(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 January 2007 (04.01.2007)

PCT

(10) International Publication Number
WO 2007/001394 A2

(51) International Patent Classification:
G06Q 99/00 (2006.01)

(21) International Application Number:
PCT/US2005/035532

(22) International Filing Date:
29 September 2005 (29.09.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/694,768 27 June 2005 (27.06.2005) US

(63) Related by continuation (CON) or continuation-in-part (CIP) to earlier application:
US 10/791,439 (CIP)
Filed on 2 March 2004 (02.03.2004)

(71) Applicant *(for all designated States except US)*: **THE 41st PARAMETER, INC.** [US/US]; 14301 North 87th Street, Suite 211, Scottsdale, AZ 85260 (US).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **EISEN, Ori** [IL/US]; 6214 East Hillery Drive, Scottsdale, AZ 85254-2568 (US).

(74) Agents: **ENG, U., P., Peter** et al.; Wilson Sonsini Goodrich & Rosati, 650 Page Mill Road, Palo Alto, CA 94304-1050 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US (patent), UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 2007/001394 A2

(54) Title: METHOD AND SYSTEM FOR IDENTIFYING USERS AND DETECTING FRAUD BY USE OF THE INTERNET

(57) Abstract: A method and system for detecting and preventing Internet fraud in online transactions by utilizing and analyzing a number of parameters to uniquely identify a computer user and potential fraudulent transaction through predictive modeling. The method and system uses a delta of time between the clock of the computer used by the actual fraudulent use and the potentially fraudulent user and the clock of the server computer in conjunction with personal information and/or non-personal information, preferably the Browser ID.

METHOD AND SYSTEM FOR IDENTIFYING USERS AND DETECTING FRAUD BY USE OF THE INTERNET

CROSS-REFERENCE

[0001] This application is a continuation-in-part application of U.S. Patent Application Serial No. 10/791,439 filed on March 2, 2004, and this application also claims the benefit of priority to U.S. Provisional Patent Application Serial No. 60/694,768 filed June 27, 2005, which are incorporated herein by reference in their entirety.

BACKGROUND OF THE INVENTION

[0002] The invention relates to Internet purchasing or e-tail transactions and specifically to detecting fraud in such transactions when ordering products, services, or downloading information over the Internet.

[0003] There is a continuing need to develop techniques, devices, and programs to detect and prevent Internet fraud. The invention provides a method and a system for detecting and preventing Internet fraud by utilizing and analyzing a number of parameters to uniquely identify a customer and a potential fraudulent Internet-based transaction.

DESCRIPTION OF THE PRIOR ART

[0004] Many methods and systems have been developed over the years to prevent or detect Internet fraud. Today, to gain consumer confidence and prevent revenue loss, a website operator or merchant desires an accurate and trustworthy way of detecting possible Internet fraud. Merely asking for the user name, address, phone number, and e-mail address will not suffice to detect and determine a probable fraudulent transaction because such information can be altered, manipulated, fraudulently obtained, or simply false.

[0005] Typically, an Internet user who accesses a website for obtaining a service, product, or information, not only enters personal information as mentioned above, but is also requested to provide a credit card account number, expiration date, and billing address. An online criminal seeking to obtain goods, services, or access to information (text and/or visuals over the Internet) commonly uses someone else's credit card information to obtain the services or products during the transaction. To prevent such occurrences, websites, via credit card companies and banks, often check to see if the address on the order corresponds or matches the address for the credit card owner. Although billing and shipping addresses can differ, such as when someone purchases a gift for another, it is a factor to consider in the verification process. Additionally, merchants utilize phone number matching between that of the Internet order and the credit card company database. Another commonly used technique for order verification is e-mail address verification where the website operator sends a message to the user e-mail address asking the customer to confirm the order prior to executing the same. Yet, online thieves frequently use e mail addresses from large portal sites that offer free e-mail accounts. These e-mail addresses are easily disposable and make it harder for the website operator to identify the fraudulent customer before executing the transaction.

[0006] More sophisticated websites now capture a variety of parameters from the user known as Common Gateway Interface parameters (CGI parameters). These parameters commonly include non-personal information such as a user Internet Protocol Address (IP Address). Every computer connected to the Internet is assigned a unique number known as its Internet Protocol (IP) Address. Much like a phone number in a home or office, an IP address can be used to identify the specific user or at least the particular computer used for an Internet transaction. In addition, since these numbers are usually assigned in country-based blocks, an IP address can often be used to identify the country from which a computer is connected to the Internet. Yet, IP addresses can change regularly if a

user connects to the Internet via a dial-up connection or reboots their computer. Online thieves also have ways of scrambling their IP addresses or adopting another IP address to make it nearly impossible for the website operator to identify the true user. Thus, websites typically use an IP address plus a further non-personal identifier such as a Browser ID (or user agent), a cookie, and/or a registration ID to try to identify a unique user and to prevent fraud in a second transaction.

[0007] A Browser ID provides the website operator with a wealth of information about the user such as the software being used to browse or surf the Internet. Additionally, the Browser ID includes information about the user computer operating system, its current version, its Internet browser and the language. Thus, the Browser ID has valuable information for identifying a unique user. The Browser ID may also have more detailed information such as the type of content the user can receive; for example, this lets the website operator know if the user can run applications in FLASH-animation, open a PDF-file, or access a Microsoft Excel document. Yet, Browser IDs from different computers can be similar, as there are so many Internet users and thus many have similar computers with the same capabilities, programs, web browsers, operating systems, and other information. A cookie refers to a piece of information sent from the web server to the user web browser which is saved on the resident browser software. Cookies might contain specific information such as login or registration information, online 'shopping cart' information, user preferences, etc. But cookies can easily be deleted by the computer user, by the browser, or turned off completely so that the server cannot save information on the browser software. Thus, cookies alone cannot serve as a unique identifier to thwart an Internet thief.

[0008] Accordingly, what is needed is a method and system that overcomes the problems associated with a typical verification and fraud prevention system for Internet transactions particularly in the purchasing of services, products, or information by uniquely identifying each consumer. Then, when that consumer seeks a second fraudulent purchase, the website operator will detect the same and block the order or, at least, obtain more information to ensure the order is legitimate. The system should be easily implemented within the existing environment and should be adaptable and compatible with existing technology.

SUMMARY OF THE INVENTION

[0009] In accordance with the invention, a method and system is provided for detecting potentially fraudulent transactions over the Internet. The method and system comprises obtaining information relating to the transaction from the consumer and combining this information with a unit corresponding to the change of time, a delta of time parameter, to create a unique computer identifier. If a future transaction involves an identical computer identifier, as described below, which was previously engaged in a fraudulent transaction, the website operator can choose to cancel the transaction, pursue legal action, seek further verification, or the like. By using information relating to the first transaction, such as the IP address and/or Browser ID, and combining it with the delta of time parameter, as detailed herein, the website host can more accurately preventively track fraudulent users online by comparing computer identifiers to each other. In so doing, an integrated fraud prevention system is provided which allows the website host, merchant, or the like, to accurately and efficiently determine the validity or fraudulent quality of a transaction sought to be transacted over the Internet.

[0010] Accordingly, the invention provides a method and system for improving fraud detection in connection with Internet transactions. Various embodiments of the invention utilize existing technological capabilities to prevent online thieves from making second fraudulent transactions.

[0011] Another aspect of the invention provides methods and systems for detecting and preventing Internet fraud committed as a result of "scams" or deceptive practices developed to acquire personal, confidential and/or financial

information. The concepts of the invention described above may be characterized as "fingerprinting" techniques and methods to identify and/or prevent fraud involving information obtained through Internet scams. These unlawful practices will likely continue as new techniques are developed in addition to schemes already known to those in field today such as phishing, pharming, spoofing, session cloning and other deceptive practices. It shall be understood that the clock based or delta of time parameters provided herein can be used within the scope of the invention either alone or together with other known or future developed fraud parameters in the fight against online fraud and Internet scams. The various methods and systems provided in accordance with the invention offer improved and enhanced fraud detection and/or prevention solutions for e-commerce and Internet based transactions. These solutions provide a degree of invisibility to users and fraudsters alike and do not require any or all of the following: user interaction (less likelihood for mistakes or carelessness), opt-in (no adoption issues and full coverage of anti-fraud measures can be provided), change in customer behavior (no confusion as to what actions need be taken or avoided), downloads or cookies (no compatibility issues with user computers or browsers). Moreover, these Internet based solutions generate low false-positives and false negatives so as to minimize loss of business for mistakenly turning down legitimate transactions and successfully rejecting transactions that are fraudulent. The invention can incorporate a type of link analysis on user information from compromised accounts to identify a fraudster and/or the computer used to conduct fraudulent transactions online.

[0012] The features and advantages to various aspects of the invention are readily apparent from the following detailed description of the best mode for carrying out the invention when taken in connection with the accompanying chart and other portions of the specification and figures herein.

INCORPORATION BY REFERENCE

[0013] All publications and patent applications mentioned in this specification are herein incorporated by reference to the same extent as if each individual publication or patent application was specifically and individually indicated to be incorporated by reference.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] FIG. 1 is a chart that illustrates the versatility and accuracy of the invention in weeding out possible fraudulent online transactions.

[0015] FIG. 2 describes a connection between a customer computer and a merchant website server whereby each device maintains respective times according to a resident clock.

[0016] FIG. 3 is an index of different Time Zones around the world.

[0017] FIG. 4 is a flowchart describing an embodiment of the invention that provides a customer computer identifier.

[0018] FIG. 5 describes components of a customer computer identifier provided in accordance with the invention.

[0019] FIG. 6 illustrates a comparison of computer identifiers that provides a matching parameter for consideration by an online merchant.

[0020] FIG. 7 shows various components and parameters that may comprise a user computer identifier in accordance with an embodiment of the invention.

[0021] FIG. 8 depicts the comparison between multiple computer identifiers to provide a matching parameter that can be compared against a preselected matching value.

DETAILED DESCRIPTION OF THE INVENTION

[0022] The present invention relates to a method and system for detecting potentially fraudulent transactions over the Internet. Various modifications to the preferred embodiment will be readily apparent to those skilled in the art and the general principles herein may be applied to other embodiments. The present invention is not intended to be limited to the embodiment shown but is to be accorded the widest scope consistent with the principles and features described herein. It is to be understood that the website, its host, or operator does not have to be a merchant of goods.

[0023] The present invention provides a fraud prevention system for online transactions by uniquely identifying a customer based on a number of parameters at least one of which is a delta of time parameter and another of which is another Internet related parameter, preferably the Browser ID of a computer.

[0024] Referring to the chart shown in FIG. 1, what is shown is a series of typical transactions on the Internet between a merchant and several customers. Each customer establishes a connection between his computer and the merchant's website. Upon making this connection, the merchant's website receives some non-personal identification information from the customer. This non-personal information typically includes Common Gateway Interface (CGI) parameters such as the customer's Internet Protocol (IP) Address and the computer's Browser ID. While "hackers" can change, disguise, and/or emulate the IP address to mask a fraudulent transaction, most do not now have the capability nor the idea to do the same for the Browser ID. While some "hackers" can change the Browser ID, it is not a trivial tool and if one needs to change it all the time it is not allowing those thieves to easily steal, hence, they are likely to go to a site that does not check Browser IDs. In a typical embodiment, when the customer decides to purchase services, goods, or information from the website, the customer must input additional and more personal information. This personal identification information may commonly include the customer's name, address, billing and shipping information, phone number, and/or e-mail address. A key feature of the present invention is that the website server also captures the local time of the customer's computer, typically through a program such as Javascript, as well as the local time of the server's computer. The server then calculates the time difference (or delta of time) between the customer's computer clock and the server's computer clock. This can be recorded in any desired format such as hours, minutes, seconds, or the like, but corresponds to a delta of time parameter. The delta of time parameter, the non-personal information, including but not limited to the preferred usage of the Browser ID, and/or the personal information are stored by the merchant and used to uniquely identify the customer.

[0025] As shown in FIG. 2, a connection may be established between a customer computer 12 and a merchant website server 14. Upon making the online connection, various information is transmitted by the customer computer 12 that may operate as a unique user and/or computer identifier. This information may include personal information specific to the customer, non-personal information corresponding to the customer computer, and the local time according to the customer computer. The merchant website can receive non-personal customer information including CGI parameters such as the customers IP address and computer Browser ID. The customer can further input personal information when making a purchase from the website including a customer name, address, billing and shipping information, phone number, and/or e-mail address(es). In accordance with this embodiment of the invention, the relative customer computer local time according to its resident clock may be captured, typically through a program such as Javascript or any other time indicator employed by telecommunications and networking systems such as timestamps within transmitted data packets (e.g., TCP timestamps in packets within a data stream wherein each packet includes a header portion containing a 32-bit

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.