

(12) **UK Patent Application** (19) **GB** (11) **2 362 489** (13) **A**

(43) Date of A Publication **21.11.2001**

(21) Application No **0011673.1**

(22) Date of Filing **15.05.2000**

(71) Applicant(s)
tom.com enterprises Limited
(Incorporated in the British Virgin Islands)
PO Box 957, Offshore Incorporations Centre,
Road Town, Tortola, British Virgin Islands

(72) Inventor(s)
Carl Chang
Sandroff Ma
Leo Hau

(74) Agent and/or Address for Service
Lloyd Wise, Tregear & Co
Commonwealth House, 1-19 New Oxford Street,
LONDON, WC1A 1LW, United Kingdom

(51) INT CL⁷
G06F 1/00 , G07F 19/00

(52) UK CL (Edition S)
G4H HTG H1A H13D H14A H14D
U1S S2124 S2196 S2215

(56) Documents Cited
EP 0844551 A2 **WO 95/19593 A1**

(58) Field of Search
UK CL (Edition R) **G4A AAP , G4H HTG**
INT CL⁷ **G06F , G07F**

(54) Abstract Title
Secure communication

(57) A method is presented for validating a purchase instruction which a user transmits to a server by internet. The server accesses a database to obtain contact information for the user, e.g. a phone number, and transmits a validation code to the user using the contact information. The user returns the validation code to the server by internet, and so validates the purchase.

GB 2 362 489

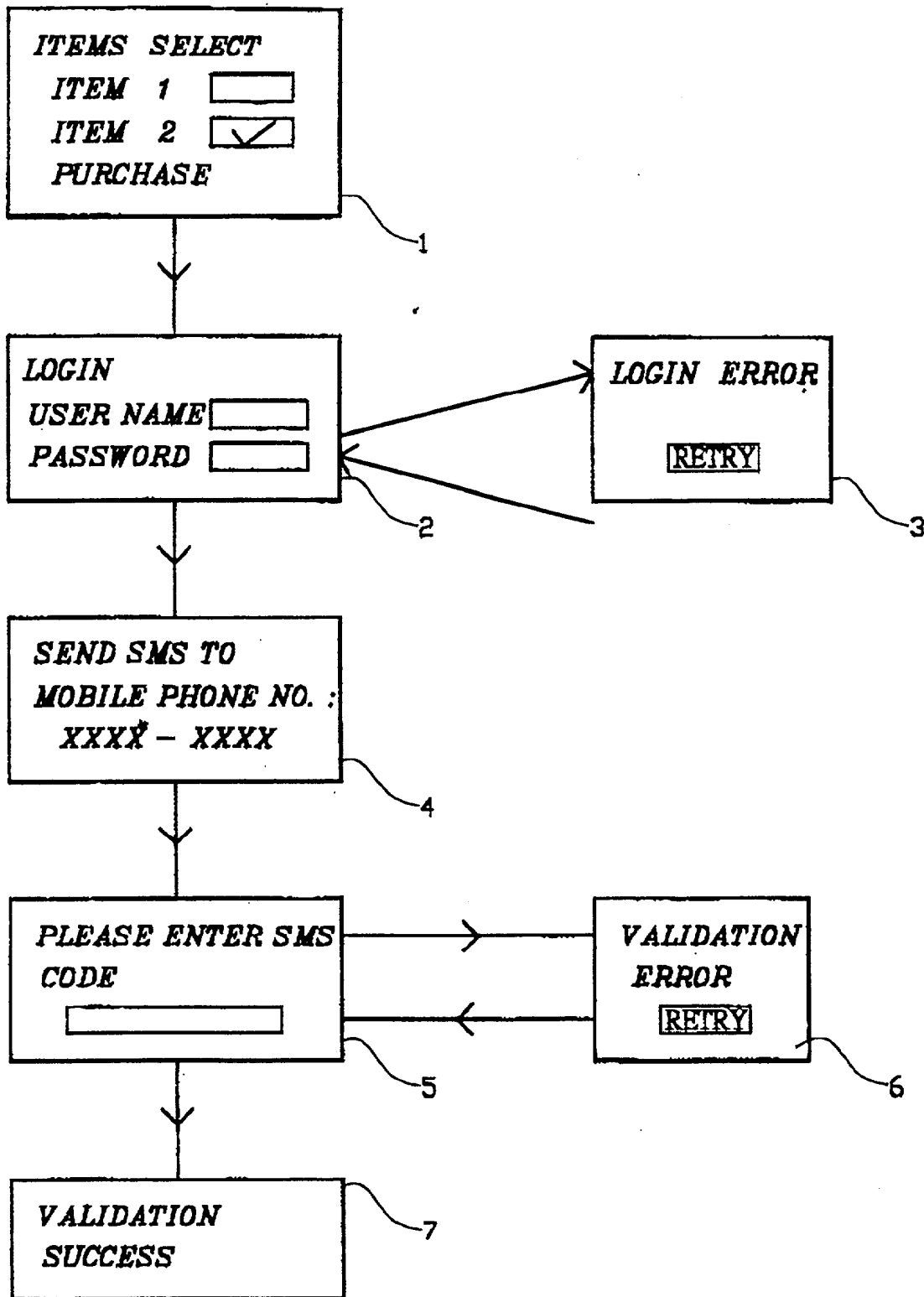


Fig.1

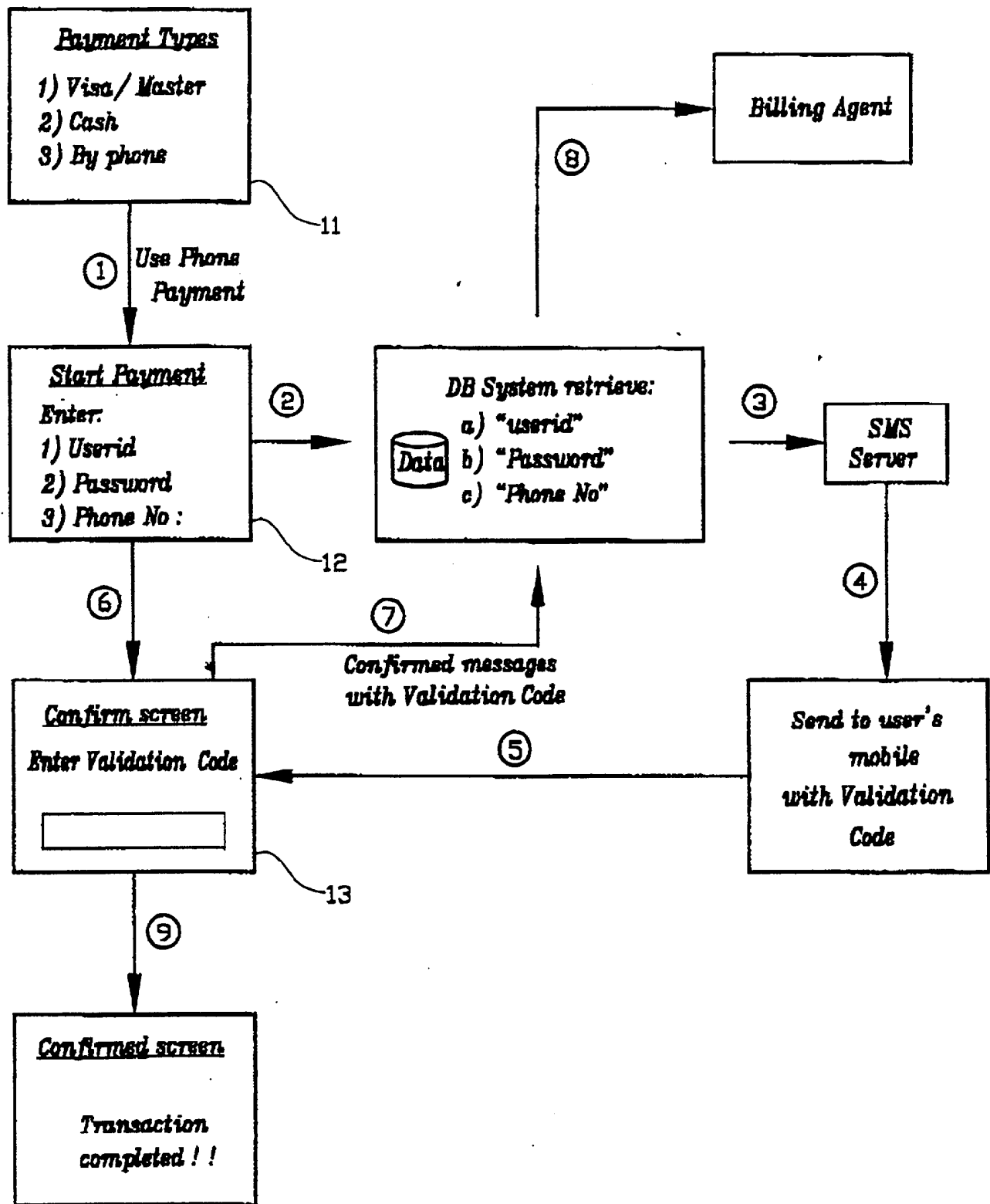


Fig.2

Secure communication

Field of the invention

- 5 The present invention relates to methods and apparatus for securely transferring instructions over a telecommunications network, such as the internet. The invention is especially useful for instructing commercial transactions online.

Background of the invention

10

Internet commerce is presently growing rapidly, and encompasses the purchase by users of goods, services and even information (e.g. it is now possible to pay to download music).

To make a purchase, a user communicates purchase instructions via the
15 internet to a website operated by a retailer. The instructions often include details of a credit card account held by the user. Typically, this data is printed on the credit card itself. The retailer accepts the purchase (e.g. the retailer may dispatch the purchased goods), and debits the user's credit card accordingly.

The above system is subject to a security problem that the data on the credit
20 card is accessible to any third party who gains access to the card. Such a person can remember the credit card data printed on the card, and make purchases on his own account at any later time.

Often a single user will make multiple purchases from the same website over

an extended period of time. To avoid the necessity for a given user to transmit the same credit card data repeatedly, it is known for the website to maintain a database of credit card information for many respective users. Each user is supplied with (or chooses) identification data which identifies him. The identification data includes a password and normally also a user name. Whenever a user wishes to make a purchase from the website he supplies the website with his identification data. The website uses the identification data to access the database of credit card data, and extracts the credit card information for the user.

This arrangement exacerbates the security problem identified above, since a third party who gains access to the identification data can use the website to make purchases. Such a third party may, for example, be an operative of the retailer. Alternatively, the third party may gain access to the identification data because the user has recorded it somewhere (e.g. on paper) to avoid having to remember it. In fact, the level of crime associated with online purchasing is rising rapidly.

Although, as explained, the problem of internet security is particularly acute in the example of online purchasing, it arises in other cases also. Indeed, there are many instances in which a user wishes to communicate securely with a website.

Summary of the invention

The present invention seeks to provide methods and apparatus for secure internet communication, especially for transmitting purchase instructions to an internet retailer.

In general terms the present invention proposes that user supplies a website

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.