I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted via the Office electronic filing system in accordance with 37 CFR § 1.6(a)(4).

Dated: January 31, 2014
Electronic Signature for Marcus E. Browne: / Marcus E. Browne /

Docket No.: W0537-700620
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Kenneth P. Weiss

Application No.: 11/768,729 | Confirmation No.: 3536

Filed: June 26, 2007 | Art Unit: 2435

For: UNIVERSAL SECURE REGISTRY | Examiner: Thomas A. Gyorfi

SUPPLEMENTAL AMENDMENT

Commissioner for Patents

Dear Madam:

INTRODUCTORY COMMENTS

In response to the Amendment filed on January 2, 2014 to the Office Action mailed October 2, 2013, and in response to the Examiner Interview conducted on January 24, 2014, please amend the above-identified U.S. patent application as follows:

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks begin on page 11 of this paper.

APPLE 1124

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Currently Amended) A secure registry system for providing information to a provider ~~first party~~ to enable transactions between the provider ~~first party~~ and entities with secure data stored in the secure registry system, the secure registry system comprising:

a database including secure data for each entity, wherein each entity is associated with a time-varying multicharacter code for each entity having secure data in the secure registry system, respectively, each time-varying multicharacter code representing an identity of one of the respective entities; and

a processor configured to receive a transaction request including at least the time-varying multicharacter code for the entity on whose behalf a transaction is to be performed and an indication of the provider ~~first party~~ requesting the transaction, ~~configured~~ to map the time-varying multicharacter code to the identity of the entity ~~in the database~~ using the time-varying multicharacter code, to execute a restriction mechanism ~~configured~~ to determine compliance with any access restrictions for the provider ~~first party~~ to secure data of the entity for completing the transaction based at least in part on the indication of the first party and the time-varying multicharacter code of the transaction request, and to allow or not allow access to the secure data associated with the entity including information required to enable the transaction based on the determined compliance with any access restrictions for the provider ~~first party~~, the information including account identifying information, wherein the account identifying information is not provided to the provider ~~first party~~ and the account identifying information is provided to a third party to enable or deny the transaction with the provider ~~first party~~ without providing the account identifying information to the provider ~~first party~~.

2. (Canceled)

3. (Previously Presented) The system of claim 1, wherein the time-varying multicharacter code is provided to the system via a secure electronic transmission device.

4. (Previously Presented) The system of claim 1, wherein the time-varying multicharacter code is encrypted and transmitted to the system, and

wherein the system is configured to decrypt the time-varying multicharacter code with a public key of the entity.

5. (Currently Amended) The system as claimed in claim 1, wherein the transaction includes a service provided by the provider ~~first party~~,

wherein said provider's ~~first party's~~ service includes delivery,

wherein the information is an address to which an item is to be delivered to the entity,

wherein the system receives the time-varying multicharacter code, and

wherein the system uses the time-varying multicharacter code to obtain the appropriate address for delivery of the item by the third party.

6. – 8. (Canceled)

9. (Previously Presented) The system as claimed in claim 1, wherein the account identifying information includes credit card account information regarding the entity, and wherein the processor is configured to provide the credit card account information based upon the multicharacter code of the entity to enable the transaction.

10. (Previously Presented) The system as claimed in claim 9, wherein the system is configured to receive an approval of the credit card transaction.

11. (Previously Presented) The system as claimed in claim 1, wherein the account identifying information includes bank card account information regarding the entity, and wherein the processor

is configured to provide the bank card account information to enable the transaction based upon the multicharacter code of the entity.

12. (Previously Presented) The system as claimed in claim 11, wherein the system is configured to provide an approval of the bank card transaction.

13. (Previously Presented) The system as claimed in claim 1, wherein the information includes personal identification information regarding the entity.

14. (Currently Amended) The system as claimed in claim 13, wherein the personal identification information comprises a photograph of the entity, and wherein the photograph is provided to the provider ~~first party~~.

15. (Previously Presented) The system as claimed in claim 1, wherein the account identifying information identifies email address information regarding the entity.

16. (Currently Amended) A method for providing information to a provider ~~first party~~ to enable transactions between the provider ~~first party~~ and entities who have secure data stored in a secure registry in which each entity is identified by a time-varying multicharacter code, the method comprising:

receiving a transaction request including at least the time-varying multicharacter code for an entity on whose behalf a transaction is to take place and an indication of the provider ~~first party~~ requesting the transaction;

mapping the time-varying multicharacter code to an identity of the entity ~~in a database~~ using the time-varying multicharacter code;

determining compliance with any access restrictions for the provider ~~first party~~ to secure data of the entity for completing the transaction based at least in part on the indication of the provider ~~first party~~ and the time-varying multicharacter code of the transaction request;

accessing information of the entity required to perform the transaction based on the determined compliance with any access restrictions for the provider ~~first party~~, the information including account identifying information;

providing the account identifying information to a third party without providing the account identifying information to the provider ~~first party~~ to enable or deny the transaction; and

enabling or denying the provider ~~first party~~ to perform the transaction without the provider's ~~first party's~~ knowledge of the account identifying information.

17. – 18. (Canceled)

19. (Previously Presented) The method of claim 16, wherein the act of receiving the time-varying multicharacter code comprises receiving the time-varying multicharacter code transmitted via a secure electronic transmission device.

20. (Previously Presented) The method of claim 16, wherein the act of receiving the time-varying multicharacter code comprises receiving an encrypted multicharacter code, and

wherein the method further comprises decrypting the encrypted multicharacter code.

21. (Currently Amended) The method as claimed in claim 16, wherein the transaction includes a service provided by the provider ~~first party~~,

wherein the service includes delivery,

wherein the account identifying information is associated with an address to which an item is to be delivered for the entity, and

wherein the third party receives the address for delivery of an item provided by the provider ~~first party~~.

22. – 23. (Canceled)

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.