US005724425A

United States Patent [19]

Chang et al.

[11] Patent Number: 5,724,425

[45] Date of Patent: Mar. 3, 1998

[54] **METHOD AND APPARATUS FOR ENHANCING SOFTWARE SECURITY AND DISTRIBUTING SOFTWARE**

[75] Inventors: **Sheue-Ling Chang**, Cupertino; **James Gosling**, Woodside, both of Calif.

[73] Assignee: **Sun Microsystems, Inc.**

[21] Appl. No.: **258,244**

[22] Filed: **Jun. 10, 1994**

[51] **Int. Cl.**[6] **H04L 9/00**; H04L 9/30; H04L 9/32

[52] **U.S. Cl.** **380/25**; 380/4; 380/23; 380/30; 380/49; 380/50

[58] **Field of Search** 380/4, 23, 25, 380/30, 49, 50

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,558,176	12/1985	Arnold et al.	380/4
4,634,807	1/1987	Chorley et al.	380/4
4,670,857	6/1987	Rackman	380/4
5,343,527	8/1994	Moore	380/4

OTHER PUBLICATIONS

Davida et al., "Defending Systems Against Viruses through Cryptographic Authentication", IEEE Symposium, 1989, pp. 312–318.

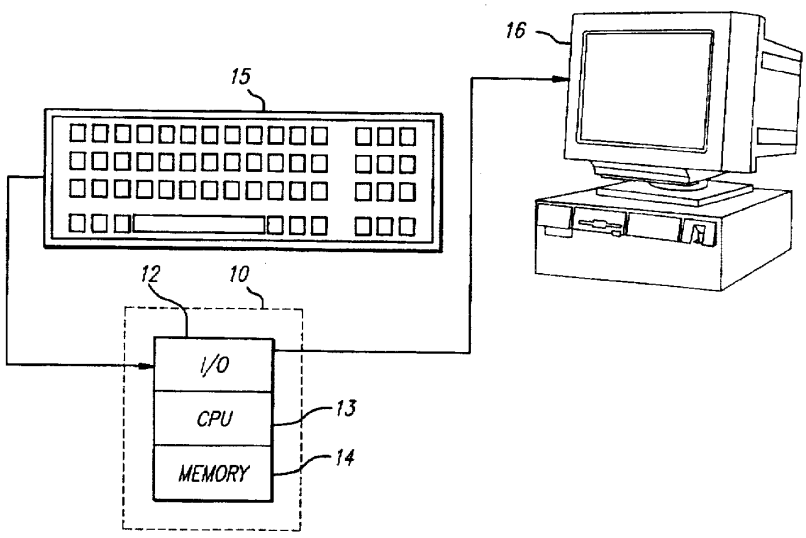
RSA Data Security, Inc., "RSA Certificate Services", Jul. 15, 1993, pp. 1–41.

Primary Examiner—Bernarr E. Gregory
Attorney, Agent, or Firm—McCutchen, Doyle, Brown & Enersen LLP; Ronald S. Laurie, Esq.; Joseph Yang

[57] **ABSTRACT**

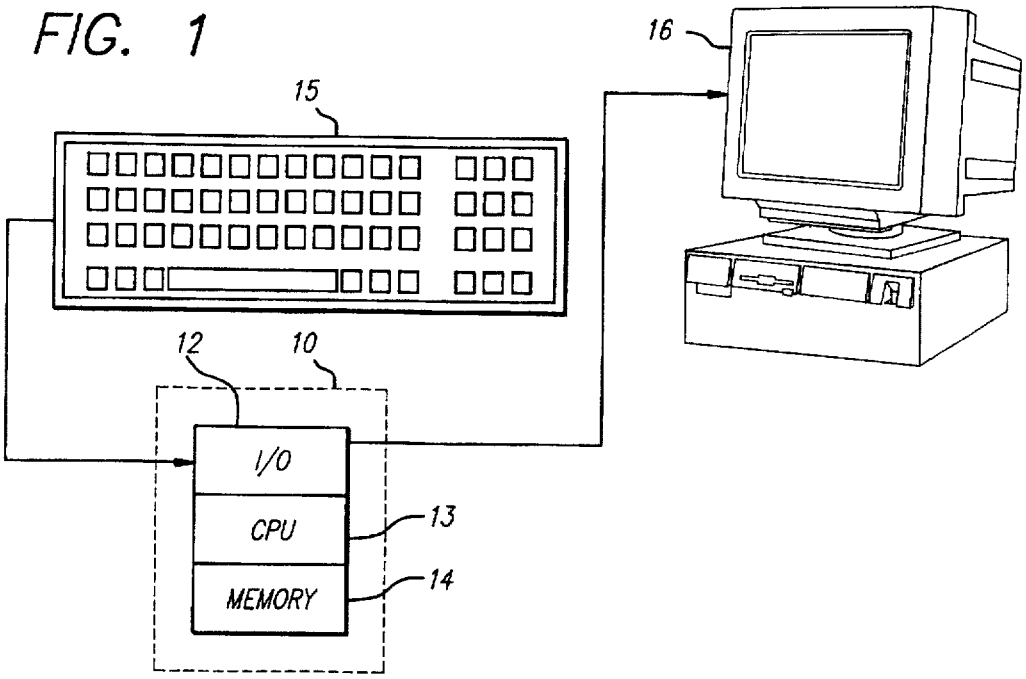
Source code to be protected, a software application writer's private key, along with an application writer's license provided to the first computer. The application writer's license includes identifying information such as the application writer's name as well as the application writer's public key. A compiler program executed by the first computer compiles the source code into binary code, and computes a message digest for the binary code. The first computer then encrypts the message digest using the application writer's private key, such that the encrypted message digest is defined as a digital "signature" of the application writer. A software passport is then generated which includes the application writer's digital signature, the application writer's license and the binary code. The software passport is then distributed to a user using any number of software distribution models known in the industry. A user, upon receipt of the software passport, loads the passport into a computer which determines whether the software passport includes the application writer's license and digital signature. In the event that the software passport does not include the application writer's license, or the application writer's digital signature, then the user's computer system discards the software passport and does not execute the binary code. As an additional security step, the user's computer computes a second message digest for the software passport and compares it to the first message digest, such that if the first and second message digests are not equal, the software passport is also rejected by the user's computer and the code is not executed. If the first and second message digests are equal, the user's computer extracts the application writer's public key from the application writer's license for verification. The application writer's digital signature is decrypted using the application writer's public key. The user's computer then compares a message digest of the binary code to be executed, with the decrypted application writer's digital signature, such that if they are equal, the user's computer executes the binary code.

72 Claims, 5 Drawing Sheets



DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

FIG. 1



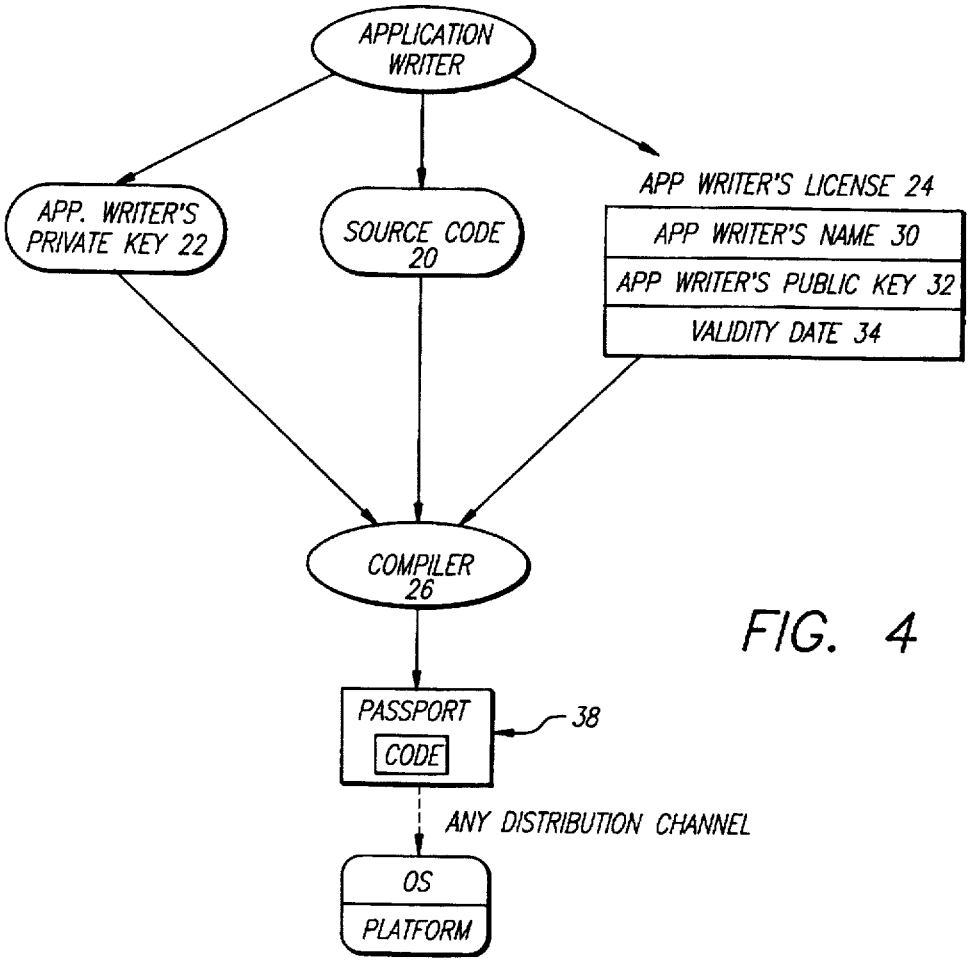
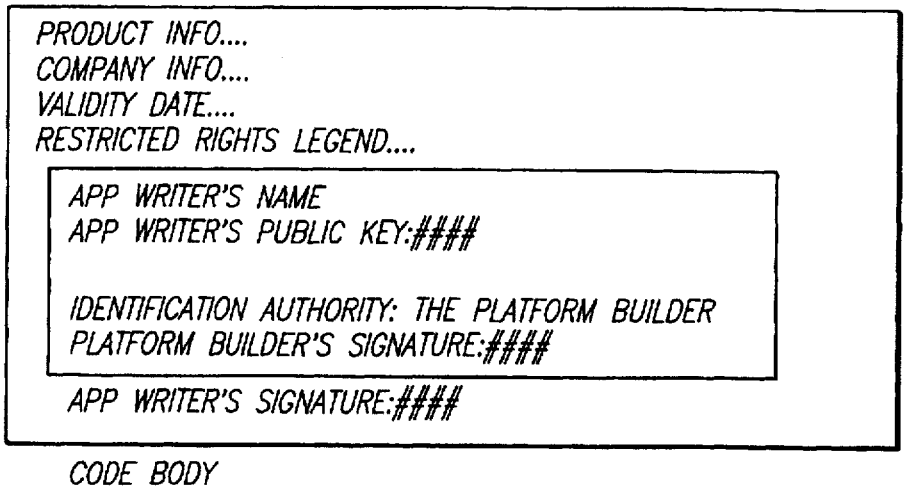


FIG. 4

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

FIG. 2



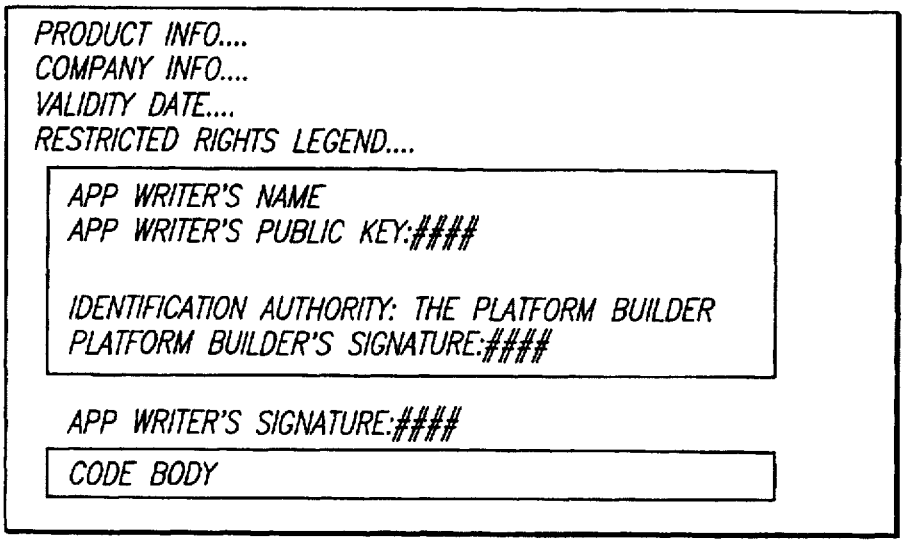
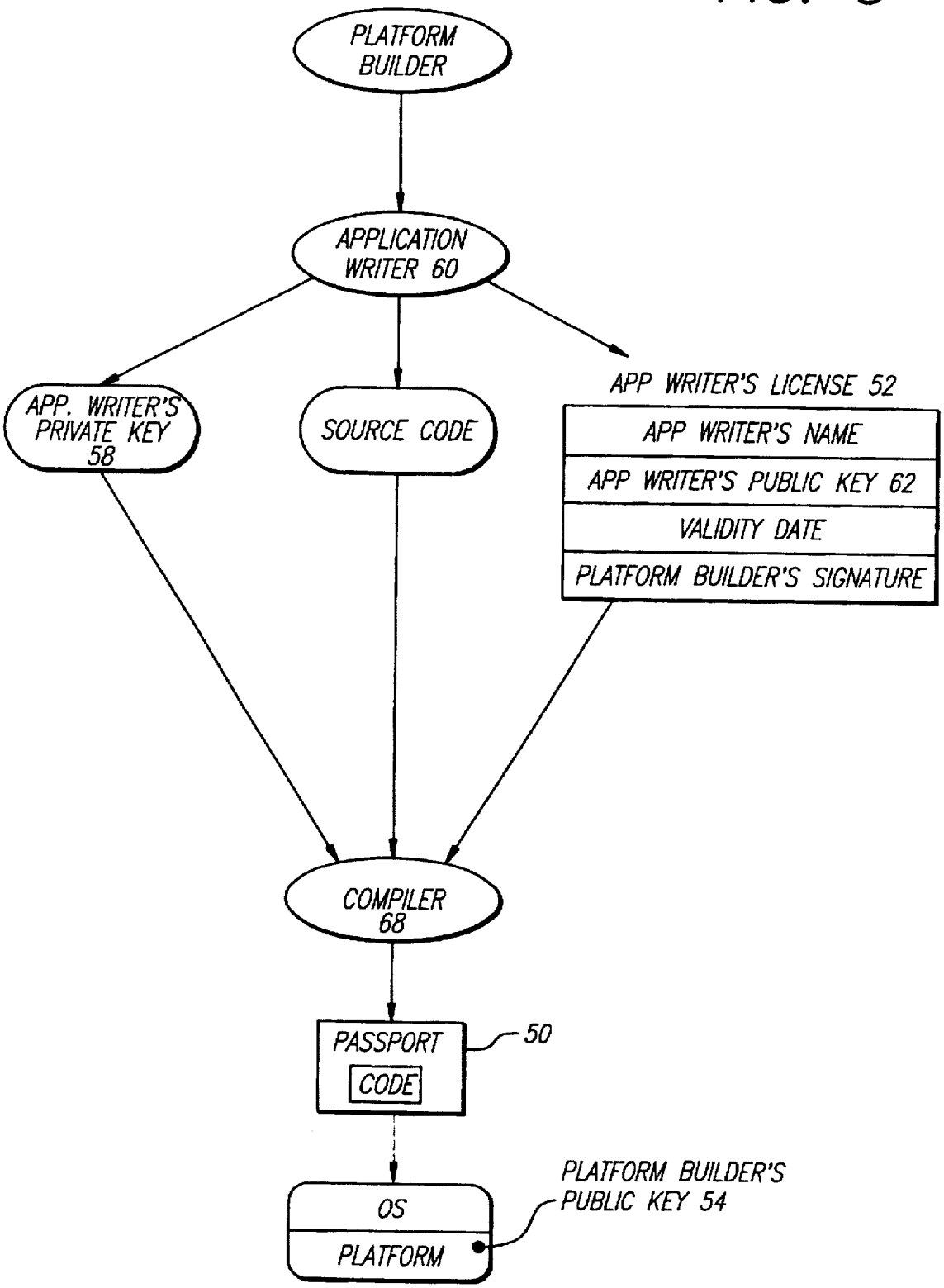


FIG. 3

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

FIG. 5



DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

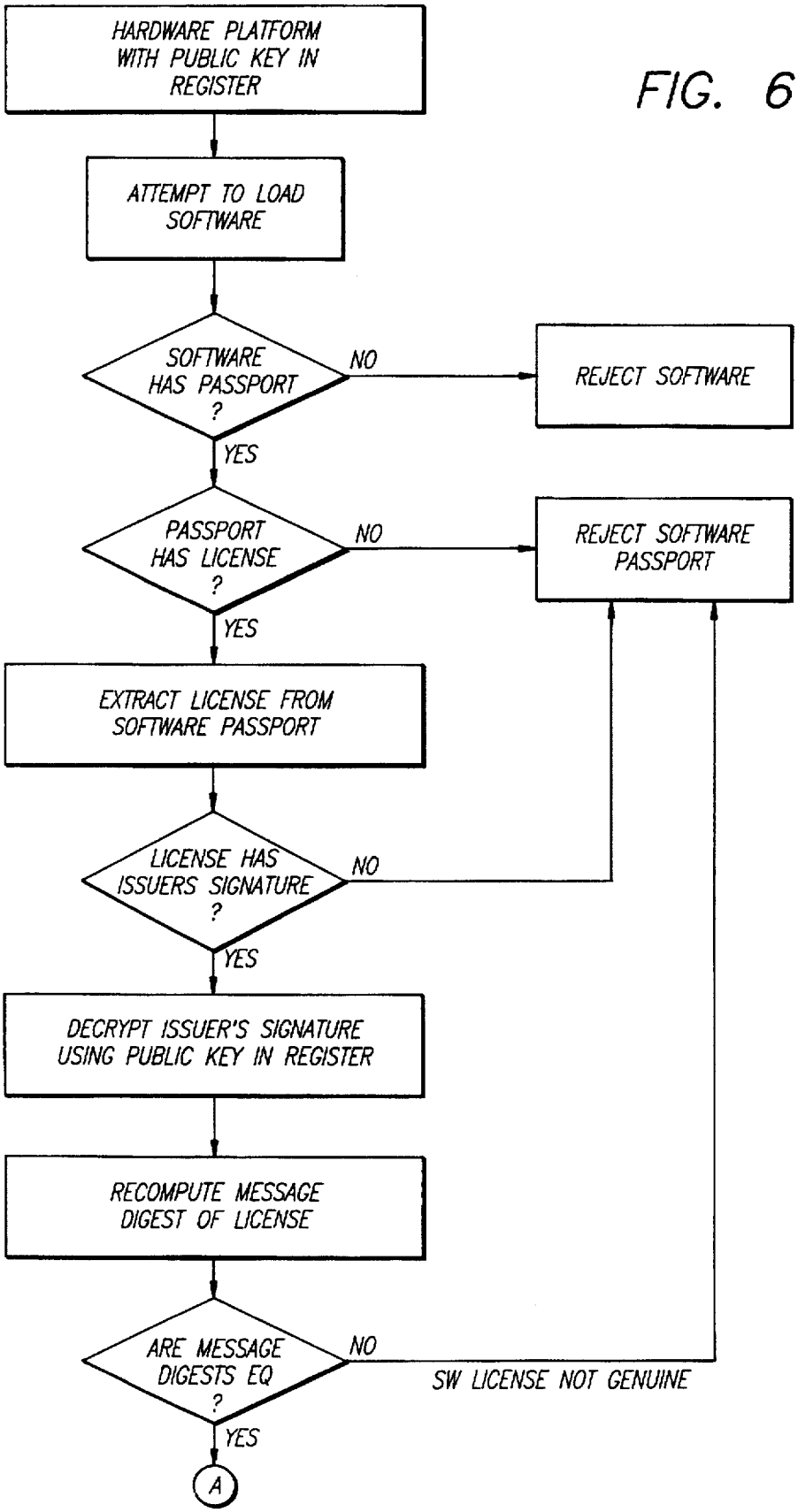


FIG. 6(a)

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

DOCKET ALARM

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.