US005673316A

United States Patent [19]

Auerbach et al.

[11] Patent Number: 5,673,316

[45] Date of Patent: Sep. 30, 1997

[54] **CREATION AND DISTRIBUTION OF CRYPTOGRAPHIC ENVELOPE**

[75] Inventors: **Joshua Seth Auerbach**, Ridgefield, Conn.; **Chee-Seng Chow**, Cupertino, Calif.; **Marc Adam Kaplan**, Katonah, N.Y.; **Jeffrey Charles Crigler**, McLean, Va.

[73] Assignee: **International Business Machines Corporation**, Armonk, N.Y.

[21] Appl. No.: **625,475**

[22] Filed: **Mar. 29, 1996**

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

[52] **U.S. Cl.** **380/4**; 380/25

[58] **Field of Search** 380/3, 4, 23, 24, 380/25, 28, 49

[56] **References Cited**

U.S. PATENT DOCUMENTS

5,319,705	6/1994	Halter et al.	380/4
5,394,469	2/1995	Nagel et al.	380/4
5,416,840	5/1995	Cane et al.	380/4
5,428,685	6/1995	Kadooka et al.	380/25
5,490,216	2/1996	Richardson	380/4
5,509,070	4/1996	Schull	380/4
5,530,752	6/1996	Rubin	380/4
5,553,143	9/1996	Ross et al.	380/25
5,586,186	12/1996	Yuval et al.	380/4

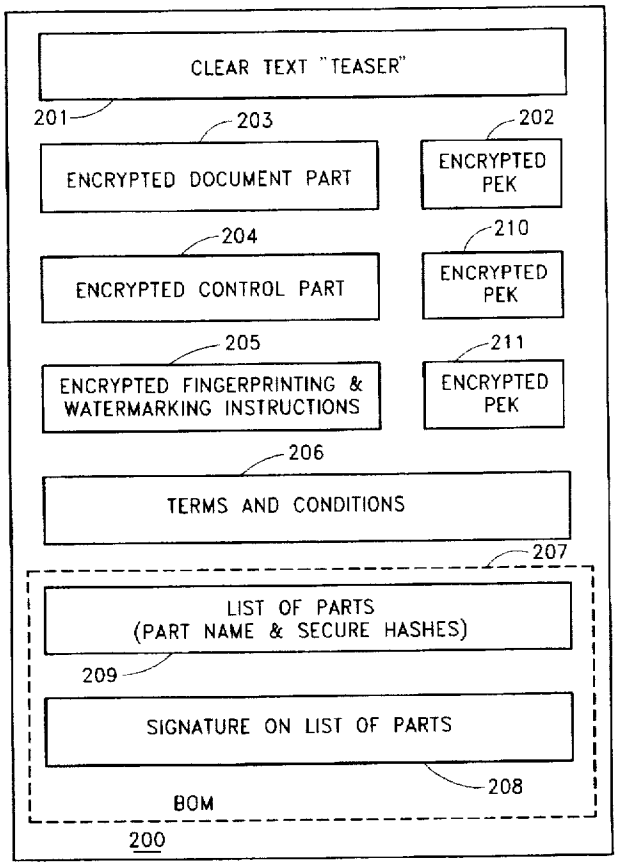
Primary Examiner—David C. Cain

Attorney, Agent, or Firm—Douglas W. Cameron

[57] **ABSTRACT**

A method and apparatus to create, distribute, sell and control access to digital documents using secure cryptographic envelopes. An envelope is an aggregation of information parts, where each of the parts to be protected are encrypted with a corresponding part encryption key. These encrypted information parts along with the other information parts become part of the envelope. Each part encryption key is also encrypted with a public key, and these encrypted part encryption keys are also included in the envelope. The envelope also includes a list of parts where each entry in the list has a part name and a secure hash of the named part. The list is then signed with a secret key to generate a signature, which is also included in the envelope. The signature can be verified using a second public key associated with first secret key, and the integrity of any information part in the envelope can be checked by computing a second hash and comparing it with the corresponding hash in the list of parts. Also, the information content of any encrypted part can only be recovered by knowledge of a second secret key corresponding to the public key that was used to encrypt the part encryption keys.

8 Claims, 6 Drawing Sheets



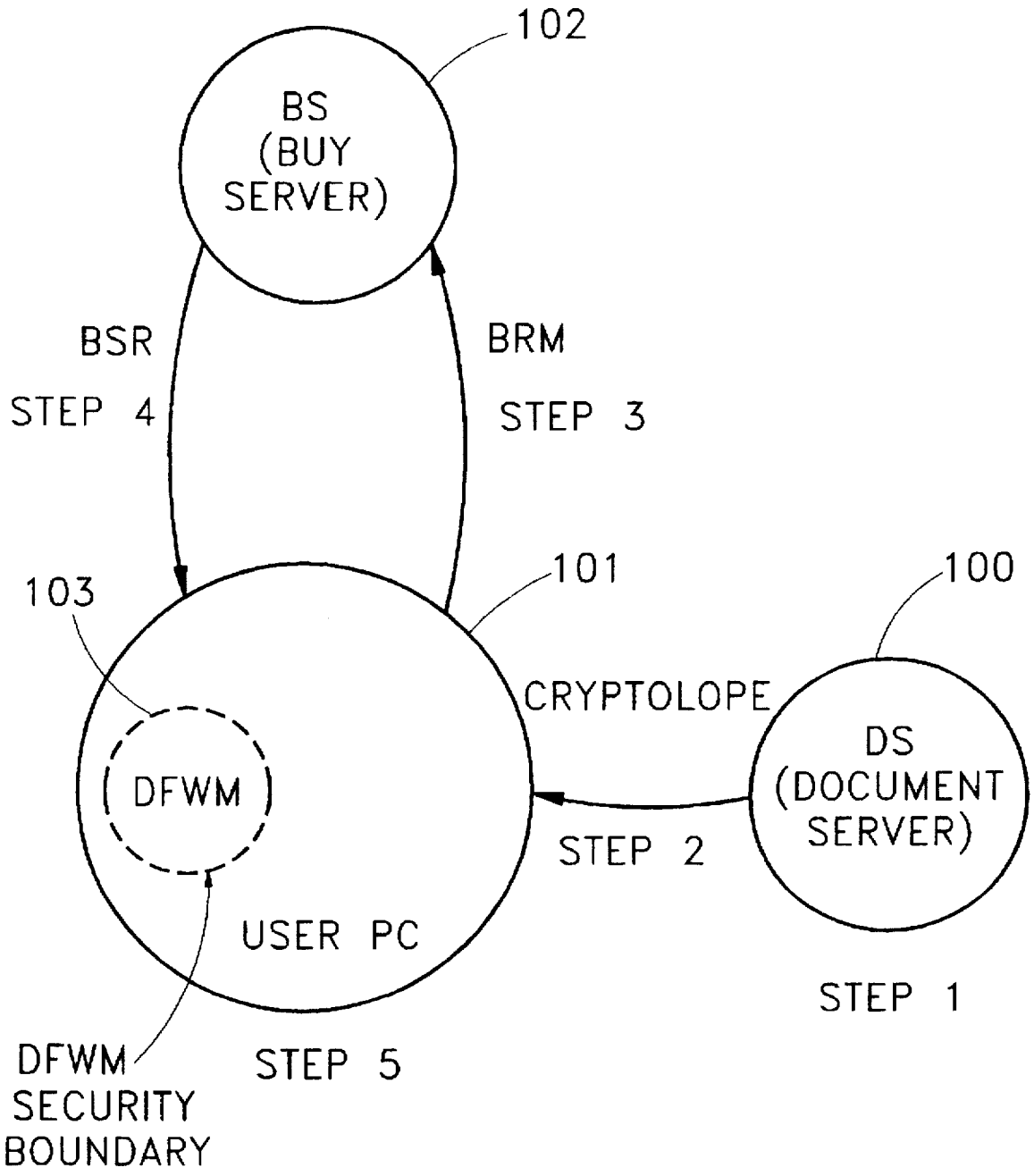


FIG. 1

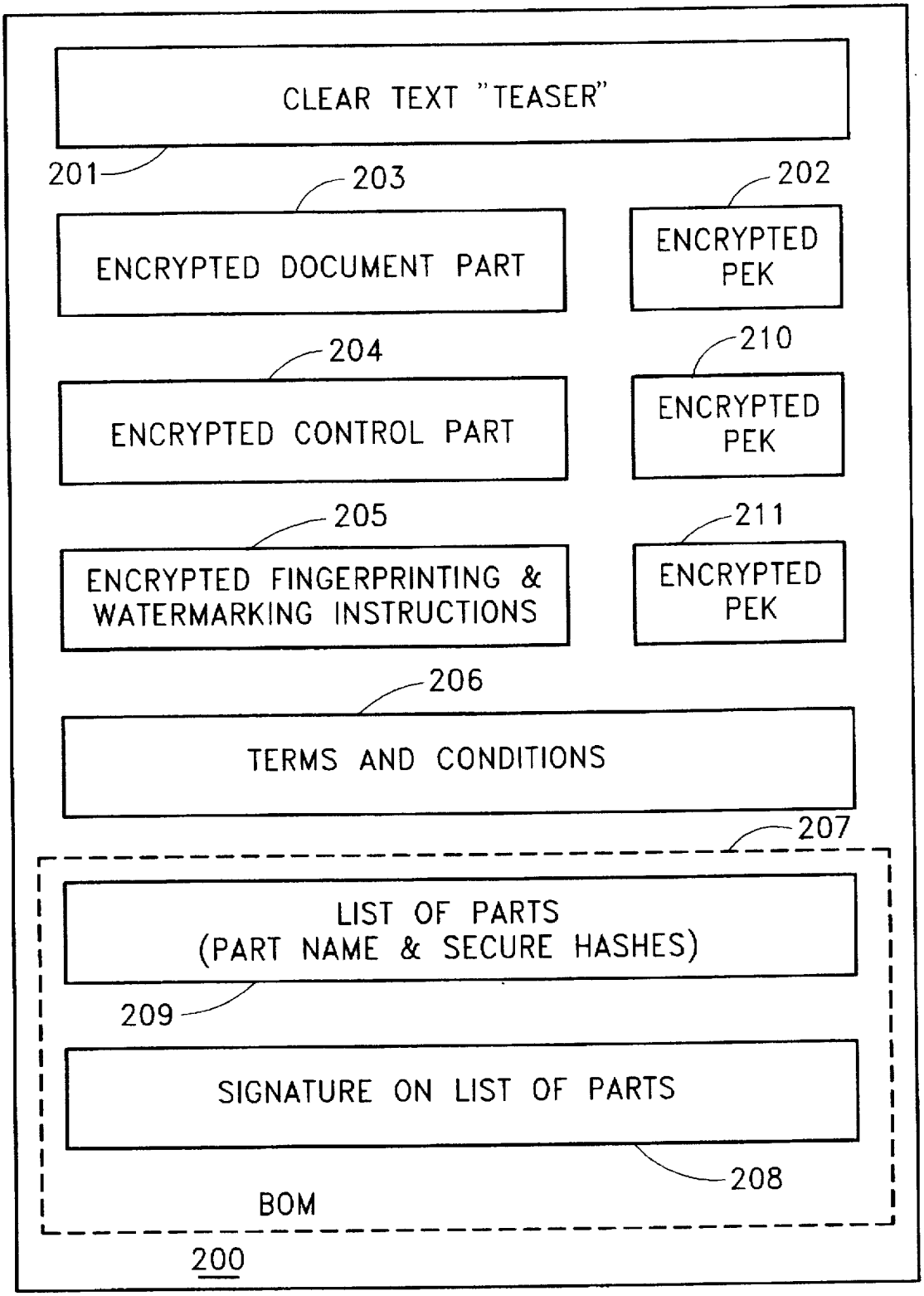


FIG.2

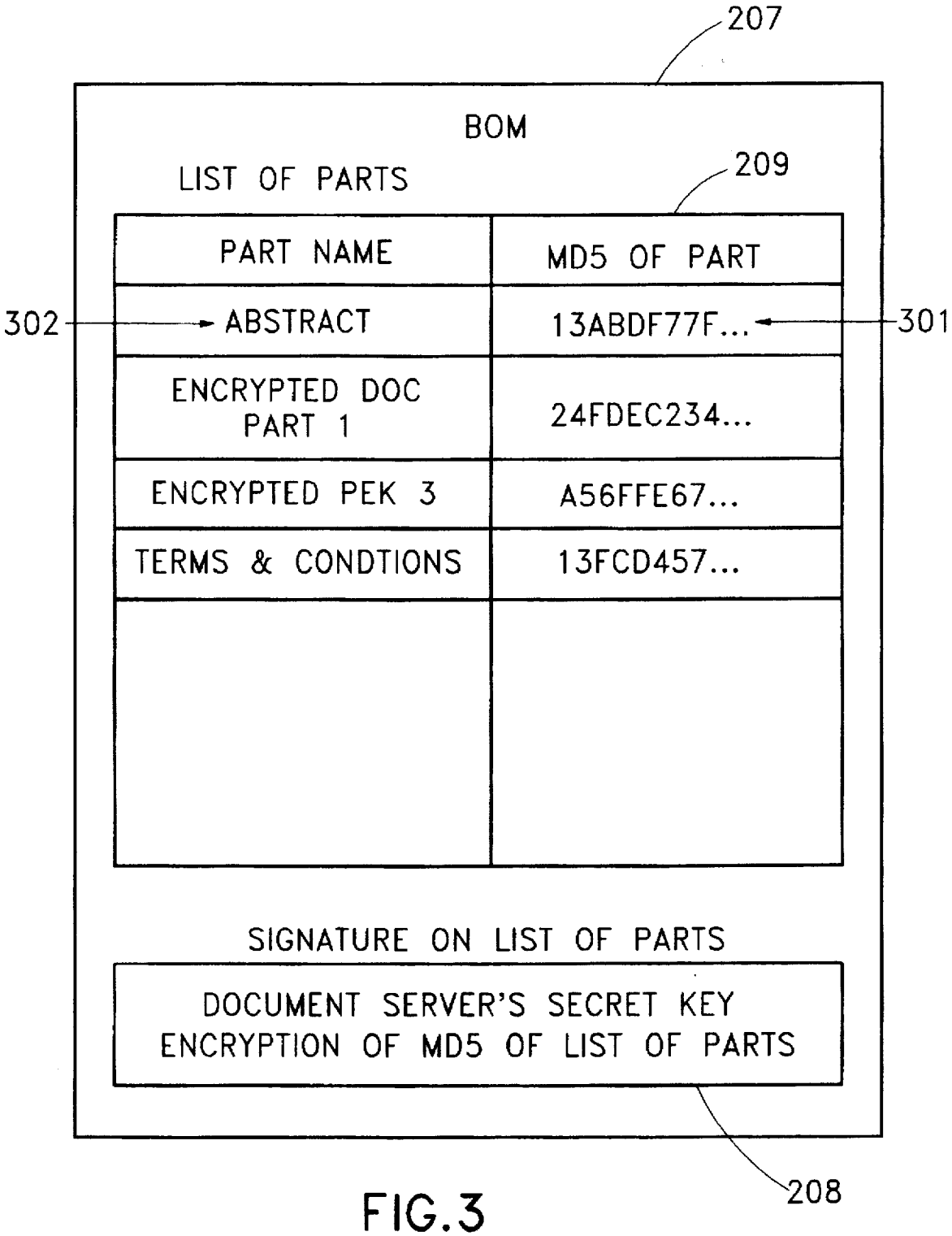


FIG.3

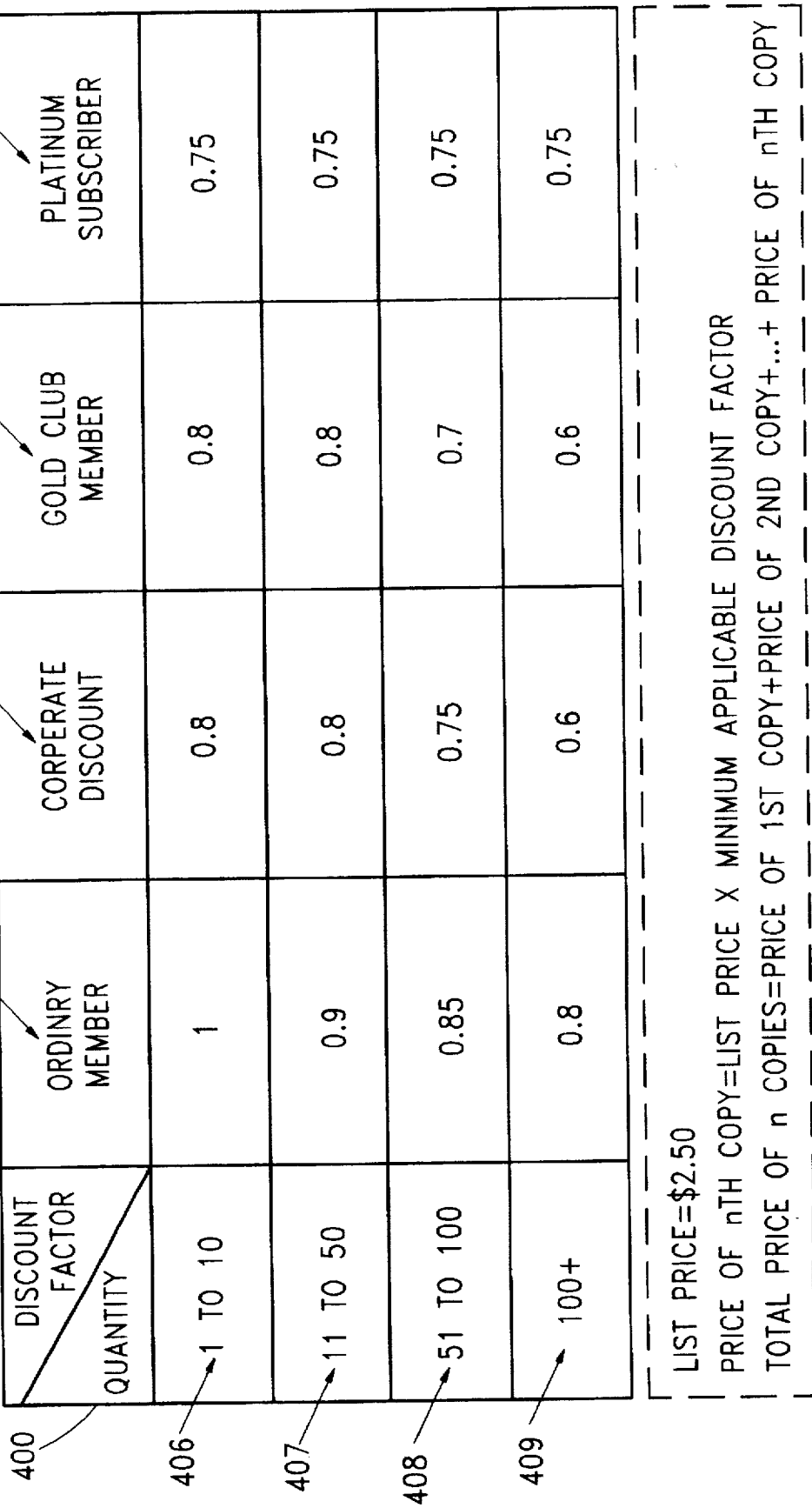


FIG. 4

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.