A/PROV

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	Type a plus sign (+) inside this box →	+

jc541 U.S. PTO 60/092500 07/13/98

jc408 U.S. PTO 07/13/98

INVENTOR(s)/APPLICANT(s)

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

TITLE OF THE INVENTION (280 characters max)

A CREDIT CARD SYSTEM

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* 28
- [ ] Drawing(s) — *Number of Sheets* _____
- [ ] Small Entity Statement
- [X] Other (specify) Claims 1-63, 14 pages; Abstract, 1 page

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 Ronald L. Grudziecki Date July 13, 1998

TYPED or PRINTED NAME Ronald L. Grudziecki Registration No. 24,970 *(if appropriate)*

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

(10/97)

"A Credit Card System"

BACKGROUND OF THE INVENTION

Field of the Invention

This invention relates to a credit card system and in particular to the security of credit cards and more particularly to remote credit card use that is to say where the credit card is not necessarily physically used in the transaction. The present invention however is not limited to such remote credit card use. Generally such credit card systems comprise:

at least one master credit card for a customer account;

a master credit card number allocated to the master credit card; and

payment clearance means for a proposed transaction by reference primarily to the master credit card number and often to other additional information.

In this specification the term "master credit card number" and "master credit card" refer to the credit card number and the credit card as generally understood namely that which is allocated by the credit card provider to the customer for his or her account. It will be appreciated that an account may have many master credit cards in the sense of this specification. For example a corporation may provide many of its employees with credit cards but essentially each of these employees holds a master credit card even if there is only one customer accounts. Each of these master credit cards will have a unique master credit card number which set of master credit card numbers will

be linked to the account. Similarly in families, various members of the family may hold a master credit card all of which are paid for out of the one customer account.

Background Information

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

The latter are equally concerned about fraud, being well aware that ultimately the user must pay for the service. However, there are particular personal concerns for the consumer in that the fraudulent use of the credit card by misuse of the master 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 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 travellers 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, expiry 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, anybody who can illegitimately obtain such details can conduct such fraud. 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 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.

Many solutions have been proposed to this problem, however, none of them allow the use of existing credit cards. Ideally the solution would be to obtain the functionality of a credit card, while never in fact revealing the master credit card number. Unfortunately, the only way to ensure that master credit card numbers cannot be used fraudulently is to never transmit the master credit card number by any direct route i.e. phone, mail, Internet or even to print out the master credit card number during the transaction such as is commonly the case at present. It is thus impossible.

The current approaches to the limiting of credit card fraud are dependent firstly on the theft of a card being reported and secondly elaborate verification systems whereby altered patterns of use initiate some enquiry from the credit card company. All 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 organisation providing the verification services.

Thus, there have been many developments in an effort to overcome this fundamental problem of fraud, firstly in the general area of fraud for ordinary use of credit cards and then 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

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.