PTO/SB/16 (11-95)
Approved for use through 01/31/98. OMB 0651-0037
Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c).

Docket Number	032376-003.2	Type a plus sign (+) inside this box →

INVENTOR(s)/APPLICANT(s)

LAST NAME	FIRST NAME	MIDDLE INITIAL	RESIDENCE (CITY AND EITHER STATE OR FOREIGN COUNTRY)
LITCROFT	Daniel	I.	Dublin, Ireland
O'CONNELL	Graham		Dublin, Ireland

TITLE OF THE INVENTION (280 characters max)

CREDIT CARD SYSTEM AND METHOD

CORRESPONDENCE ADDRESS

Ronald L. Grudziecki
BURNS, DOANE, SWECKER & MATHIS, L.L.P.
P.O. Box 1404
Alexandria,

STATE	Virginia	ZIP CODE	22313-1404	COUNTRY	United States of America

ENCLOSED APPLICATION PARTS *(check all that apply)*

- [X] Specification — *Number of Pages* 48
- [X] Drawing(s) — *Number of Sheets* 4
- [ ] Small Entity Statement
- [ ] Other (specify)

METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT *(check one)*

[X] A check or money order is enclosed to cover the Provisional filing fees	PROVISIONAL FILING FEE AMOUNT(S)	$ [ ] $75.00
[X] The Commissioner is hereby authorized to charge any deficiency in filing fees or credit any overpayment to Deposit Account Number 02-4800. This paper is submitted in triplicate.		$ [X] $150.00

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

- [X] No.
- [ ] Yes, the name of the U.S. Government agency and the Government contract number are:

Respectfully submitted,

SIGNATURE David M. Hunsaker (Reg. No. 40,309) Date September 9, 1998

TYPED or PRINTED NAME Charles F. Wieland III for Registration No. 33,096 *(if appropriate)*

- [ ] Additional inventors are being named on separately numbered sheets attached hereto

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

CREDIT CARD SYSTEM AND METHOD

This application claims the benefit of U.S. Provisional Application No. 60/_____ (our reference number 032376-003) filed August 26, 1998, U.S. Provisional Application No. 60/092,500 (our reference number 032376-003) filed on July 13, 1998, the entire contents of which are incorporated by reference herein. This Application also claims the benefit of Irish Patent Application Nos. S98 0223, filed March 25, 1998, S98 0346, filed May 7, 1998, and S98 0458, filed June 15, 1998, the entire contents of each of which are incorporated by reference herein.

BACKGROUND

1. Field of the Invention

This invention relates to a credit card system and method, and more particularly, to a credit card system and method offering reduced potential of credit card number misuse.

2. Related Art

The development of retail electronic commerce has been relatively slow in spite of the perceived demand for such trade. The single greatest deterrent to the expansion of retail electronic commerce is the potential for fraud. This potential for fraud has been a major concern for the credit card companies and financial institutions as well as the customers and the providers of the goods and services.

The former are concerned about fraud because essentially the financial institutions have to bear the cost of the fraud. Additionally, the credit card companies have an efficient credit card system which is working well for face to face transactions, i.e., "card present" transactions where the credit card is physically presented to a trader and the trader can obtain the credit card number, compare signatures and in many cases photographs before accepting a particular credit card.

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

The latter are equally concerned about fraud being well aware that ultimately the user must pay for the fraud. However, there are particular personal concerns for the consumer in that the fraudulent use of the credit card by misuse of the credit card number by a third party may not become apparent for some time. This can happen even if the card is still in his or her possession. Further, when fraud does occur the consumer has the task of persuading the credit card provider that fraud by another did indeed occur.

There is also the additional fear of being overcharged on a credit card. There are thus particular risks for those credit card holders who have relatively high spending limits, in that if fraud should occur, it may be some considerable time before it is detected. One particular form of fraud referred to as "skimming" is particularly difficult to control. What happens is that the card holder proffers his or her card at an establishment to make a transaction, the relevant information is electronically and/or physically copied from the card and the card is subsequently reproduced. This can be a particular problem with travelers particularly during an extensive period of travel as the fraudulent card may turn up in other places and it may be some considerable time before the fraud is detected.

For remote credit card use, the credit card holder has to provide details of name, master credit card number, expiration date and address and often many other pieces of information for verification; the storing and updating of the information is expensive but necessary. This of itself is a considerable security risk as anybody will appreciate that this information could be used to fraudulently charge goods and services to the card holder's credit card account. Such fraudulent use is not limited to those people to whom the credit card information has been given legitimately, but extends to anybody who can illegitimately obtain such details. A major problem in relation to this form of fraud is that the credit card may still be in the possession of the legitimate holder as these fraudulent transactions are taking place. This is often referred to as "compromised numbers" fraud. Indeed all this fraud needs is one

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

dishonest staff member, for example in a shop, hotel or restaurant, to record the credit card number. It is thus not the same as card theft.

The current approaches to the limiting of credit card fraud are dependent on the theft of a card being reported and elaborate verification systems whereby altered patterns of use initiate some enquiry from the credit card company. Many users of credit cards have no doubt received telephone calls, when their use of the card has been exceptional, or otherwise unusual in the eyes of the organization providing the verification services.

Thus, there have been many developments in an effort to overcome this fundamental problem of fraud, both in the general area of fraud for ordinary use of credit cards and for the particular problems associated with such remote use.

One of the developments has been the provision of smart cards which are credit card devices containing embedded electronic circuitry that can either store information or perform computations. Generally speaking they contribute to credit card security systems by using some encryption system. A typical example of such a smart card is disclosed in U.S. Patent No. 5,317,636 (Vizcaino).

Another method used is the Secure Electronic Transaction (SET) protocol which represents the collaboration between many leading computer companies and the credit card industry which is particularly related to electronic transmission of credit card details and in particular via the Internet. It provides a detailed protocol for encryption of credit card details and verification of participants in an electronic transaction.

There are then specific electronic transaction systems such as "Cyber Cash," "Check Free" and "First Virtual." Unfortunately, there are serious problems with what has been proposed to date. Firstly, any form of reliance on encryption is a challenge to those who will then try to break it. The manner in which access has been gained to extremely sensitive information in Government premises, would make even the most foolhardy wary of any reliance on an encryption system. Secondly, a further

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

problem is that some of the most secure forms of encryption system are not widely available due to government and other security requirements. Limiting the electronic trading systems and security systems for use to the Internet is of relatively little use. While electronic commerce is perceived to be an area of high risk, in practice to date it is not.

Japanese Patent Publication No. Hei 6-282556 discloses a one time credit card settlement system. This system employs a credit card which can be used only once in which various information such as specific personal information, use conditions, and an approved credit limit identical to those of the original credit card are recorded on a data recording element and displayed on the face of the card. The one-time credit card contains the same member number, expiration date, card company code, and the like as on existing credit card, as well as one-time credit card expiration date not exceeding the expiration date of credit card, available credit limit, and the like. The one-time credit card makes use of the same settlement means as the conventional credit card. However, the system also requires use permission information to be recorded on the credit card, the information permitting the credit card to be used only once or making it impossible to use the credit card when the credit limit has been exceeded. A special card terminal device checks the information taken from the card for correctness and imparts use permission information for when the card is not permitted to be used on the transmission to the credit card issuing company. The use permission information takes the form of a punched hole on the card itself. This system has obvious flaws, such as the card terminal having to be modified for additional functions (e.g., punching holes, detected punched holes, imparting additional information, etc.). Also, such a system offers little additional security insofar as fraud can still be practiced by covering the holes or otherwise replacing the permission use information on the credit card. Such a system would require a change in nearly all card terminal equipment if it were adopted.

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

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.