

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
PATENT TRIAL & APPEAL BOARD**

In re Patent of: John D'Agostino
U.S. Patent No.: 8,036,988
Issue Date: October 11, 2011
Application No.: 12/902,399
Filing Date: October 23, 2010
Title: System and Method for Performing Secure Credit Card Transactions

DECLARATION OF DR. JACK D. GRIMES, Ph.D.

I, Jack D. Grimes, Ph.D., declare as follows:

(1) I have written this Declaration at the request of MasterCard International Incorporated ("MasterCard"). In forming my opinions, I rely on my knowledge and experience in the field and on documents and information referenced in this Declaration.

(2) I reside at 5025 Wine Cellar Drive, Sparks, NV. I am an independent consultant. I have prepared this Declaration for consideration by the Patent Trial and Appeal Board. I am over eighteen years of age and I would otherwise be competent to testify as to the matters set forth herein if I am called upon to do so.

I. BACKGROUND AND QUALIFICATIONS

(3) I earned B.S. and M.S. degrees in Electrical Engineering, and a Ph.D. degree in Electrical Engineering (with a minor in Computer Science), all from

Iowa State University. I also earned an M.S. degree in Experimental Psychology from the University of Oregon. I have been active in several professional societies and have worked in the computer and electronics field for over forty (40) years including teaching at two universities. Details of my education and work experience are set forth in my curriculum vitae, which is attached as Appendix A.

(4) From 1996 until 1999, I worked at Visa International (“Visa”) and was Senior Vice President for Technology, Architecture & Strategy. My responsibilities included developing the strategies for Visa in chip card technology, management of large-scale software projects, and the evaluation of investments in technology companies. My duties included management of two technology and strategy groups containing over 30 people. One group provided chip card and related technology development for new products and services, including SET (Secure Electronic Transactions over the Internet). The other group was responsible for the global network and processing architecture strategy to replace the then current VisaNet services, providing credit card authorization and settlement. I also served as an internal consultant on Internet payment systems.

(5) I have reviewed United States Patent No. 8,036,988¹ (“the ’988 patent”) to D’Agostino. I have also reviewed the publications cited within this declaration

¹ John D’Agostino, “System and Method for Performing Secure Credit Card Transactions,” *U.S. Patent No. 8,036,988*, issued October 11, 2011 (Exh. 1001).

and referenced in the covered business method patent review petition submitted herewith.

II. STATE OF THE ART

(6) The technology for performing secure credit card purchases in connection with remote commercial transactions was well known by the year 1999.

Credit Card Fraud

(7) There are many well-known ways that an unauthorized user can obtain your name, credit card number and expiration date. Credit cards have become so widely used that fraud is a major problem and concern for most cardholders.

(8) In attended, point-of-sale (POS) transactions, the cardholder's signature is compared to the signature printed on the credit card. This provides authentication that the person utilizing the credit card is, in fact, the cardholder. In Europe, where chip cards are common, attended transactions typically require the entry of a PIN at the point-of-sale.

(9) However, these solutions do not work for "remote transactions," such as on-line purchases using the Internet or for transactions over the telephone. In this case, the customer's signature cannot be verified and there is no PinPad to provide for the entry of a PIN.

(10) As a result, in remote transactions, the opportunity exists for an unauthorized user to provide a stolen credit card number with accompanying info

to conduct a purchase transaction. For example, for Internet transactions, it is difficult to differentiate between an unauthorized user and the true cardholder based on the credit card information provided for a transaction. The fraudulent transaction can only be identified later (e.g., if the cardholder realizes that a fraudulent transaction has occurred).

(11) To address the problem of credit card fraud, several solutions were proposed, including the technology disclosed by U.S. Patent No. 6,422,462 to Cohen (Exh. 1004, “Cohen”), and by U.S. Patent No. 6,636,833 to Flitcroft et al. (Exh. 1005, “Flitcroft”).

(12) One well-known solution to credit card fraud is creating a limited-use credit card that is restricted to a single use. (*See* Cohen at C2:35-43; Flitcroft at C6:53-56) Each of these single use cards has a unique card number that is different from to the master credit card account number. That way, if the card number and accompanying info is subsequently stolen, that card number cannot be used for a second purchase. After the card is used, it may be discarded.

(13) Another well-known solution to credit card fraud is creating a limited-use credit card with restrictions on its usage, such as limiting the dollar amount, limiting the frequency of use, or limiting the merchant category where the card may be used – such as for airline tickets or for clothing stores, etc. (*See* Cohen at C7:66-8:46; Flitcroft at C8:2-10). These limited use cards also have numbers that

are different from the master credit card account number. That way, the limited-use card number cannot be used for purchases that are inconsistent with the restrictions on its usage.

Repeating Credit Card Transactions

(14) It was well known in the art at the time the patent was filed that you can call your bank and set up a repeating payment account to pay for reoccurring charges, e.g., on a monthly basis for your health club. For example, U.S. Patent No. 5,283,829 to Anderson (Exh. 1011, “Anderson”) discloses that various banking institutions offer their subscribers the option of automatically paying monthly reoccurring charges (such as car notes, insurance premiums, mortgages, etc.) via automatic funds transfer (Anderson at C1:57:63).

(15) It was also well known in the art at the time the patent was filed that these repeating payments could be set-up and charged to a credit card account. For example, U.S. Patent No. 6,064,987 to Walker (Exh. 1010, “Walker”) discloses the use of credit cards for “installment plans” in which a user can set up a repeating transaction with a credit card to make payments at various time intervals, such as once a month. (See Walker at C1:66-2:10; C4:25-32; C4:37-40).

III. LEVEL OF ORDINARY SKILL IN THE ART

(16) The level of ordinary skill in the art of the ’988 Patent is a person having a B.S. degree in Electrical Engineering or Computer Science, or the equivalent

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.