. in the United States and other countries.)

Reference will now be made in detail to an exemplary implementation of a system consistent with the present invention which is also illustrated in the accompanying drawings. While the description includes exemplary embodiments, other embodiments are possible, and changes may be made to the implementation described without departing from the spirit and scope of the invention. Wherever possible, the same reference numbers will be used throughout the drawings to refer to the same or like parts.

B. Computer Architecture

Methods and systems consistent with the present invention may be implemented using distributed systems such as exemplary distributed system **10** shown in FIG. **1**. Client **100** is a conventional computer that includes a bus **102** or other communication mechanism for communicating information and a processor **116** coupled with bus **102** for processing information and executing application programs. Client **100** also includes a main memory **114** comprising, for example, a random access memory (RAM) **106** or other dynamic storage device and a read only memory (ROM) **108** or other static storage device, coupled to bus **102** for storing information and instructions to be executed by processor **116**. A storage device **110**, such as a magnetic disk or optical disk, is provided and coupled to bus **102** for storing information and instructions.

Client **100** may be coupled via bus **102** to a display **103**, such as a cathode ray tube (CRT), for displaying information to a computer user. An input device **104**, including alphanumeric and other keys, is coupled to bus **102** for communicating information and command selections to processor **116**. Another type of user input device is cursor control **106**, such as a mouse, a trackball, or cursor direction keys for communicating direction information and command selections to processor **116** and for controlling cursor movement on display **103**. This input device typically has two degrees of freedom in two axes, a first axis (e.g., x) and a second axis (e.g., y), that allows the device to specify positions in a plane.

Methods and systems consistent with the present invention utilize client **100** for transmitting a secure message across an insecure connection. Consistent with one implementation, processor **116** of client **100** executes one or more sequences of one or more instructions contained in main memory **114**. Such instructions may be read into main memory **114** from another computer-readable medium, such as storage device **110**, or received in the form of an object from server **130**. Execution of the sequences of instructions contained in main memory **114** causes processor **116** to perform the process steps described herein. In an alternative implementation, hard-wired circuitry may be used in place of or in combination with software instructions to implement the invention. Thus, implementations of the invention are not limited to any specific combination of hardware circuitry and software.

The term "computer-readable medium" as used herein refers to any media that participates in providing instructions to processor **116** for execution. Such a medium may take many forms, including but not limited to, non-volatile media, volatile media, and transmission media. Non-volatile media includes, for example, optical or magnetic disks, such as storage device **110**. Volatile media includes dynamic memory, such as main memory **114**. Transmission media includes coaxial cables, copper wire, and fiber optics, including the wires that comprise bus **102**. Transmission media can also take the form of acoustic or light waves, such as those generated during radio wave and infrared data communications.

Common forms of computer-readable media include, for example, a floppy disk, a flexible disk, hard disk, magnetic tape, or any other magnetic medium, a CD-ROM, any other optical medium, punch cards, papertape, any other physical medium with patterns of holes, a RAM, PROM, and EPROM, a FLASH-EPROM, any other memory chip or cartridge, a carrier wave, or any other medium from which a computer can read.

Various forms of computer readable media may be involved in carrying one or more sequences of one or more instructions to processor **116** for execution. For example, the instructions may initially be carried on a magnetic disk of a remote computer. The remote computer can load the instructions into its dynamic memory and send the instructions over a telephone line using a modem. A modem local to client **100** can receive the data on the telephone line and use an infrared transmitter to convert the data to an infrared signal. An infrared detector coupled to bus **102** can receive the data carried in the infrared signal and place the data on bus **102**. Bus **102** carries the data to main memory **114**, from which processor **116** retrieves and executes the instructions. The instructions received by main memory **114** may optionally be stored on storage device **110** either before or after execution by processor **116**.

Client **100** also includes a communication interface **118** coupled to bus **102**. Communication interface **112** provides a two-way data communication coupling to a network link **120** that is connected to local network **122**. For example, communication interface **112** may be an integrated services digital network (ISDN) card or a modem to provide a data communication connection to a corresponding type of telephone line. As another example, communication interface **112** may be a local area network (LAN) card providing a data communication connection to a compatible LAN. Wireless links may also be implemented. In any such implementation, communication interface **112** sends and receives electrical, electromagnetic, or optical signals that carry digital data streams representing various types of information.

Network link **120** typically provides data communication through one or more networks to other data devices. For example, network link **120** may provide a connection through local network **122** to a host computer **124** and/or to data equipment operated by an Internet Service Provider (ISP) **126**. ISP **126**, in turn, provides data communication services through the Internet **128**. Local network **122** and Internet **128** both use electric, electromagnetic, or optical signals that carry digital data streams. The signals through the various networks and the signals on network link **120** and through communication interface **112**, which carry the digital data to and from client **100**, are exemplary forms of carrier waves transporting the information.

Client **100** can send messages and receive data, including program code, through the network(s), network link **120**, and communication interface **112**. In the Internet example, a server **130** might transmit a requested code for an application program through Internet **128**, ISP **126**, local network **122**, and communication interface **112**. In accordance with one implementation, one such downloaded application comprises a software object with encapsulated security procedure and recipient information, as described herein. The received code may be executed by processor **116** as it is received and/or stored in storage device **110** or other non-volatile storage for later execution. In this manner, client **100** may obtain application code in the form of a carrier wave.

Although client **100** is shown in FIG. **1** as being connectable to one server **130**, those skilled in the art will recognize that client **100** may establish connections to multiple servers on Internet **128**.

C. One Embodiment of the Method

Methods consistent with the present invention will be described in terms of the operation of a server with references to the diagram in FIG. **2**. For example, in one embodiment of the present invention, server **130** receives a request for the security software object from client **100**, the computer of the entity wishing to transmit a secured message. The request may be in the form of, for example, "clicking" a web site button or icon, an e-mail, or a verbal request for the software. The server transmits the security software object to the client over network **140**. Network **140** may be a plurality of local networks, network links, and communication interfaces including, but not limited to, Internet **128**, ISP **126**, local network **122**, and communications interface **112** as depicted in FIG. **1**. Client **100** receives the security software object. After execution of the security software object, an encrypted message is transmitted from client **100** to recipient **160** via network **140**. The encrypted message may also be received by server **130** and retransmitted to recipient **160** via network **140**.

FIG. **3** is a flowchart of the steps performed by a processor consistent with the present invention for generating a security software object. Methods consistent with the present invention implement object-oriented programming techniques, such as the C++ or Java® programming languages. Object-oriented programming is a form of software development that involves the creation and use of "objects". Objects are software entities that contain data as well as instructions that manipulate the data.

One of the principle benefits of object-oriented programming is encapsulation. In object-oriented programming, "encapsulation" refers to the process of grouping data and the code that manipulates it into a single entity or object.

To prepare the object, a security procedure is chosen (step **310**). The security procedure can be, for example, public-key encryption or any other procedure suitable for securing electronic data. If other information related to the execution of the security procedure is needed (step **315**), that information is generated (step **320**). A security procedure based on public-key encryption for example, will require that the sender use the recipient's public key to encrypt the message. In methods consistent with the present invention, the public key is obtained or generated and is encapsulated in the security software object along with the security algorithm (step **330**).

The recipient may also want to facilitate receipt of the encrypted message by providing routing information. If such routing information is needed (step **335**), routing information is encapsulated in the security software object (step **340**). Routing information may be, for example, the recipient's e-mail address, Internet protocol address, or other network identification information. Routing information may also include a communications procedure used by the recipient. The security software object may then be made available for public use by, for example, posting on the World Wide Web, creating disks for distribution, saving as a file for attachment to an e-mail, or by some other means.

FIG. **4** is a flowchart of the steps performed by a processor consistent with the present invention for facilitating the transmission of a secure message across an insecure network. If a sender wants to communicate with the recipient, the sender requests the security software object (step **410**). The sender can make such a request by, for example, accessing the recipient's web site and requesting downloading of the object by "clicking" on a button or icon, using his or her computer (client **100**). The security software object is transferred to the client computer, for example, by transmitting the file across the Internet or by loading the file from disk (step **420**). If loaded from disk, the security software object may contain a function that automatically connects the client to the Internet or, alternatively, the sender may need to activate the object. If the object is downloaded from the Internet, the object may automatically prompt the sender to enter a message or attach a file for transfer. The sender composes a message (step **430**). When the sender indicates completion by, for example, clicking on a button or icon (step **440**), the security software object encrypts the message using the encapsulated security information in the security software object (step **450**). For example, if the security procedure is a public-key algorithm, the security software object will encrypt the message using the recipient's public key that is encapsulated in the security software object. The encrypted message is transmitted across the Internet to the recipient (step **460**). If necessary, the security software object may use routing information that is encapsulated in the security software object. Upon receipt of the encrypted message, the recipient can decrypt and use the message.

D. Conclusion

In accordance with the present invention, methods and systems consistent with the present invention facilitate the transmission of secure messages across an insecure network. The sender requests a recipient's security software object by, for example, clicking on a button or icon on the recipient's web page. A security software object with encapsulated security information and routing information is transmitted to the sender. The sender composes a message using the security software object. When sender indicates completion, the security software object secures the message according to the security procedure of the object and transmits the secured message to the recipient.

The foregoing description of an implementation of the invention has been presented for purposes of illustration and description. It is not exhaustive and does not limit the invention to the precise form disclosed. Modifications and variations are possible in light of the above teachings or may be acquired from practicing of the invention. For example, the described implementation includes software but the present invention may be implemented as a combination of hardware and software or hardware alone. The scope of the invention is defined by the claims and their equivalents.

What is claimed:

1. A method for facilitating the transmission of a secure message from a sender to a recipient comprising the steps, performed by a processor, of:

receiving a request for a recipient's security software object from a sender;

transmitting the software object in response to the request, the software object comprising a security procedure and recipient information;

receiving a secured message secured using the security procedure and the recipient information; and

transmitting the secured message to the recipient based on the recipient information.

2. A method of claim **1** wherein the security procedure comprises a public-key encryption algorithm.

3. A method of claim **2** wherein the recipient information comprises:

a public key associated with a recipient.

4. A method of claim **1** wherein the recipient information comprises the recipient's routing information.

5. A method for facilitating the transmission of a secure message from a sender to a recipient comprising the steps, performed by a processor, of:

receiving a request from a sender for recipient information encapsulated in a self-executable security procedure;

transmitting the recipient information encapsulated in a self-executable security procedure in response to the request;

receiving a secured message secured using the self-executable security procedure and the recipient information; and

transmitting the secured message to the recipient based on the recipient information.

6. A method of claim **5** wherein the security procedure comprises a public-key encryption algorithm.

7. A method of claim **6** wherein the recipient information comprises:

a public key associated with a recipient.

8. A method of claim **5** wherein the recipient information comprises the recipient's routing information.

9. A method for creating and transmitting a secured message over an insecure network, comprising the steps, performed by a processor, of:

obtaining a software object comprising a security procedure and recipient information;

generating a message;

executing the software object to secure the message; and

transmitting the secured message based on the recipient information.

10. A method for creating and transmitting a secured message over an insecure network comprising the steps, performed by a processor, of:

transmitting a request for recipient information;

obtaining the recipient information embedded in a self-executable security procedure;

generating a message; and

transmitting the message secured by the self-executable security procedure and the recipient information.

11. A method for constructing a software object for transmitting a secure message to an intended recipient over an insecure network comprising the steps of:

determining a security procedure;

determining recipient information;

encapsulating the recipient information and the security procedure in a software object; and

storing the software object to a storage medium accessible by users.

12. A computer program product comprising:

a computer-usable medium having computable-readable code embodied therein for transmitting a secure message across an insecure network between a client and a server, the computer program product comprising the steps, performed by a processor, of:

receiving a request from a sender;

transmitting a software object in response to the request, the software object comprising a security procedure and recipient information;

receiving a secured message secured using the security procedure and the recipient information; and,

transmitting the secured message to the recipient based on the recipient information.

13. The computer program product of claim **12** wherein the security procedure comprises a public-key encryption algorithm.

14. The computer program product of claim **13** wherein the recipient information comprises:

a public key associated with a recipient.

15. The computer program product of claim **12** wherein the recipient information comprises the recipient's routing information.

16. A computer program product comprising:

a computer-usable medium having computable-readable code embodied therein for transmitting a secure message across an insecure network between a client and a server, the computer program product comprising the steps, performed by a processor, of:

determining a security procedure;

determining recipient information;

encapsulating the recipient information and the security procedure in a software object; and,

storing the software object to a storage medium.

17. The computer program product of claim **16** wherein the security procedure comprises a public-key encryption algorithm.

18. The computer program product of claim **17** wherein the recipient information comprises:

a public key associated with a recipient.

19. The computer program product of claim **16** wherein the recipient information comprises the recipient's routing information.

20. A system for facilitating the transmission of a secure message from a sender to a recipient comprising:

a first receiver for receiving a request for a recipient's security software object from a sender;

a first transmitter for transmitting the software object in response to the request, the software object comprising a security procedure and recipient information;

a second receiver for receiving a secured message secured using the security procedure and the recipient information; and,

a second transmitter for transmitting the secured message to the recipient based on the recipient information.

21. The system of claim **20** wherein the security procedure comprises a public-key encryption algorithm.

22. The system of claim **21** wherein the recipient information comprises:

a public key associated with a recipient.

23. The system of claim **20** wherein the recipient information comprises the recipient's routing information.

24. An apparatus for facilitating the transmission of a secure message from a sender to a recipient comprising:

a component configured to receive a request from a sender;

a component configured to transmit a software object in response to the request, the software object comprising a security procedure and recipient information;

a component configured to receive a secured message secured using the security procedure and the recipient information; and,

a component configured to transmit the secured message to the recipient based on the recipient information.

25. The apparatus of claim **24** wherein the security procedure comprises a public-key encryption algorithm.

26. The apparatus of claim **25** wherein the recipient information comprises:

a public key associated with a recipient.

27. The apparatus of claim **24** wherein the recipient information comprises the recipient's routing information.

* * * * *

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

NOTICE OF ASSIGNMENT TO UNITED STATES MAGISTRATE JUDGE FOR DISCOVERY

This case has been assigned to District Judge Ronald S. W. Lew and the assigned discovery Magistrate Judge is Charles Eick.

The case number on all documents filed with the Court should read as follows:

CV12- 4255 RSWL (Ex)

Pursuant to General Order 05-07 of the United States District Court for the Central District of California, the Magistrate Judge has been designated to hear discovery related motions.

All discovery related motions should be noticed on the calendar of the Magistrate Judge

=======================================

NOTICE TO COUNSEL

A copy of this notice must be served with the summons and complaint on all defendants (if a removal action is filed, a copy of this notice must be served on all plaintiffs).

Subsequent documents must be filed at the following location:

[X] **Western Division**
312 N. Spring St., Rm. G-8
Los Angeles, CA 90012

[ ] **Southern Division**
411 West Fourth St., Rm. 1-053
Santa Ana, CA 92701-4516

[ ] **Eastern Division**
3470 Twelfth St., Rm. 134
Riverside, CA 92501

Failure to file at the proper location will result in your documents being returned to you.

AO 440 (Rev. 12/09) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

Central District of California

WOLF RUN HOLLOW, LLC	)	CV12-4255-RSWL (E)
Plaintiff	)	
v.	)	Civil Action No.
CITY NATIONAL BANK	)	
Defendant	)	

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)*

CITY NATIONAL BANK
City National Plaza
555 South Flower Street
Los Angeles, CA 90071

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are:

Kris Le Fan, Esq.
433 North Camden Drive, Sixth Floor
Beverly Hills, CA 90210

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: MAY 16 2012

Ann M. Martinez
Signature of Clerk or Deputy Clerk

Civil Action No.

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* ______________________________
was received by me on *(date)* ______________ .

❒ I personally served the summons on the individual at *(place)* ______________________________
______________________________ on *(date)* ______________ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* ______________
______________________________ , a person of suitable age and discretion who resides there,
on *(date)* ______________ , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* ______________________________ , who is
designated by law to accept service of process on behalf of *(name of organization)* ______________
______________________________ on *(date)* ______________ ; or

❒ I returned the summons unexecuted because ______________________________ ; or

❒ Other *(specify)*:

My fees are $ __________ for travel and $ __________ for services, for a total of $ 0 .

I declare under penalty of perjury that this information is true.

Date: ______________

____
Server's signature

____
Printed name and title

____
Server's address

Additional information regarding attempted service, etc:

AO 440 (Rev. 12/09) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

Central District of California

WOLF RUN HOLLOW, LLC

Plaintiff

v.

CITY NATIONAL BANK

Defendant

Civil Action No. CV12-4255-RSWL(E)

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)*

CITY NATIONAL BANK
City National Plaza
555 South Flower Street
Los Angeles, CA 90071

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are:

Kris Le Fan, Esq.
433 North Camden Drive, Sixth Floor
Beverly Hills, CA 90210

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: MAY 16 2012

ANN M. MARTINEZ

Signature of Clerk or Deputy Clerk

SEAL OF THE U.S. DISTRICT COURT
CENTRAL DIST. OF CALIFORNIA

1197

UNITED STATES DISTRICT COURT, CENTRAL DISTRICT OF CALIFORNIA
CIVIL COVER SHEET

I (a) PLAINTIFFS (Check box if you are representing yourself □)

WOLF RUN HOLLOW, LLC

DEFENDANTS

CITY NATIONAL BANK

(b) Attorneys (Firm Name, Address and Telephone Number. If you are representing yourself, provide same.)

Law Office of Kris Le Fan
433 North Camden Drive, Sixth Floor
Beverly Hills, CA 90210
213-290-1091

Attorneys (If Known)

BY FAX

II. BASIS OF JURISDICTION (Place an X in one box only.)

□ 1 U.S. Government Plaintiff

☑ 3 Federal Question (U.S. Government Not a Party)

□ 2 U.S. Government Defendant

□ 4 Diversity (Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES - For Diversity Cases Only (Place an X in one box for plaintiff and one for defendant.)

	PTF	DEF		PTF	DEF
Citizen of This State	□ 1	□ 1	Incorporated or Principal Place of Business in this State	□ 4	□ 4
Citizen of Another State	□ 2	□ 2	Incorporated and Principal Place of Business in Another State	□ 5	□ 5
Citizen or Subject of a Foreign Country	□ 3	□ 3	Foreign Nation	□ 6	□ 6

IV. ORIGIN (Place an X in one box only.)

☑ 1 Original Proceeding □ 2 Removed from State Court □ 3 Remanded from Appellate Court □ 4 Reinstated or Reopened □ 5 Transferred from another district (specify): □ 6 Multi-District Litigation □ 7 Appeal to District Judge from Magistrate Judge

V. REQUESTED IN COMPLAINT: JURY DEMAND: ☑ Yes □ No (Check 'Yes' only if demanded in complaint.)

CLASS ACTION under F.R.C.P. 23: □ Yes ☑ No ☑ **MONEY DEMANDED IN COMPLAINT: $** TBD

VI. CAUSE OF ACTION (Cite the U.S. Civil Statute under which you are filing and write a brief statement of cause. Do not cite jurisdictional statutes unless diversity.)

35 USC 271 et seq. - patent infringement

VII. NATURE OF SUIT (Place an X in one box only.)

OTHER STATUTES
- □ 400 State Reapportionment
- □ 410 Antitrust
- □ 430 Banks and Banking
- □ 450 Commerce/ICC Rates/etc.
- □ 460 Deportation
- □ 470 Racketeer Influenced and Corrupt Organizations
- □ 480 Consumer Credit
- □ 490 Cable/Sat TV
- □ 810 Selective Service
- □ 850 Securities/Commodities/ Exchange
- □ 875 Customer Challenge 12 USC 3410
- □ 890 Other Statutory Actions
- □ 891 Agricultural Act
- □ 892 Economic Stabilization Act
- □ 893 Environmental Matters
- □ 894 Energy Allocation Act
- □ 895 Freedom of Info. Act
- □ 900 Appeal of Fee Determination Under Equal Access to Justice
- □ 950 Constitutionality of State Statutes

CONTRACT
- □ 110 Insurance
- □ 120 Marine
- □ 130 Miller Act
- □ 140 Negotiable Instrument
- □ 150 Recovery of Overpayment & Enforcement of Judgment
- □ 151 Medicare Act
- □ 152 Recovery of Defaulted Student Loan (Excl. Veterans)
- □ 153 Recovery of Overpayment of Veteran's Benefits
- □ 160 Stockholders' Suits
- □ 190 Other Contract
- □ 195 Contract Product Liability
- □ 196 Franchise

REAL PROPERTY
- □ 210 Land Condemnation
- □ 220 Foreclosure
- □ 230 Rent Lease & Ejectment
- □ 240 Torts to Land
- □ 245 Tort Product Liability
- □ 290 All Other Real Property

TORTS
PERSONAL INJURY
- □ 310 Airplane
- □ 315 Airplane Product Liability
- □ 320 Assault, Libel & Slander
- □ 330 Fed. Employers' Liability
- □ 340 Marine
- □ 345 Marine Product Liability
- □ 350 Motor Vehicle
- □ 355 Motor Vehicle Product Liability
- □ 360 Other Personal Injury
- □ 362 Personal Injury-Med Malpractice
- □ 365 Personal Injury-Product Liability
- □ 368 Asbestos Personal Injury Product Liability

IMMIGRATION
- □ 462 Naturalization Application
- □ 463 Habeas Corpus-Alien Detainee
- □ 465 Other Immigration Actions

TORTS
PERSONAL PROPERTY
- □ 370 Other Fraud
- □ 371 Truth in Lending
- □ 380 Other Personal Property Damage
- □ 385 Property Damage Product Liability

BANKRUPTCY
- □ 422 Appeal 28 USC 158
- □ 423 Withdrawal 28 USC 157

CIVIL RIGHTS
- □ 441 Voting
- □ 442 Employment
- □ 443 Housing/Accommodations
- □ 444 Welfare
- □ 445 American with Disabilities - Employment
- □ 446 American with Disabilities - Other
- □ 440 Other Civil Rights

PRISONER PETITIONS
- □ 510 Motions to Vacate Sentence Habeas Corpus
- □ 530 General
- □ 535 Death Penalty
- □ 540 Mandamus/ Other
- □ 550 Civil Rights
- □ 555 Prison Condition

FORFEITURE / PENALTY
- □ 610 Agriculture
- □ 620 Other Food & Drug
- □ 625 Drug Related Seizure of Property 21 USC 881
- □ 630 Liquor Laws
- □ 640 R.R. & Truck
- □ 650 Airline Regs
- □ 660 Occupational Safety /Health
- □ 690 Other

LABOR
- □ 710 Fair Labor Standards Act
- □ 720 Labor/Mgmt. Relations
- □ 730 Labor/Mgmt. Reporting & Disclosure Act
- □ 740 Railway Labor Act
- □ 790 Other Labor Litigation
- □ 791 Empl. Ret. Inc. Security Act

PROPERTY RIGHTS
- □ 820 Copyrights
- ☑ 830 Patent
- □ 840 Trademark

SOCIAL SECURITY
- □ 861 HIA (1395ff)
- □ 862 Black Lung (923)
- □ 863 DIWC/DIWW (405(g))
- □ 864 SSID Title XVI
- □ 865 RSI (405(g))

FEDERAL TAX SUITS
- □ 870 Taxes (U.S. Plaintiff or Defendant)
- □ 871 IRS-Third Party 26 USC 7609

FOR OFFICE USE ONLY: Case Number: CV12-4255

AFTER COMPLETING THE FRONT SIDE OF FORM CV-71, COMPLETE THE INFORMATION REQUESTED BELOW.

UNITED STATES DISTRICT COURT, CENTRAL DISTRICT OF CALIFORNIA
CIVIL COVER SHEET

VIII(a). IDENTICAL CASES: Has this action been previously filed in this court and dismissed, remanded or closed? ☑ No □ Yes
If yes, list case number(s): ____________________

VIII(b). RELATED CASES: Have any cases been previously filed in this court that are related to the present case? ☑ No □ Yes
If yes, list case number(s): ____________________

Civil cases are deemed related if a previously filed case and the present case:

(Check all boxes that apply)
□ A. Arise from the same or closely related transactions, happenings, or events; or
□ B. Call for determination of the same or substantially related or similar questions of law and fact; or
□ C. For other reasons would entail substantial duplication of labor if heard by different judges; or
□ D. Involve the same patent, trademark or copyright, and one of the factors identified above in a, b or c also is present.

IX. VENUE: (When completing the following information, use an additional sheet if necessary.)

(a) List the County in this District; California County outside of this District; State if other than California; or Foreign Country, in which **EACH** named plaintiff resides.
□ Check here if the government, its agencies or employees is a named plaintiff. If this box is checked, go to item (b).

County in this District:*	California County outside of this District; State, if other than California; or Foreign Country
	Delaware

(b) List the County in this District; California County outside of this District; State if other than California; or Foreign Country, in which **EACH** named defendant resides.
□ Check here if the government, its agencies or employees is a named defendant. If this box is checked, go to item (c).

County in this District:*	California County outside of this District; State, if other than California; or Foreign Country
Los Angeles	

(c) List the County in this District; California County outside of this District; State if other than California; or Foreign Country, in which **EACH** claim arose.
Note: In land condemnation cases, use the location of the tract of land involved.

County in this District:*	California County outside of this District; State, if other than California; or Foreign Country
Los Angeles	

*** Los Angeles, Orange, San Bernardino, Riverside, Ventura, Santa Barbara, or San Luis Obispo Counties**
Note: In land condemnation cases, use the location of the tract of land involved

X. SIGNATURE OF ATTORNEY (OR PRO PER): ____________________ **Date** May 15, 2012

Notice to Counsel/Parties: The CV-71 (JS-44) Civil Cover Sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law. This form, approved by the Judicial Conference of the United States in September 1974, is required pursuant to Local Rule 3-1 is not filed but is used by the Clerk of the Court for the purpose of statistics, venue and initiating the civil docket sheet. (For more detailed instructions, see separate instructions sheet.)

Key to Statistical codes relating to Social Security Cases:

Nature of Suit Code	Abbreviation	Substantive Statement of Cause of Action
861	HIA	All claims for health insurance benefits (Medicare) under Title 18, Part A, of the Social Security Act, as amended. Also, include claims by hospitals, skilled nursing facilities, etc., for certification as providers of services under the program. (42 U.S.C. 1935FF(b))
862	BL	All claims for "Black Lung" benefits under Title 4, Part B, of the Federal Coal Mine Health and Safety Act of 1969. (30 U.S.C. 923)
863	DIWC	All claims filed by insured workers for disability insurance benefits under Title 2 of the Social Security Act, as amended; plus all claims filed for child's insurance benefits based on disability. (42 U.S.C. 405(g))
863	DIWW	All claims filed for widows or widowers insurance benefits based on disability under Title 2 of the Social Security Act, as amended. (42 U.S.C. 405(g))
864	SSID	All claims for supplemental security income payments based upon disability filed under Title 16 of the Social Security Act, as amended.
865	RSI	All claims for retirement (old age) and survivors benefits under Title 2 of the Social Security Act, as amended. (42 U.S.C. (g))