US 20060010072A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2006/0010072 A1**

Eisen (43) **Pub. Date: Jan. 12, 2006**

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

(76) Inventor: **Ori Eisen**, Scottsdale, AZ (US)

Correspondence Address:
U.P. PETER ENG
WILSON SONSINI GOODRICH AND ROSATI
650 PAGE MILL ROAD
PALO ALTO, CA 94304 (US)

(21) Appl. No.: **10/791,439**

(22) Filed: **Mar. 2, 2004**

Publication Classification

(51) **Int. Cl.**
G06Q 40/00 (2006.01)

(52) **U.S. Cl.** **705/44**

(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

FIELD OF THE INVENTION

[0001] 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.

[0002] There is a continuing need to develop techniques, devices, and programs to detect and prevent Internet fraud. The present 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

[0003] 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's 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.

[0004] 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's database. Another commonly used technique for order verification is e-mail address verification where the website operator sends a message to the user's 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.

[0005] 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's 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's 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.

[0006] 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's 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's 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's user, by the browser, or "turned off" completely so that the server cannot save information on the browser's software. Thus, cookies alone cannot serve as a unique identifier to thwart an Internet thief.

[0007] 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

[0008] In accordance with the present 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.

[0009] Accordingly, it is an object of the invention to provide a method and system for improving fraud detection in connection with Internet transactions.

[0010] It is another object of the invention to utilize existing technological capabilities to prevent online thieves from making second fraudulent transactions.

[0011] The above object and other objects, features, and advantages of the present 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.

BRIEF DESCRIPTION OF THE CHART

[0012] The chart illustrates the versatility and accuracy of the present invention in weeding out possible fraudulent online transactions.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT AND THE CHART

[0013] 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.

[0014] 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 preferably the Browser ID of the computer. Referring to the chart, 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.

[0015] Because computer users rarely personally change the internal clocks within their computers, the delta of time parameter will likely be the same (or within a range) for a computer every time that computer is used to conduct an online transaction with the same merchant even if the user disguises or changes the IP address. The Browser ID is also not likely to be changed, even by a consumer seeking to perpetuate a fraudulent transaction. Thus, the delta of time parameter (the difference between the time of day of the computer user's clock and the time of day on the website's server clock) is an important component of the computer identifier because it, along with the preferred Browser ID or other personal or non-personal information, is a good indication of the identity of a subsequent user on the same computer. The delta of time parameter also allows the merchant to potentially locate the computer in terms of a time zone, region, or country.

[0016] Once a merchant determines that a first fraudulent transaction may have been made, the merchant can flag the customer's computer identifier, i.e. Browser ID and delta of time. In a preferred embodiment, the computer identifier will include at least its delta of time and Browser ID, but may also include other personal and/or non-personal information. Then, the matching parameter can be used to identify a subsequent transaction which reveals a user with an identical set of computer identifiers. The matching is typically implemented by software, for example, on a hard disk, floppy disk, or other computer-readable medium. After the comparison has been made, the software assigns a matching value to the pair of transactions based on the similarities between the first and subsequent transaction. The website server may inform the merchant of the matching value, cancel the transaction, inform the costumer of the status of their order, demand more information, or the like. The merchant may then choose its desired course of action.

[0017] A particularly important feature of the present invention is the merchant's ability to include, remove, and weigh each parameter within the computer identifier. For example, the merchant may choose to only use the delta of time parameter and Browser ID to form the unique computer identifier. Accordingly, the merchant may set the matching parameter to fit a level of comparison between the first and subsequent transaction. For example, since deltas of time may slightly change because of the differences in accuracy between the server and the user's computer clock mechanism, computer clocks and deltas may slightly vary over time. The merchant may set the matching parameter to

include a range of delta of time, such as a few minutes, instead of an exact match. This way, even if the user's computer "loses time," the matching parameter will still identify the subsequent transaction as a potential fraudulent one based on other information within the computer identifier.

[0018] Although the present invention has been described in accordance with the embodiments shown, one of ordinary skill in the art will recognize that there could be variations to the embodiment and those variations would be within the spirit and scope of the present invention. Therefore, although the present invention was described in terms of a particular fraud prevention method and system, one of ordinary skill in the art readily recognizes, that any number or parameters can be utilized and their use would be within the spirit and scope of the present invention.

1. A method for creating a computer identifier for an online customer for detecting a possible fraudulent transaction in the course of an online transaction comprising the steps of:

receiving, from said customer's computer, at least one personal or non-personal identification parameter;

capturing, from the clock of said customer's computer, said customer's computer local time;

capturing, from a website's server clock, said server's local time;

creating and storing a delta of time parameter based upon the difference between said customer's computer local time and said server's local time; and

uniquely identifying said customer with said delta of time parameter and said at least one personal or non-personal identification parameter.

2. The method of claim 1 further including the step of receiving, from said customer, an additional identification parameter comprising personal identification information relating to said transaction.

3. The method of claim 1 wherein said at least one non-personal identification parameter is said computer's IP address.

4. The method of claim 1 wherein said at least one non-personal identification parameter is said computer's Browser ID.

5. The method of claim 1 wherein said delta of time parameter is stored as a range of time.

6. A method for detecting fraud in an online transaction by a customer comprising the steps of:

creating a first computer identifier in the course of an online transaction comprising the steps of claim 1;

creating at least a second computer identifier in the course of a second proposed online transaction comprising the steps of claim 1;

utilizing a matching parameter to compare said first computer identifier with said second computer identifier;

creating a matching value based on the similarities between said first computer identifier and said second computer identifier; and

classifying said second online transaction as fraudulent, not fraudulent, or requiring further consideration based upon the value of said matching parameter.

7. The method in claim 6, further comprising:

communicating to the website operator an indication, as to whether said second online transaction is fraudulent, not fraudulent, or requires further consideration.

8. The method in claim 6, further comprising:

blocking said second online transaction based upon the value of said matching parameter.

9. The method in claim 6, further comprising:

communicating to said customer the status of said second online transaction based upon the value of said matching parameter.

10. The method in claim 6, wherein said delta of time parameter is stated as a range of time.

11. The method of claim 6 wherein said personal or non-personal identification parameter is a Browser ID.

12. A computer readable medium containing program instructions for creating a computer identifier in the course of an online transaction comprising the steps of:

receiving, from an online customer's computer, at least one of either a personal or non-personal identification parameter;

capturing, from the clock of said customer's computer, said computer's local time;

capturing, from the clock of said website's server computer, said server computer's local time;

creating and storing a delta of time parameter based upon the difference between said customer's computer's local time and said server computer's local time; and

uniquely identifying said customer with customer identification customer identification data comprising said delta of time parameter and said at least one of either of said personal or non-personal identification parameter.

13. The computer readable medium of claim 12 further including the step of:

receiving and storing, from said customer, personal identification information relating to said transaction.

14. The computer readable medium of claim 12 further including the step of:

communicating to the website operator an indication as to whether a second online transaction may be fraudulent because of the similarity existing between the stored customer identification data and the new customer's identification data.

15. The computer readable medium of claim 14 further including the step of:

blocking said second online transaction based upon said indication as to whether a second online transaction may be fraudulent.

16. The computer readable medium of claim 14 further including the step of:

communicating to said customer the status of said second online transaction based upon the similarity of said stored customer identification data and the new customer's identification data.

17. A computer readable medium as claims in claim 11 wherein said non-personal computer identification parameter is a Browser ID.

18. A computer readable medium containing program instructions for detecting likelihood of fraud in an online transaction comprising the steps of:

creating a first computer identifier in the course of an online transaction comprising the steps of claim 1;

creating at least one additional computer identifier in the course of an additional online transaction comprising the steps of claim 1;

utilizing a matching routine to compare said first computer identifier with said at least one additional computer identifier; and

deciding as to whether the online transaction is fraudulent, not fraudulent or requires further consideration

based on the similarities between said first computer identifier and said at least one additional computer identifier.

* * * * *