



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	PATENT NUMBER	GROUP ART UNIT	FILE WRAPPER LOCATION
60/572,776			



Correspondence Address/Fee Address Change

The following fields have been set to Customer Number 80048 on 07/16/2008

- Correspondence Address
- Power of Attorney Address

The address of record for Customer Number 80048 is:

80048
Pearl Cohen Zedek Latzer, LLP
1500 Broadway
12th Floor
New York, NY 10036

PART 1 - ATTORNEY/APPLICANT COPY

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

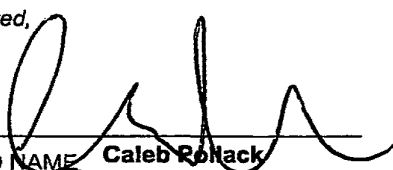
This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c).

INVENTOR(S)					
Given Name (first and middle (if any))		Family Name or Surname		Residence (City and either State or Foreign Country)	
Naftali Lior Nira		BENNETT GOLAN RIVNER		New York, NY Tel Aviv, Israel Ramat Gan, Israel	
<input type="checkbox"/> Additional inventors are being named on the ^ separately numbered sheets attached hereto					
TITLE OF THE INVENTION (280 characters max)					
SYSTEM AND METHOD OF FRAUD REDUCTION					
Direct all correspondence to: CORRESPONDENCE ADDRESS					
<input checked="" type="checkbox"/> Customer Number		27130		Place Customer Number Bar Code Label here	
OR		Type Customer Number here			
<input checked="" type="checkbox"/> Firm or Individual Name		Eitan, Pearl, Latzer & Cohen Zedek, LLP.			
Address		10 Rockefeller Plaza			
Address		Suite 1001			
City		State		ZIP	
New York		New York		10020	
Country		Telephone		Fax	
USA		212-632-3480		212-632-3489	
ENCLOSED APPLICATION PARTS (check all that apply)					
<input checked="" type="checkbox"/> Specification		Number of Pages		19	
<input type="checkbox"/> Drawing(s)		Number of Sheets			
<input type="checkbox"/> Application Data Sheet. See 37 CFR 1.76		<input checked="" type="checkbox"/> Other (specify)		postcard	
METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT (check one)					
<input checked="" type="checkbox"/> Applicant claims small entity status. See 37 CFR 1.27.		<input type="checkbox"/> A check or money order is enclosed to cover the filing fees		FILING FEE AMOUNT (\$)	
<input checked="" type="checkbox"/> The Commissioner is hereby authorized to charge filing fees or credit any overpayment to Deposit Account Number:		05-0649		80	
<input type="checkbox"/> Payment by credit card. Form PTO-2038 is attached.					
The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.					
<input checked="" type="checkbox"/> No.		<input type="checkbox"/> Yes, the name of the U.S. Government agency and the Government contract number are:			

Respectfully submitted,

Date 21 / May / 2004

SIGNATURE



REGISTRATION NO.
(if appropriate)

37,912

TYPED or PRINTED NAME

Caleb Rollack

TELEPHONE

212-632-3480

Docket Number:

P-6864-USP

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

This collection of information is required by 37 CFR 1.51. The information is used by the public to file (and by the PTO to process) a provisional application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 8 hours to complete, including gathering, preparing, and submitting the complete provisional application to the PTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, Washington, D.C. 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Provisional Application, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

UNITED STATES PROVISIONAL PATENT APPLICATION FOR:
SYSTEM AND METHOD OF FRAUD REDUCTION

Embodiments of the present invention relate to a method and system for addressing massive theft (or suspected theft) of identification information used in order to access services that contain confidential information of the users of those services, or services where the user can perform sensitive operations (such identifying information includes but is not limited to user-names and passwords of any form, or any other personal identifying data that can be used in order to access services that contain confidential information. all together referred herein as "Credentials" or "User Credentials").

The system and method described herein can be implemented whenever massive Credentials' theft has occurred, as well as when it is suspected to have occurred, or anytime.

One of the advantages of an embodiment of the invention is that it can be deployed immediately when needed and where needed, and has very low operational and deployment costs, moreover, it does not require prior access (such as pre-enrolment, or pre-distribution of hardware) to users, who are potential victims of such theft.

An embodiment of the invention extends authentication to a two-factor out-of-band form, requiring an additional data element (in addition to the credentials) to be transmitted to the user via a different channel. Such channel could be, but is not limited to a mobile phone or a landline phone, or a pager, or any channel that has the characteristic that it is difficult (either logistically, money-wise, or time-wise) to obtain access to many access points to it (for example it is difficult/expensive to own numerous telephone lines, or mobile numbers to beeper numbers), and in a preferable embodiment of this invention, it is widely available and easy to access by users (on an individual basis).

It should be noted that unlike typical two-factor authentication methods, the additional authentication channel does not have to be previously uniquely linked to a user, and therefore there is no need for prior access to the users (either in the form of registration, distribution of hardware or education of users) prior to deploying the method. Security is achieved by limiting the number of different user service accounts that can use the same authentication channel (for example, if the service is a bank account, such limitation would be achieved by limiting the number of bank accounts that can be linked to a certain telephone number, , or by limiting the number of users who can link their accounts to that telephone number (based on name/ SSN/ whether they are members of the same family), and by deploying as part of the method only those channels that have the characteristic that it is difficult (either logistically, money-wise, or time-wise) to obtain access to many access points to it (for example, it is both expensive and logistically difficult to obtain access to a significant number of land-line telephone numbers).

The deployment of an embodiment of the invention can be governed and set according to criteria intended to specify the level of the threat of fraud. It can also be applied selectively to users according to various criteria intended to assess the probability of fraud (for example, at various levels of fraud users logging into a service from their typical IP location may be exempt from the method, or users who performed a successful out of band authentication, for example from a certain location (such as computer or ATM machine) according to the method would be exempt from the method in their next attempt to access the service from the same location).

In summary this method pertains to a two factor authentications using a communication channel that meets certain criteria. When using this method, users will be authenticated using a combination of their regular Credentials and proof that the User has access to a communication channel that meets the criteria of this method (for example, without limitation, such proof could

be delivered by the user presenting a dynamic piece of data that would be delivered to it via a communication channel that meets the criteria of this method, or by the user showing it knows the content of this dynamic data; or by the user initiating a call from the phone/ channel to a certain phone number). The criteria that the additional communication channel needs to meet under this method, is that it would be difficult and/or cumbersome and/or expensive to obtain a significant number of it (for example, without limitation, it is expensive and cumbersome to obtain numerous telephone/ mobile phone numbers including access to them). Security is achieved not only by selecting such a type of communication channel for delivery of the dynamic password, but also by restricting the number of Users or User accounts (or any other number of distinct values of a property of the user/account, such as owner name, SSN, billing address) that can be linked to a particular channel. This method can be used either with respect to Users who have pre-registered the details of their secondary authentication channel, as well as with respect to users who have not pre-registered. With respect to the latter, such details can be collected during the authentication session, as shall be illustrated in the following sections

This method can more generally be seen as a method for achieving a sufficient level of security in authentication not by actually validating user's identity but rather by (i) requiring users to provide details of "something" that is either expensive, complicated or hard to achieve (Ideally, it should be something that meets the above criteria, but that is readily available (such as a telephone line)); and (ii) by limiting the number of different user service accounts or users who can use the same "something" for authentication

In one embodiment, this method and system would not protect from any single false authentication. It is rather intended to protect from massive use of stolen or fabricated data.

BACKGROUND:

Various service providers use Credentials in order to authenticate users in remote applications. Authentication is required whenever a sensitive operation takes place – viewing personal information, performing financial transactions, updating the user's profile and more.

During authentication the user is usually required to supply a pre-established password and optionally an additional shared secret between the user and the service provider.

Users' credentials enable access to sensitive information as well as funds, and therefore getting hold of them has become a popular criminal activity. Stealing users' credentials can be done in various ways. For example, theft of a file containing credentials from the bank or a third party (including an "inside job"), a large and successful "Phishing" attack, keyboard sniffing and more.

When there is no threat of fraud, a service provider may elect to operate, using Credentials via the regular single communication channel as the only means for authentication. However when faced with a fraud alert using Credentials only may not provide sufficient security.

In general, service providers may face various levels of fraud alert, and act accordingly, implementing their contingency plans which are appropriate to a given level of alert. For ease of exposition the current description shall refer to 3 levels of alert: (i) **no alert** (i.e. business as usual); (ii) suspected fraud – **medium level alert**; (iii) actual (massive) fraud – **high level of alert**. Other numbers and types of alerts may be used.

When faced with a major theft of user credentials, the service provider may execute one or more of the following unsatisfactory options:

- Operate its business at a much higher risk level – checking and analyzing transactions to make sure no fraudulent activity takes place

- Perform a costly operation of changing the user credentials or deploying a new authentication mechanism
- Shut down parts of the business in case the other two options are not acceptable
- Perform other sets of actions.

It should be noted that many times the service provider will not have any external alert as to the occurrence of a massive credential theft. For example – it may not know when a large set of credentials is stolen by an insider job, or from a 3rd party service provider. In addition, even when a large theft is known, like in the case of a large phishing attempt, the service provider may not know when the stolen credentials will actually be used.

Service providers are therefore looking for alternative authentication options. Some of the alternative solutions offered today are:

- Ask for shared secret information that changes over time and is therefore more difficult to obtain (or that loses its value after some time, as it becomes irrelevant) - like details about recent transactions, or invoicing
- Ask for random parts of shared secret information: Like random digits of the password, or random data elements out of a set of known data elements
- Mobile / phone authentication – in which the mobile phone is pre-registered to the service and is used to authenticate the user
- Token based authentication

The current solutions are not satisfactory, since none of them strikes a good balance between security and usability. Either they are not secure enough (like asking for random pieces of a shared secret– information which can easily be obtained during the initial user credentials theft) not usable enough or too expensive to actually deploy (like token authentication – which is expensive to implement, requires customer education, and deployment ahead of time to all users).

To create an efficient and cost-effective solution, one must make sure the solution offered:

1. Provides adequate security
2. Is non-intrusive – can be deployed on demand and not burden all customers all of the time
3. Requires low deployment and operation costs

DETAILED DESCRIPTION OF THE INVENTION

In the description herein, various aspects of the present invention will be described. For purposes of explanation, specific configurations and details are set forth in order to provide a thorough understanding of the present invention. However, it will also be apparent to one skilled in the art that the present invention may be practiced without the specific details presented herein. Furthermore, well-known features may be omitted or simplified in order not to obscure the present invention. Various examples are given throughout this description. These are merely descriptions of specific embodiments of the invention, but the scope of the invention is not limited to the examples given.

Embodiments of the invention may be used so Service Providers that provide services containing confidential information, will be able to continue providing access to such services to their users, even in the face of massive theft, or suspected theft of Credentials of the users of their services. It will be appreciated, however that the present invention is not limited to usage by

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.