PTO/SB/16 (04-04)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
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).

Express Mail Label No.

## INVENTOR(S)

| Given Name (first and middle [if any]) | Family Name or Surname | Residence (City and either State or Foreign Country) |
|---|---|---|
| JOHN ROBERTSON | CAMPBELL | 572 Windermere Avenue, Ottawa, Ontario K2A 2W5 CANADA |

*Additional inventors are being named on the _____ separately numbered sheets attached hereto*

## TITLE OF THE INVENTION (500 characters max)

METHOD AND SYSTEM FOR MANAGING AUTHENTICATION ATTEMPTS

*Direct all correspondence to:* **CORRESPONDENCE ADDRESS**

☑ Customer Number: 33,721

***OR***

| | | | | | |
|---|---|---|---|---|---|
| ☐ Firm or Individual Name | | | | | |
| Address | | | | | |
| Address | | | | | |
| City | | State | | Zip | |
| Country | | Telephone | | Fax | |

## ENCLOSED APPLICATION PARTS *(check all that apply)*

☑ Specification *Number of Pages* 7 ☐ CD(s), Number _____

☑ Drawing(s) *Number of Sheets* 3 ☐ Other (specify) _____

☑ Application Data Sheet. See 37 CFR 1.76

## METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT

☑ Applicant claims small entity status. See 37 CFR 1.27.

☐ A check or money order is enclosed to cover the filing fees.

☐ The Director is hereby authorized to charge filing fees or credit any overpayment to Deposit Account Number: _____

☑ Payment by credit card. Form PTO-2038 is attached.

FILING FEE Amount ($): $80.00

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

☑ No.

☐ Yes, the name of the U.S. Government agency and the Government contract number are: _____



*Respectfully submitted,*

SIGNATURE _____ Date July 7, 2004

TYPED or PRINTED NAME T. Andrew Currier REGISTRATION NO. 45,400 *(if appropriate)*

Docket Number: 33174-2001

TELEPHONE (416) 865-8213

***USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT***

This collection of information is required by 37 CFR 1.51. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an 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 completed application form to the USPTO. 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, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

PTO/SB/17 (10-03)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE


# FEE TRANSMITTAL for FY 2004

*Effective 10/01/2003. Patent fees are subject to annual revision.*

☑ Applicant claims small entity status. See 37 CFR 1.27

**TOTAL AMOUNT OF PAYMENT** ($) 80.00

| *Complete if Known* | |
|---|---|
| Application Number | N/A |
| Filing Date | Filed concurrently herewith |
| First Named Inventor | CAMPBELL, John Robertson |
| Examiner Name | N/A |
| Art Unit | N/A |
| Attorney Docket No. | 33174-2001 |

## METHOD OF PAYMENT *(check all that apply)*

☐ Check ☑ Credit card ☐ Money Order ☐ Other ☐ None

☐ Deposit Account:

Deposit Account Number

Deposit Account Name

**The Director is authorized to:** *(check all that apply)*

☑ Charge fee(s) indicated below ☑ Credit any overpayments

☑ Charge any additional fee(s) or any underpayment of fee(s)

☐ Charge fee(s) indicated below, **except for the filing fee** to the above-identified deposit account.

## FEE CALCULATION

### 1. BASIC FILING FEE

| Large Entity Fee Code | Large Entity Fee ($) | Small Entity Fee Code | Small Entity Fee ($) | Fee Description | Fee Paid |
|---|---|---|---|---|---|
| 1001 | 770 | 2001 | 385 | Utility filing fee | |
| 1002 | 340 | 2002 | 170 | Design filing fee | |
| 1003 | 530 | 2003 | 265 | Plant filing fee | |
| 1004 | 770 | 2004 | 385 | Reissue filing fee | |
| 1005 | 160 | 2005 | 80 | Provisional filing fee | $80.00 |

**SUBTOTAL (1)** ($) 80.00

### 2. EXTRA CLAIM FEES FOR UTILITY AND REISSUE

| | | Extra Claims | | Fee from below | | Fee Paid |
|---|---|---|---|---|---|---|
| Total Claims | | -20** = | | X | = | |
| Independent Claims | | - 3** = | | X | = | |
| Multiple Dependent | | | | | = | |

| Large Entity Fee Code | Large Entity Fee ($) | Small Entity Fee Code | Small Entity Fee ($) | Fee Description |
|---|---|---|---|---|
| 1202 | 18 | 2202 | 9 | Claims in excess of 20 |
| 1201 | 86 | 2201 | 43 | Independent claims in excess of 3 |
| 1203 | 290 | 2203 | 145 | Multiple dependent claim, if not paid |
| 1204 | 86 | 2204 | 43 | ** Reissue independent claims over original patent |
| 1205 | 18 | 2205 | 9 | ** Reissue claims in excess of 20 and over original patent |

**SUBTOTAL (2)** ($) 0.00

**or number previously paid, if greater; For Reissues, see above

## FEE CALCULATION (continued)

### 3. ADDITIONAL FEES

| Large Entity Fee Code | Large Entity Fee ($) | Small Entity Fee Code | Small Entity Fee ($) | Fee Description | Fee Paid |
|---|---|---|---|---|---|
| 1051 | 130 | 2051 | 65 | Surcharge - late filing fee or oath | |
| 1052 | 50 | 2052 | 25 | Surcharge - late provisional filing fee or cover sheet | |
| 1053 | 130 | 1053 | 130 | Non-English specification | |
| 1812 | 2,520 | 1812 | 2,520 | For filing a request for *ex parte* reexamination | |
| 1804 | 920* | 1804 | 920* | Requesting publication of SIR prior to Examiner action | |
| 1805 | 1,840* | 1805 | 1,840* | Requesting publication of SIR after Examiner action | |
| 1251 | 110 | 2251 | 55 | Extension for reply within first month | |
| 1252 | 420 | 2252 | 210 | Extension for reply within second month | |
| 1253 | 950 | 2253 | 475 | Extension for reply within third month | |
| 1254 | 1,480 | 2254 | 740 | Extension for reply within fourth month | |
| 1255 | 2,010 | 2255 | 1,005 | Extension for reply within fifth month | |
| 1401 | 330 | 2401 | 165 | Notice of Appeal | |
| 1402 | 330 | 2402 | 165 | Filing a brief in support of an appeal | |
| 1403 | 290 | 2403 | 145 | Request for oral hearing | |
| 1451 | 1,510 | 1451 | 1,510 | Petition to institute a public use proceeding | |
| 1452 | 110 | 2452 | 55 | Petition to revive - unavoidable | |
| 1453 | 1,330 | 2453 | 665 | Petition to revive - unintentional | |
| 1501 | 1,330 | 2501 | 665 | Utility issue fee (or reissue) | |
| 1502 | 480 | 2502 | 240 | Design issue fee | |
| 1503 | 640 | 2503 | 320 | Plant issue fee | |
| 1460 | 130 | 1460 | 130 | Petitions to the Commissioner | |
| 1807 | 50 | 1807 | 50 | Processing fee under 37 CFR 1.17(q) | |
| 1806 | 180 | 1806 | 180 | Submission of Information Disclosure Stmt | |
| 8021 | 40 | 8021 | 40 | Recording each patent assignment per property (times number of properties) | |
| 1809 | 770 | 2809 | 385 | Filing a submission after final rejection (37 CFR 1.129(a)) | |
| 1810 | 770 | 2810 | 385 | For each additional invention to be examined (37 CFR 1.129(b)) | |
| 1801 | 770 | 2801 | 385 | Request for Continued Examination (RCE) | |
| 1802 | 900 | 1802 | 900 | Request for expedited examination of a design application | |

Other fee (specify) _____

*Reduced by Basic Filing Fee Paid

**SUBTOTAL (3)** ($) 0.00

## SUBMITTED BY

(Complete *(if applicable)*)

| | | | | | |
|---|---|---|---|---|---|
| Name *(Print/Type)* | T. Andrew Currier | Registration No. *(Attorney/Agent)* | 45,400 | Telephone | (416) 865-8213 |
| Signature | | | | Date | July 7, 2004 |

**WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.**

This collection of information is required by 37 CFR 1.17 and 1.27. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on

## Method and System for Managing Authentication Attempts

The purpose of this invention is to take effective action to manage invalid authentication attempts through pattern analysis and the use of a separate communication channel to communicate with Users in real time. Invalid authentication attempts could include fraudulent or abusive situations as well as a lack of User knowledge.

The identification and management of authentication attempts can be improved in a unique way by having a real time communication channel with the end user that is separate from the channel being used for authentication. An example of this is where Internet users are a) identified by their cell phone numbers and may b) access the internet from many different physical locations. The invention allows for authentication issue detection to be extended with superior action compared to prior art, utilizing the separate communication channel to communicate directly with the User. This allows the authenticating authority to take more proactive action on a more automatic basis with the ability to distinguish fraud or abuse attempts from user problems aided by the separate communication channel.

### Brief Description of the Drawings

Preferred embodiments of the present invention will now be described by way of example only with reference to the attached figures herein.

Figure 1 is a system block diagram of a system for managing attempted illegitimate authentication attempts in accordance with another embodiment of the invention.

Figure 2 and 3 are a flow chart of a method for managing attempted illegitimate authentication attempts in accordance with another embodiment of the invention.

### Detailed Description of the Invention

Referring to Figure 1, the system for managing authentication attempts is generally located at 35. The System 35 includes an Authentication Server 25, which, for example, could be a RADIUS server. The System also includes a User Database 40, which could be many different standards and products. The System also includes an Event Database 45 which is used to store information about authentication events such as User ID, location of authentication attempt, time of attempt, if password matched User ID. The Location Database 50 stores information about the geographic coordinates of access locations and the type of access location (e.g. airport). The System also contains an Application 30 which can interface with the databases, the Authentication Server and the Cellular Network 55. The System may be contained in any kind of computer that has suitable processing power, RAM, Disc capacity and communications ports. The computer may run any OS that is compatible with the applications 25, 30, 40, 45, 50.

Users requiring authentication are equipped with internet devices such as a computer, a notebook computer, a PDA or a WLAN enabled cell phone 15. Such devices must be able to support internet communication protocols.

These devices are attempting to access the internet from various locations. The access could be via wireless or wired network. The internet equipment 20 at the location is able to block access to the internet until the device 15 has been authenticated. The Internet equipment communicates with the Authentication Server 25 to pass information about the User to the Authentication Server 25. The Internet equipment will not permit the Device to access the network until it has been advised to do so by the Authentication Server. This often takes the form of an "authentication accept" message.

The Authentication Server interfaces to the User Database 40 to compare the User ID and password offered by the Internet Device 15 with that stored in the User Database 40. The Authentication Server passes information about the authentication attempt to the Application and receives a message back from the application indicating if Authentication can proceed. If the authentication may proceed, the Authentication Server will communicate with the Internet equipment to inform the equipment that access may be permitted. This often takes the form of an "authentication accept" message.

The Application 30 receives information about authentication attempts, referred hereafter as "events", from the Authentication Server 25.

The Application 30 may:

a) Record the event in Even Database (45)
b) Retrieve and analyse information about events when a new even occurs. The Application searches the database and compares the event to criteria. The criteria may include:
    1) Authentication attempt when the same User ID has been used to successfully authenticate an internet access, and said internet access is still active.
    2) Authentication attempt when an attempt using the same User ID occurred from a different location, and the time between the attempts would not allow a legitimate Internet user to travel from the first location to the second. When locations are established, the geographic coordinates (such as UMT coordinates) must be determined. The geographic coordinates are stored in the Location database (50). When an authentication attempt occurs, the Application will search the Location database to determine the geographic location of the current attempt and the geographic location of the most recent successful attempt. The time of most recent successful attempt will be obtained by searching the Event database.
    3) Multiple authentication attempts using a cellular number (irrespective of location of attempts) within a time period, where the number of attempts and the duration of the time period indicate atypical use.
    4) Multiple authentication attempts from a given location (irrespective of cellular number) within a time period, where the number of attempts and the duration of the time period indicate atypical use.

The Application 30 may make use of a separate communications channel, in this case a cellular network 55, to communicate with a legitimate user via a device they possess, in this case a cellular phone 60.

The Application 30 may perform one or more of the following actions depending upon criteria that may be established in the Application.

1) Automatic action to change the password and inform the legitimate user of the new password. The Application 30 would generate a new password and then a) store the new password in the User Database 40 and b) send the new password to the cellular phone via the Cellular Network 55 using SMS or IVR methods, along with a message explaining the reason a new password is being sent.
2) Automatic action to suspend the account and distribution of passwords. The Application 30 would place the User ID on a Block List in the User database. The Block List would over-ride other Authentication server functions to authenticate, create a new account, or create and distribute new password to the cellular phone 60.
3) In the case of 2) above, or otherwise, automatic action to contact the Internet user via their cellular phone and request them to take/not take action, including requesting them to initiate contact with the service provider. Such contact could be via the Cellular Network 55 using SMS or IVR methods to the legitimate User's cellular phone 60.
4) Notification to personnel so that they may initiate manual action to contact the Internet user via a phone call or SMS message to their cellular number. If contact cannot be made between personnel and the User, and a suitable explanation given by the User, then the account may be suspended or law enforcement agency contacted. If there is a suitable explanation, assistance may be offered to the legitimate user.

Some or all of the functions of the Application may be distributed and be associated with the Authentication Server or other applications such as a web server not necessarily part of this system.

The Event database functions maybe provided in a separate database or combined with other databases that may be part of a system.

The Location database functions maybe provided in a separate database or combined with other databases that may be part of a system.

The implementation of the invention could have a logical flow as depicted in Figure 2 and Figure 3. This is an example of how a system could function, and others are possible, considering other factors and combinations of these factors and other factors in the decisions.

The method starts with an attempt to access the internet at a location (105). Equipment at the location will capture the request and forward it to a centralized Server (110) making

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.