METHOD OF USING PERSONAL DEVICE WITH INTERNAL BIOMETRIC IN CONDUCTING TRANSACTIONS OVER A NETWORK

BACKGROUND OF THE INVENTION

1. Field Of The Invention

The present invention relates to a method and system for authorizing a transaction between two parties over a network and, more particularly, to authorizing a transaction over the network when an authorization code has been received by an authorizing entity, the authorization code being produced by a fingerprint identification device in response to comparing a fingerprint of one of the parties to a stored fingerprint in the device.

2. Related Art

As the use of networks, for example the Internet, become more prevalent, an ever expanding quantum of electronic commerce will be conducted between users over these networks. Typically, a consumer of goods and/or services electronically connects to a provider of goods and/or services over a network, for example, by way of a website. Using known website browser software, the consumer may review and select goods or services and request that such goods or services be delivered to a specified address.

The provider of goods or services, of course, expects to be paid for any goods or services requested by the consumer. Typically, this is accomplished by asking the consumer to enter his or her credit card number and expiration date. Sometime thereafter, and most likely after the consumer has disconnected from the provider's website, the provider telephones an authorizing entity (e.g., the originator or managing entity) of the credit card and requests authorization to complete the transaction. In particular, the provider of goods and/or services transmits the credit card number, expiration date, consumer name, and purchase amount to the authorizing entity and awaits authorization. The authorizing entity accesses the consumer's credit card account and verifies that the consumer is in good standing and that the purchase amount will not cause the consumer's credit balance to exceed his or her credit limit. If the authorizing entity's review of the consumer's credit account is favorable, then authorization is transmitted to the provider of goods and/or services to complete the transaction with the consumer.

As the provider of goods and/or services never actually sees the consumer and cannot assess the consumer in terms of whether or not the consumer is attempting to fraudulently utilize the credit card, both the provider of goods and/or services and the

authorizing entity (originator of the credit card) must assume that the consumer is the authorized user of the credit card. It is only when the authorized user of a lost or stolen credit card calls the authorizing entity (or its representative) to report the lost and/or stolen card, that fraudulent uses of the credit card may be avoided.

Similar problems occur when goods and/or services are requested and confirmed by a user of the network simply by connecting with the provider's website. For example, when a provider of goods and/or services requires an initial registration with a particular consumer that authorizes billing the consumer for use of the website, accidental (or fraudulent) use of the website is likely by non-authorized users. More particularly, a parent (authorized user) may contract with a provider of goods and/or services to permit the authorized consumer to utilize the website. The terms of the contract (or registration) may be that the consumer's credit card will be charged for an amount representing use of the website by the authorized consumer (e.g., obtaining information from the website or purchasing goods). Unfortunately, the only way that the provider of goods and/or services knows that a user of the website is an authorized consumer is by way of an identification number (e.g., password etc.) given by the authorized consumer or automatically transmitted by the

authorized consumer's personal computer. Thus, any user of the authorized consumer's personal computer who obtains the password (if employed) may access the website and incur charges without the knowledge of the authorized consumer.

Accordingly, there is a need in the art for a new method and system for facilitating and authorizing transactions between parties over a network which provides all parties to the transaction with confidence that the initiator of the transaction is authorized to enter into the transaction.

SUMMARY OF THE INVENTION

In order to overcome the disadvantages of the prior art, the present invention provides a method of conducting a commercial transaction between a customer and a provider of goods or services over a network. The method includes the steps of:

providing the customer with a fingerprint identification device which produces an authentication code when a fingerprint of the customer matches a stored fingerprint within the fingerprint identification device;

maintaining an electronic site on the network over which the customer may request goods or services from the provider of goods or services;

requesting that the customer provide authentication by activating the fingerprint identification device;

receiving at least the authentication code and a account number of the customer at the provider of goods or services over the network from the fingerprint identification device;

transmitting the authentication code and the account number from the provider of goods or services to a managing entity of the account over the network in encrypted form, and requesting authorization to complete the transaction; and

completing the transaction if the managing entity of the account provides the authorization.

Preferably, the stored fingerprint is in an encrypted format and at least one of the authentication code and account number are received over the network in an encrypted form.

The method of the present invention also contemplates permitting the customer to access the account. The steps according to this aspect of the invention include: establishing an electronic connection over the network between the customer and a managing entity of the account; requesting that the user provide authentication to the managing entity of the account by activating the fingerprint identification device; receiving at least the

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.