# Exhibit 1

US007137140B2

(12) **United States Patent**
**Safa**

(10) **Patent No.: US 7,137,140 B2**
(45) **Date of Patent: Nov. 14, 2006**

(54) **TRANSACTION VERIFICATION**

(75) Inventor: **John Aram Safa**, Nottingham (GB)

(73) Assignee: **Simplex Major SDN.BHD**, Selangor DE (MY)

( * ) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 918 days.

(21) Appl. No.: **09/905,572**

(22) Filed: **Jul. 13, 2001**

(65) **Prior Publication Data**

US 2002/0010864 A1 Jan. 24, 2002

(30) **Foreign Application Priority Data**

Jul. 18, 2000 (GB) ..... 0017479.7

(51) **Int. Cl.**
***G06F 17/30*** (2006.01)

(52) **U.S. Cl.** ..... **726/6**; 726/18; 726/21

(58) **Field of Classification Search** ..... 713/200–202; 726/2, 3, 4, 6, 18, 21
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

| | | | |
|---|---|---|---|
| 4,885,777 | A | 12/1989 | Takaragi et al. |
| 5,337,357 | A | 8/1994 | Chou et al. |
| 5,521,980 | A | 5/1996 | Brands |
| 5,668,878 | A | 9/1997 | Brands |
| 5,696,827 | A | 12/1997 | Brands |
| 5,793,028 | A | 8/1998 | Wagener et al. |
| 6,023,509 | A | 2/2000 | Herbert et al. |
| 6,078,902 | A | 6/2000 | Schenkler |
| 6,131,162 | A | 10/2000 | Yoshiura et al. |
| 6,148,407 | A | 11/2000 | Aucsmith |
| 6,948,168 | B1 | 9/2005 | Kuprionas |

FOREIGN PATENT DOCUMENTS

| | | | |
|---|---|---|---|
| GB | 2 355 322 | 4/2001 | |
| WO | 97/50207 | 12/1997 | |
| WO | 98/44402 | 10/1998 | |
| WO | 00/31644 | 6/2000 | |

OTHER PUBLICATIONS

http://www.east-shore.com/verify.html.*
http://www.divassoftware.com/services/securityNet.htm.*
http://biz.yahoo.com/pz/050131/71730.html.*
Access control system with high level security using fingerprints, Younhee Gil; Dosung Ahn; Sungbum Pan; Yongwha Chung; Applied Imagery Pattern Recognition Workshop, 2003. Proceedings. 32nd, Oct. 15-17, 2003 pp. 238-243.*
Fingerprint multicast in secure video streaming, Zhao, H.V.; Liu, K.J.R.; Image Processing, IEEE Transactions on, vol. 15, Issue 1, Jan. 2006 pp. 12-29.*
Forensic analysis of nonlinear collusion attacks for multimedia fingerprinting, Zhao, H.V.; Min Wu; Wang, Z.J.; Liu, K.J.R.; Image Processing, IEEE Transactions on, vol. 14, Issue 5, May 2005 pp. 646-661.*
Lang, Paul, "How to Beat Credit Card Fraud," NETrageous Inc., Olney, MD. http://web.archive.org/web/20000118013545/http://scambusters.org/reports/lang.html.

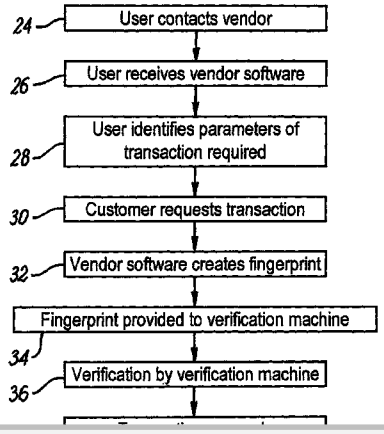
* cited by examiner

*Primary Examiner*—David Jung
(74) *Attorney, Agent, or Firm*—Smith-Hill and Bedell

(57) **ABSTRACT**

A customer computer **12**, vendor computer **16** and verification computer **14** are interconnected by means of a network **18**, such as the internet The customer **12** can initiate a transaction, such as the purchase of information from the vendor **16**. However, the vendor **16** will not proceed until verification of the transaction has been received from the site **14**. This is not provided until the customer **12** has sent a unique fingerprint of data to the site **14**, identifying the customer machine by reference to hardware device types or serial numbers, software types or licences, e-mail addressed or the like. This fingerprint is stored for future reference in showing that the transaction was validly implemented by the customer machine **12**.

**37 Claims, 2 Drawing Sheets**



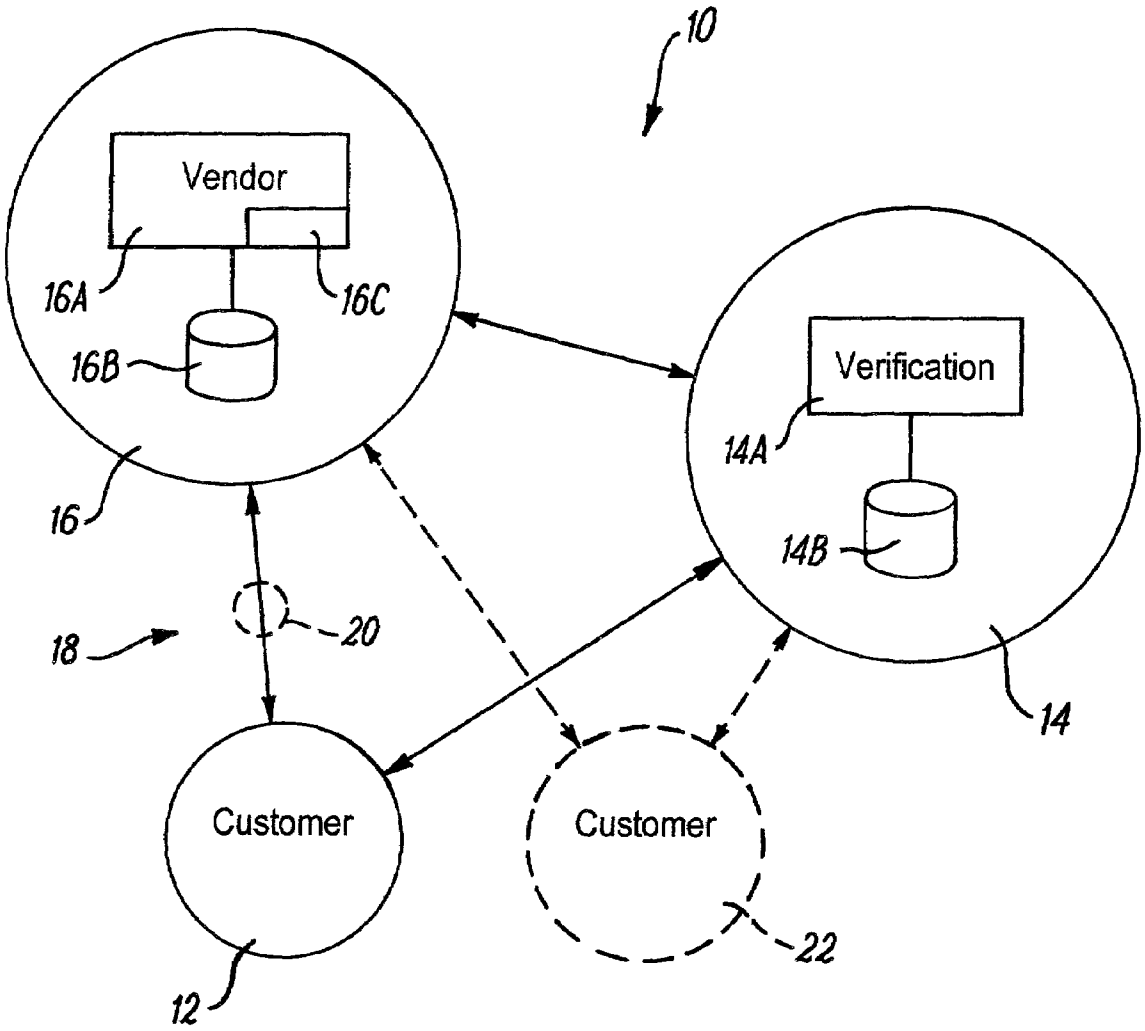



FIG. 1

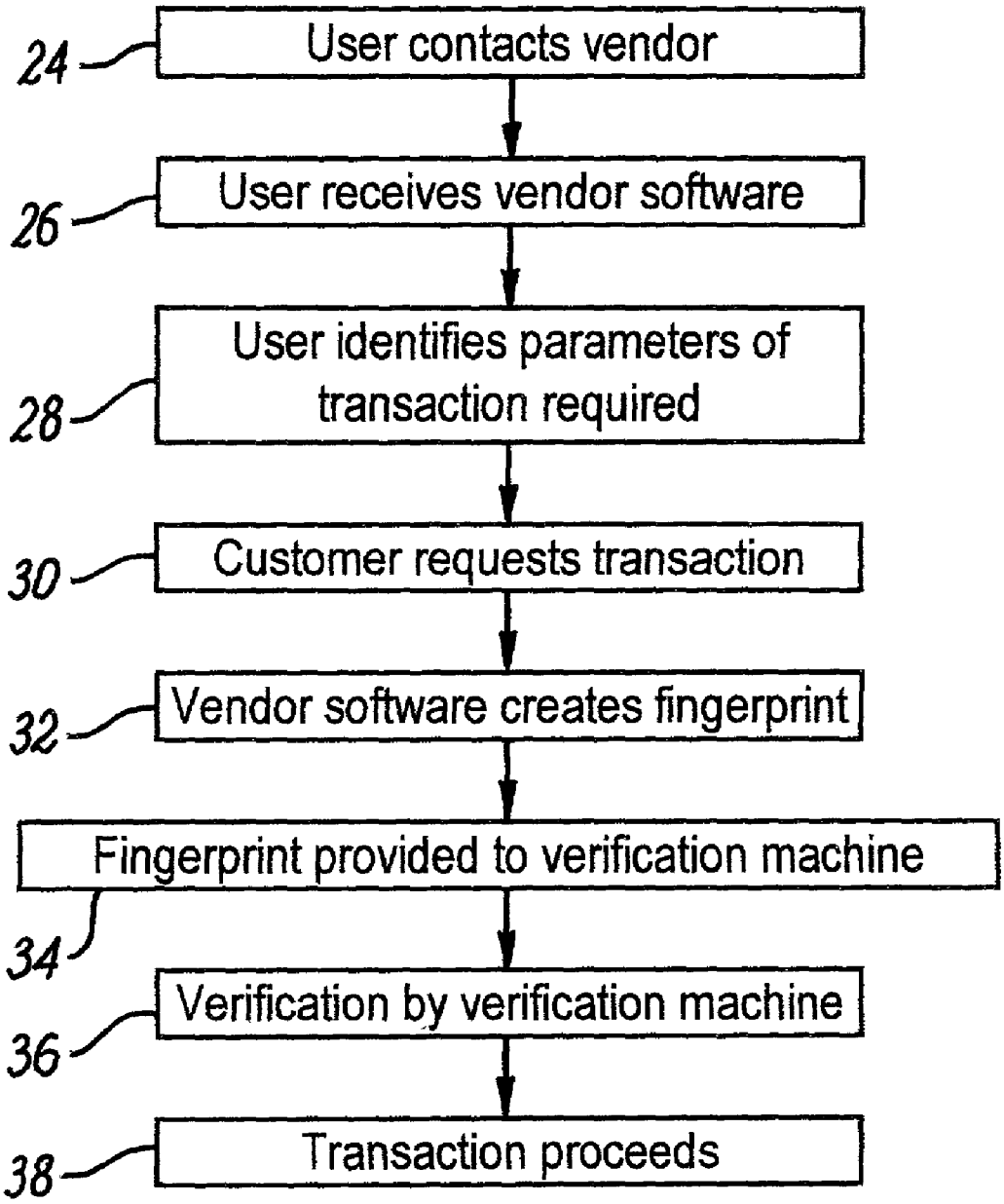



FIG. 2

# TRANSACTION VERIFICATION

## CROSS REFERENCE TO RELATED APPLICATION

This application claims priority under 35 USC 119 of United Kingdom Patent Application No. 0017479.7 filed Jul. 18, 2000.

The present invention relates to transaction verification and in particular, to a system for verification of transactions executed by means of computer-based networks.

Commercial transactions conducted by means of computer networks, such as the internet, are becoming increasingly common. These transactions are often termed "e-commerce". It is important to provide adequate security for these transactions if businesses based on them are to be successful. Various encryption techniques have been proposed for providing security, but have not proved entirely successful. In particular, the encryption technique being used by the sender must be understood by the recipient in order for the recipient to be able to decrypt the information sent. This gives rise to compatibility problems in practice, at least until encryption techniques become standardised. Therefore, there exists a problem in providing a system by which e-commerce transactions can be executed, but which is constructed in a manner which allows transactions to be verified in advance, by an arrangement which presents minimal technical constraints on the user. This allows the equipment of a wide range of users to be technically compatible with the system without extensive modification or setting up procedures, which would act as a deterrent to the use of the system.

The present invention provides a transaction verification system for use in verifying transactions between computers connected by a computer network, the system comprising fingerprint means operable in association with at least one first computer of the network to seek information relating to the first computer in order to create a group of data to serve as a fingerprint which is substantially unique to the first computer, and to provide the fingerprint for transmission to a second computer when the first computer is operated to initiate a transaction, to allow the source of the transaction initiation to be substantially uniquely identified.

The fingerprint preferably includes data which identifies components of the system of the first computer. The fingerprint may include data relating to hardware present within the first computer, or to software present within the first computer. The fingerprint may further include data input by the user in response to a prompt provided by the fingerprint means.

The second computer may store the fingerprint in association with details of the transaction, for future reference to identify the first computer. The second computer is preferably operable to provide a message confirming that the fingerprint has been stored and authorising the transaction to proceed. The second computer may be operable to store, with the fingerprint, the route by which the fingerprint travelled across the network, including details of any servers through which the fingerprint passed. The second computer may use the fingerprint to provide active verification of the validity of the transaction. The second computer may be operable to effect a payment authorisation in response to receiving details of the transaction. The second computer may incorporate a database operable to identify the payment required and/or made in relation to the transaction. The



transaction, for authorising the transaction in accordance with the result of the comparison.

The first computer may comprise transaction means operable to create a transaction request identifying a required transaction, and means operable to transmit the transaction request over the network to another computer with which the transaction is to be conducted. The said another computer may be a third computer. The system may comprise a plurality of first computers able to initiate transactions as aforesaid, a plurality of third computers operable to execute transactions requested by the first computers, and a second computer common to at least some of the first and third computers and operable to receive a fingerprint associated with a transaction, and to store that fingerprint as verification of that transaction.

Alternatively, the system may comprise a plurality of first computers able to initiate a transaction as aforesaid, and a plurality of further computers, at least one of which is operable to execute transactions requested by the first computers and also to receive a fingerprint associated with each transaction, and to store that fingerprint as verification of that transaction.

A transaction may include the purchase of data which is downloaded to the first computer over the network.

The fingerprint means may comprise software operable as aforesaid.

The, or each of the computers which are connected to the network and are operable to complete transactions requested by the first computer are preferably operable to download the fingerprint means to the first computer. Preferably the fingerprint means is downloaded as part of a dialogue by which the parameters of the transaction are set by operation of the first computer, and wherein the fingerprint means are required to be run to create a fingerprint as aforesaid, before the transaction takes place.

The invention also provides a computer comprising means operable to connect the computer to a network over which transactions can be executed, the computer further comprising fingerprint means operable to seek information relating to the computer in order to create a group of data to serve as a fingerprint which is substantially unique to the computer, and operable when the said computer is operated to initiate a transaction, to provide the fingerprint for transmission to a second computer to allow the source of the transaction initiation to be uniquely defined.

The fingerprint preferably includes data which uniquely identifies components of the system of the first computer. The fingerprint may include data relating to hardware present within the first computer. The fingerprint may include data relating to software present within the first computer. The fingerprint may include data input by the user in response to a prompt provided by the fingerprint means.

The said first computer may comprise transaction means operable to create a transaction request identifying a required transaction, and means operable to transmit the transaction request over the network to another computer with which the transaction is to be conducted. The transaction may include the purchase of data which is downloaded to the first computer over the network.

The fingerprint means may comprise software operable as aforesaid.

The invention also provides a computer comprising means operable to connect the computer to a network over which transaction can be executed, the computer comprising

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.