US006493824B1

(12) United States Patent
Novoa et al.

(10) Patent No.: **US 6,493,824 B1**
(45) Date of Patent: **Dec. 10, 2002**

(54) **SECURE SYSTEM FOR REMOTELY WAKING A COMPUTER IN A POWER-DOWN STATE**

(75) Inventors: **Manuel Novoa**, Houston, TX (US); **Adrian Crisan**, Cypress, TX (US)

(73) Assignee: **Compaq Information Technologies Group, L.P.**, Houston, TX (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/253,637**

(22) Filed: **Feb. 19, 1999**

(51) **Int. Cl.**[7] **H04L 9/12**; H04L 9/18

(52) **U.S. Cl.** **713/162**; 709/203; 709/208; 709/217; 709/220; 709/228; 713/160; 713/161; 713/178; 713/179

(58) **Field of Search** 709/250, 245, 709/229, 225; 713/200, 201

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,634,073	A	5/1997	Collins et al.	395/825
5,680,547	A	10/1997	Chang	395/200.01
5,727,221	A	3/1998	Walsh et al.	395/750
5,751,951	A	5/1998	Osborne et al.	395/200.8
5,802,305	A	9/1998	McKaughan et al.	395/200.57
5,826,015	A *	10/1998	Schmidt	
5,915,119	A *	6/1999	Cone	
5,938,771	A *	8/1999	Williams et al.	
6,119,228	A *	9/2000	Angelo et al.	713/178
6,131,167	A *	10/2000	Cruz	
6,286,111	B1 *	9/2001	Snover	
6,292,831	B1 *	9/2001	Cheng	
6,311,276	B1 *	11/2001	Connery et al.	

OTHER PUBLICATIONS

IBM, WakwOn Lan——an Administrator's perspective, IBM White paper, 1997.*

SCYLD Computing, Corporation, Using Wake–On–LAN with Linux, Http://www.SCYld.com/expert/wake–on–lan, 1999–2002.*

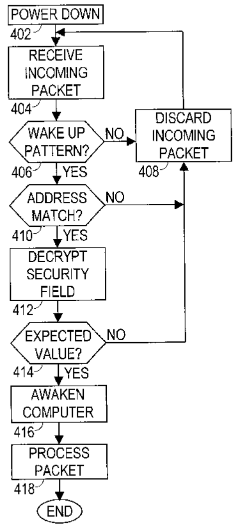
* cited by examiner

Primary Examiner—Gail Hayes
Assistant Examiner—Taghi T. Arani
(74) *Attorney, Agent, or Firm*—Conley, Rose & Tayon, P.C.; Michael F. Heim; Daniel J. Krueger

(57) **ABSTRACT**

A secure system and method is provided for remotely waking a computer from a power down state. In one embodiment, a network interface card receives incoming data packets via a network connector. A control module is coupled to the network connector and is configured to search the incoming packets for a wake-up pattern. The control module also verifies that the packet's destination address matches the destination address of the network interface card. If the destination addresses match and a wake-up pattern is found, the control module decrypts an encrypted value from the incoming packet and compares the result to an expected value. A successful comparison causes the control module to assert a signal to wake up the host computer. Preferably, a standard public/private key pair encryption scheme is used, and the source of the data packet encrypts the expected value with a private key. All computers which may receive wake-up packets are provided with a public key with which to decrypt values contained in a security field of any wake-up packets. A successful decryption serves to certify that the wake-up packet was transmitted from an authorized source. For added security, the expected value and public/private keys may be changed on a regular basis, or even every time a valid wake-up packet is received. The new value may be provided in the wake-up packet, to be stored by the network card for the next use.

11 Claims, 3 Drawing Sheets



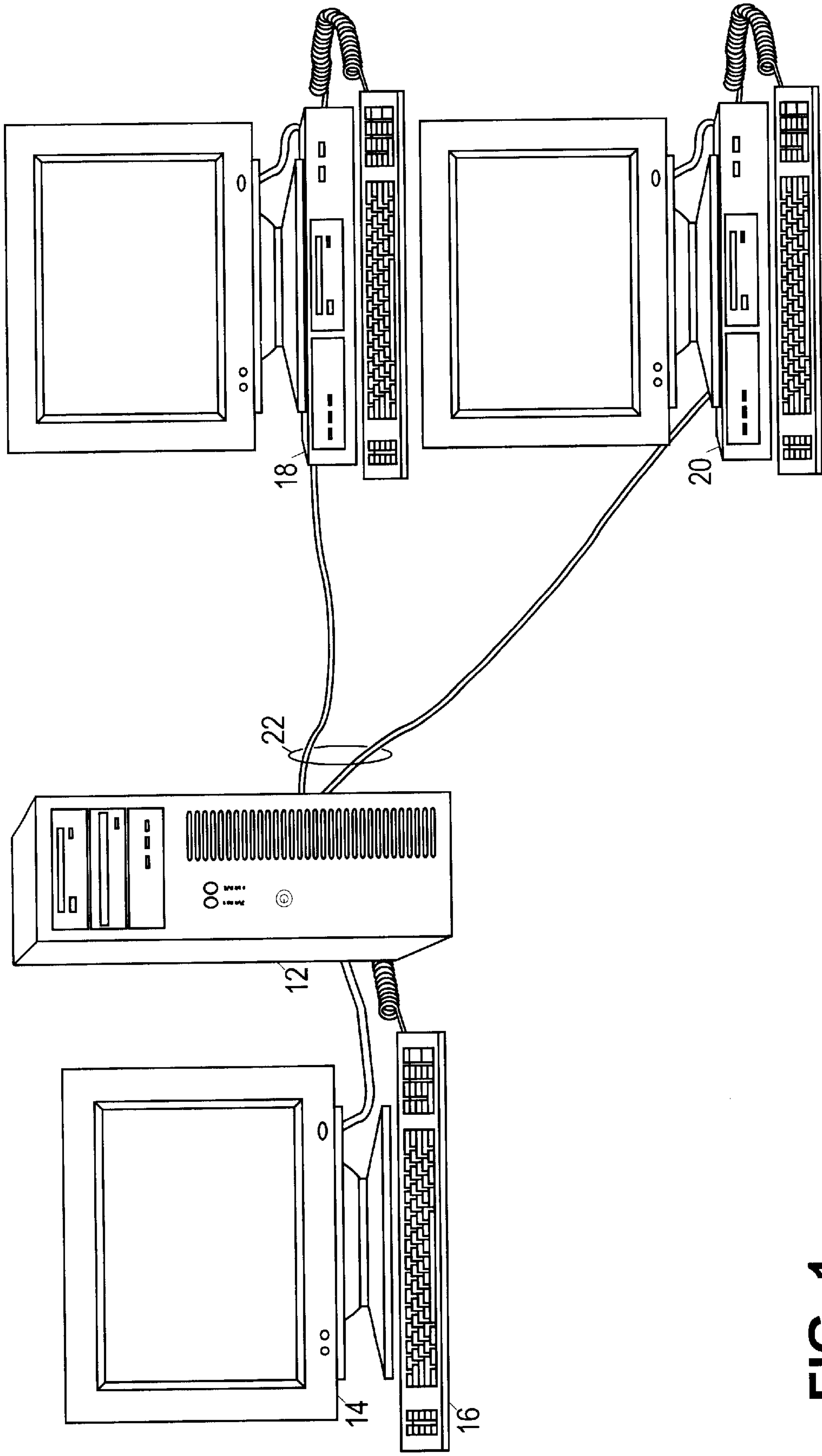


FIG. 1

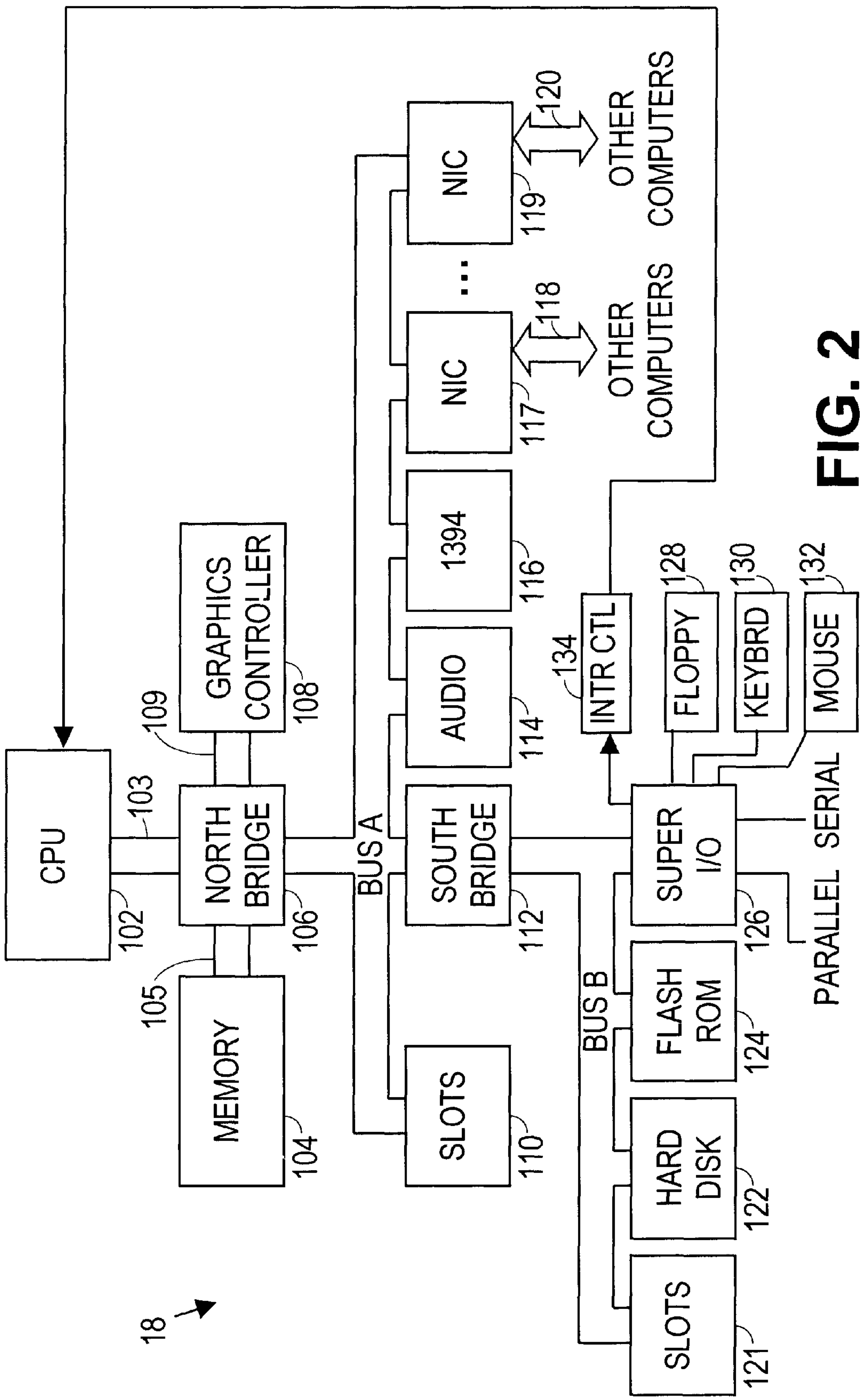

18
CPU
102
103
NORTH BRIDGE
105
106
109
GRAPHICS CONTROLLER
108
MEMORY
104
BUS A
SOUTH BRIDGE
112
SLOTS
110
AUDIO
114
1394
116
NIC
117
118
NIC
119
120
OTHER COMPUTERS
OTHER COMPUTERS
BUS B
SUPER I/O
126
INTR CTL
134
FLOPPY
128
KEYBRD
130
MOUSE
132
SERIAL
PARALLEL
FLASH ROM
124
HARD DISK
122
SLOTS
121

FIG. 2

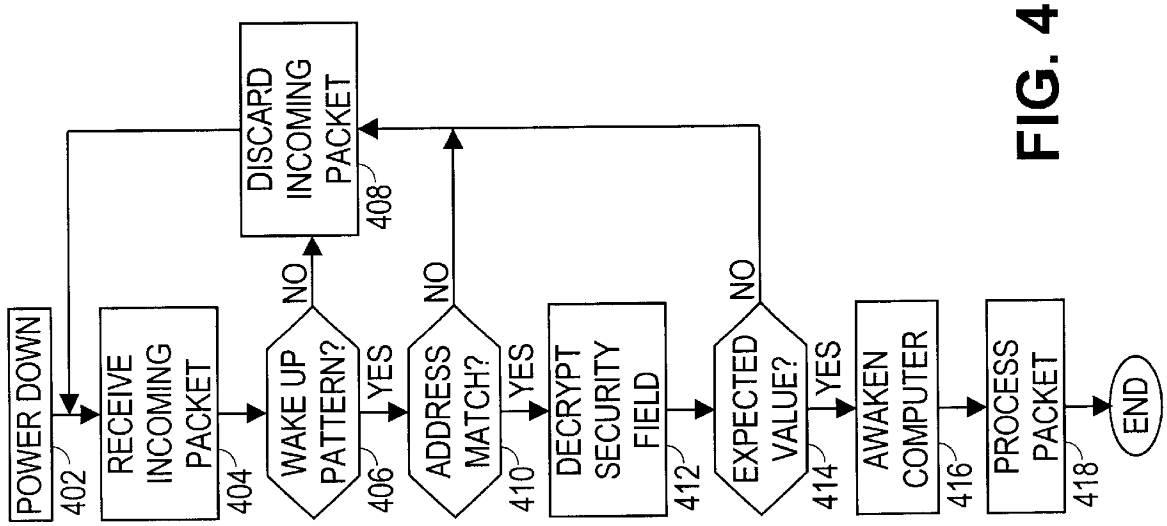

POWER DOWN
402
RECEIVE INCOMING PACKET
404
WAKE UP PATTERN?
406
NO
YES
DISCARD INCOMING PACKET
408
ADDRESS MATCH?
410
NO
YES
DECRYPT SECURITY FIELD
412
EXPECTED VALUE?
414
NO
YES
AWAKEN COMPUTER
416
PROCESS PACKET
418
END

FIG. 4

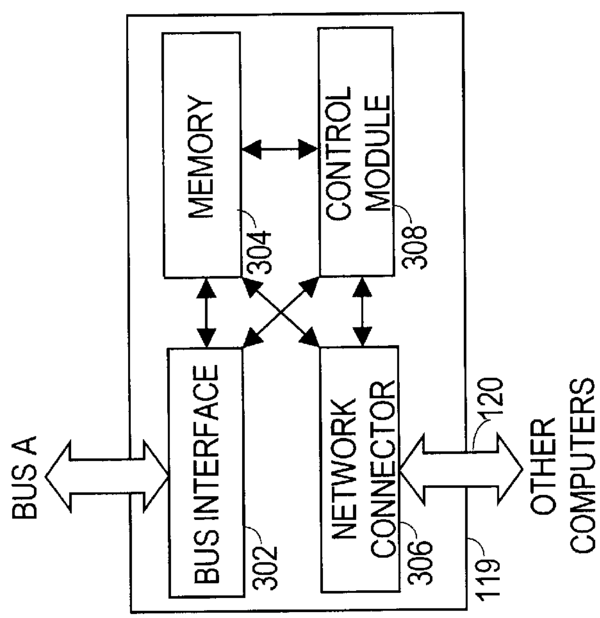

BUS A
BUS INTERFACE
302
MEMORY
304
NETWORK CONNECTOR
306
CONTROL MODULE
308
119
120
OTHER COMPUTERS

FIG. 3

SECURE SYSTEM FOR REMOTELY WAKING A COMPUTER IN A POWER-DOWN STATE

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates generally to network computing systems, and more particularly, to a secure method for remotely waking up a computer on a network.

2. Background of the Invention

Computer networks are commonly used in offices or corporate environments to interconnect personal computers. Well-known local area networks (LANs), such as Ethernet, Token Ring, and ARCnet, are widely used to interconnect a group of computers and other devices that are dispersed over a relatively limited area, such as an office or building, and new LANs continue to be developed. These local area networks provide an efficient and economical way for personal computers to share information and peripherals.

Of course, computer networks are not limited to the confines of an office or building. Smaller networks are commonly interconnected into wide area networks (WANs), such as the Internet, to provide a communications link over a larger area. The Internet is actually a collection of networks that share the same namespace (a set of names in which all names are unique) and use the well-known transmission control protocol/internet protocol (TCP/IP). The Internet currently connects over four hundred networks and tens of thousands of nodes in over forty-two countries. It is estimated that the Internet is now accessed by more than 10 million people every day.

As is well known in the art, the transmission of data packets across networks is governed by a set of rules called "transport protocols". In order for two computers in a local area network to communicate with one another, each computer must use the proper transport protocol for the particular network. During the last decade, many different transport protocols have evolved for use in different networks. For example, TCP/IP is the transport protocol widely used in UNIX based networks and with Ethernet 802.3 LANs; IPX/SPX is the transport protocol used by Novell Corporation's NetWare developed by IBM to operate underneath Microsoft's NetBIOS network interface; DECnet is the transport protocol used by Digital Equipment Corporation for linking computer systems to DECnet-based networks; AppleTalk is the transport protocol developed by Apple Computer, Inc. for linking systems to Apple Macintosh network systems; and XNS is the transport protocol developed by Xerox Corporation that was used in early Ethernet networks. The transport protocols, which are all well known in the art, are often implemented as software drivers which can be loaded into and out of a computer system.

In order to connect to a network, a computer is usually provided with one or more network interface cards (NICs) that provide a data link to the network. Each network interface card has a unique address, referred to herein as its "destination address", which enables each computer to be individually addressed by any other computer in the network. The destination address is typically, but not always, a 12 digit hexadecimal number (e.g., 00AA00123456) that is programmed into memory located on the network interface card and is generally hidden from the user's view. Users are not expected to know and remember the destination address of every computer in the network. Instead, every computer generally has a computer name (commonly corresponding to the user's name and/or machine location) that is more widely known. When a user desires to send a message to another computer, the transport protocol in the network is responsible for converting the name of the other computer into the corresponding destination address to establish a communications link between the two computers.

Because wide area networks often include a collection of a wide variety of machines, organizations and individuals, these networks must provide the means to exchange data between dissimilar machines and across many different transport protocols. Each transport protocol has its own version of addressing information that enables it to exchange electronic mail, data files, programs, etc. between one LAN and another LAN. As a data packet is transmitted across different networks, the addressing information for one transport protocol is replaced by the addressing information for the next transport protocol. Over the Internet, this LAN addressing information is abstracted from the Internet address.

The address of an individual, computer, or organization on the Internet has several layers or components including the domain name or user name, the underlying identifiers used by the transport protocol(s) that govern the data exchange, and the actual destination address. Each transport protocol is designed to extract the appropriate destination address to ensure that each message packet is routed to its intended recipient.

To illustrate the distinctions between the various layers of addressing information, consider an individual computer user in Atlanta that wishes to send an e-mail message to a destination computer in Seattle where the computer in Atlanta is connected to an Internet service provider and the computer in Seattle is connected to a corporate local area network. Generally, the user in Atlanta will know, or can readily obtain, the recipient's computer (e.g., www.recipient.com), but will not know the recipient's Internet address or actual destination address. Nonetheless, the transport protocols will abstract the destination address from the message packet as it is transmitted across the network.

Therefore, the user in Atlanta will simply type the recipient's computer name, www.recipient.com, as the address of the destination computer. The message packet will be sent via the Internet, where the TCP/IP transport protocol will convert the computer name into a more primitive Internet address, which is a 32-bit value that identifies the host's network ID and host ID within the network, e.g., 123.234.5.6. The message packet is then routed to the corporate LAN in Seattle, where a component in the LAN, typically a network router, switch, or server, converts the Internet address into the destination address of the recipient's network interface card, e.g., 00AA00123456.

Meanwhile, the network interface card of the destination computer is designed to continually monitor incoming packets over the network. When the network interface card detects an incoming packet containing its destination address, the network interface card will determine that it is the intended recipient of the packet, and will forward information content of the packet to the destination computer's core, thereby completing the communications link.

In normal operations, in which both the source computer and the destination computer are operating in full power mode, all of these address conversions occur automatically and completely invisible to the user, and the communications link is readily established between the two computers. However, efforts are now being made to extend the use of network computing to power management applications, in

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.