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 NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/655,880	10/19/2012	Sreyash Kenkre	IN920120146US1 (790.168)	1515

89885 7590 11/21/2016
FERENCE & ASSOCIATES LLC
409 BROAD STREET
PITTSBURGH, PA 15143

EXAMINER	
AZIZ, ABDULMAJEED	

ART UNIT	PAPER NUMBER
3694	

MAIL DATE	DELIVERY MODE
11/21/2016	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte SREYASH KENKRE and RAGHURAM KRISHNAPURAM

Appeal 2014–006916
Application 13/655,880
Technology Center 3600

Before ANTON W. FETTING, BIBHU R. MOHANTY, and BRADLEY B. BAYAT, *Administrative Patent Judges.*

FETTING, *Administrative Patent Judge.*

DECISION ON APPEAL

STATEMENT OF THE CASE[1]

Sreyash Kenkre and Raghuram Krishnapuram (Appellants) seek review under 35 U.S.C. § 134 of a final rejection of claims 1, 5, 7–12, 16, and 18–21, the only claims pending in the application on appeal. We have jurisdiction over the appeal pursuant to 35 U.S.C. § 6(b).

---

[1] Our decision will make reference to the Appellants' Appeal Brief ("App. Br.," filed January 27, 2014) and Reply Brief ("Reply Br.," filed May 23, 2014), and the Examiner's Answer ("Ans.," mailed March 26, 2014), and Final Action ("Final Act.," mailed August 29, 2013).

The Appellants invented a way of facilitating the detection of prominent transactions in complex networks, such as money laundering transactions. Spec., para. 19.

An understanding of the invention can be derived from a reading of exemplary claim 1, which is reproduced below (bracketed matter and some paragraphing added).

1. A method comprising:

utilizing one or more processors to execute a program of instructions configured to:

[1] identify a locality

comprising a set of nodes in a graph of nodes and edges

via identifying nodes within a predetermined connective distance of a core node,

wherein the edges represent financial transactions between nodes;

[2] identify, in the locality, at least one target source-destination node pair for monitoring;

[3] generate, with respect to the monitoring, at least one rule relating to money laundering;

[4] flag interactions upon detected violations of at least one rule;

and

[5] update, in response to the detected rule violations:

the identified locality;

the at least one target source-destination pair;

and

the at least one rule.

The Examiner relies upon the following prior art:

Reiter	US 2002/0156747 A1	Oct. 24, 2002
Steier	US 2005/0222929 A1	Oct. 6, 2005
Kolhatkar	US 2013/0018796 A1	Jan. 17, 2013

Claims 11, 12, 16, and 18–20 stand rejected under 35 U.S.C. § 101 as directed to non–statutory subject matter.

Claims 1, 5, 7–9, 11, 12, 16, 18, 19, and 21 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Steier and Kolhatkar.

Claims 10 and 20 stand rejected under 35 U.S.C. § 103(a) as unpatentable over Steier, Kolhatkar, and Reiter.

ISSUES

The issues of obviousness turn primarily on the predictability of updating data in response to detecting an underlying problem identified by some rule.

FACTS PERTINENT TO THE ISSUES

The following enumerated Findings of Fact (FF) are believed to be supported by a preponderance of the evidence.

Facts Related to the Prior Art:

Kolhatkar

01. Kolhatkar is directed to detecting electronic payment card money laundering. Kolhatkar describes receiving real-time payment card transaction data from ingress channels and egress channels of at least one payment card system through a first

application programming interface (API); generating transactional profiles for each of at least payment cards, the ingress channel, the egress channels, and funding sources of the payment cards; in response to receiving transaction data for a current payment card transaction, evaluating the transaction data using a predictive algorithm that compare the transaction data to the transactional profiles to calculate a probabilistic money laundering score for the current transaction; evaluating the probabilistic money laundering score and current transaction data based on a set of rules to generate a suspicious activity report that recommends whether to approve or report the current transaction; and transmitting the suspicious activity report back to the payment card system and transmitting the suspicious activity report to an identified regulatory body. Kolhatkar, para. 12.

02. An exemplary system for identifying money laundering allows for real-time monitoring of funds moving into and exiting an electronic payment card across multiple channels. This system has the capacity for dynamically updating an Anti-Money Laundering monitoring (AML) system to reflect current AML trends with (a) the use of real-time feedback events that notify the AML system of known money laundering behavior, and (b) self-learning money laundering prediction algorithms that use this real-time feedback to modify the algorithms to account for current patterns in money laundering behavior. This AML system has the capability of tracking fund movements to both other electronic payment cards and other exit channels. The system has the ability

to use every transaction to build profiles of users, payment cards, ingress and egress channels, and funding sources across multiple dimensions. The system has the ability to evaluate every transaction in a payment system in real-time using internal and external data to predict money laundering risk with a dynamic rules engine and/or predictive models to recommend a decision to approve or file a suspicious activity report (SAR) for the card holder. Kolhatkar, paras. 25–26.

03. The anti-money laundering rules component may use multiple predictive algorithms in general as well as within a given use case. The predictive algorithms may include, but are not limited to, regression, decision trees, neural networks, random forest, and genetic algorithms. The result of the anti-money laundering rules component is a probabilistic score assigned to a transaction and/or to the parties involved in the transaction. The anti-money laundering rules component is designed to be self-learning with the ability to incorporate new anti-money laundering behaviors into the predictive algorithms. Kolhatkar, para. 40.

Steier

04. Steier is directed to financial accounting and auditing, and more particularly to systems and methods of identifying risks of material misstatement due to fraudulent financial reporting in connection with a financial audit, and to systems and methods of investigating financial fraud with regard to forensic and investigative accounting. Steier, para. 2.

05. A way to examine and analyze transactions is to find rules that can be applied to the characteristics of the transactions to distinguish transactions that result in anomalous account values from those that result in non-anomalous account values. The transactions are divided into two sets, anomalous transactions and non-anomalous transactions, depending on whether the transactions are linked to anomalous account activity or other anomalies, as determined above. The two sets of transactions are then input into a decision tree algorithm or a rule induction algorithm to construct a set of rules that describes each set. For example, the decision tree algorithm processes the set of transactions linked to anomalous account activity or other anomalies. In processing this set, the decision tree identifies a set of rules, such that each transaction meets at least one of the rules. This set of rules is then outputted. A similar set of rules is generated for the transactions linked to non-anomalous account activity or other non-anomalous data. The rules that are output are similar to the common characteristics identified in the descriptions of the clusters above. Once generated, these rules may be more succinct and easier to use, because the rules include only the characteristics relevant to the operation of the rules. Steier, para. 88.

06. Once the clustering algorithms have identified the common characteristics of the anomalous data points, such as the transactions known to generate the anomalies in the activity, or the decision tree algorithms have identified the set of rules that

describe the characteristics of the anomalous data points, then the common characteristics of each cluster are compared with characteristics predictive of risks of material misstatement due to fraud, such as the characteristics of clusters of transactions or the set of rules generated from analyses of companies known to be fraudulent. For example, data retrieved from a company where fraud is already known to have existed is analyzed to identify anomalous account activity and then identify the common characteristics or set of rules of the underlying transactions which contributed to the anomalous account activity. Alternatively, the financial data from known fraudulent companies may be analyzed using other methods, such as the classical forensic investigative techniques to identify such predictive characteristics or sets of rules. Steier, para. 89.

07. At a high level, one way to determine which subsets to use in the multivariate regression analysis follows the method of Figure 11. A structural equivalence profiling is applied to the money flow graph. The results of the structural equivalence profiling are analyzed to identify structurally similar accounts or account clusters, based on the money flows between accounts. These account clusters are subjected to further analysis. The flow of money amongst the accounts of the company can be depicted as a graph, with each account being represented by a node in the graph, and each transfer of money between accounts being represented by a line (known as an edge) connecting a pair of nodes in the graph. The nodes of the graph in Figure 12 are derived from the

account data, by associating one node with each account in the financial accounting system for XYZ Company. The edges of the graph are derived from the transaction data from XYZ Company's financial accounting system, over a given time period. An edge between two account nodes is created if the two accounts appear in the same transaction. The arrows on the edges between each pair of nodes in the graph indicate which direction the money is flowing in the graph. The edges of the money flow graph may depict simple flow paths between accounts during the time period, or alternatively the edges may include additional data, such as the number of transactions, the average dollar value of the transactions, the total dollar value of the transactions, or other such data. The nodes of the money flow graph may represent accounts within the company, or alternatively they may represent other aggregations of transaction or other financial information, such as financial statement line items, consolidated spreadsheet entries, account category aggregations, sub-accounts, or any other aggregation of transaction information useful to the analysis. Steier, paras. 113–117.

08. Principal component analysis is applied to the collection of time series derived from the changes to each account in the general ledger over time. The anomaly detection algorithms are then applied, to only the first few principal components to detect dates on which there are sudden changes in coefficients of the terms. These dates are then flagged as anomalies and are then used as inputs by the algorithms that compare the entries on the

> anomalous dates to the entries on the previous dates, as well as the other algorithms used to process the anomalous data, such as to determine potential reasons for the anomalies, common characteristics of the anomalies, or compare the anomalous data to fraud predictive data. Use of the smaller number of principal components instead of the larger underlying collection of time series data streamlines the anomaly detection process significantly, because the anomaly detection algorithms are processing significantly less data, without losing significant levels of accuracy. Steier, para. 135.

ANALYSIS

Claims 11, 12, 16, and 18–20 rejected under 35 U.S.C. § 101 as directed to non–statutory subject matter

We summarily affirm this uncontested rejection.

Claims 1, 5, 7–9, 11, 12, 16, 18, 19, and 21 rejected under 35 U.S.C. § 103(a) as unpatentable over Steier and Kolhatkar

Claims 10 and 20 rejected under 35 U.S.C. § 103(a) as unpatentable over Steier, Kolhatkar, and Reiter

We are not persuaded by Appellants' argument that

> the applied references whether considered alone or in combination, at the very least fail to teach (as presently broadly claimed by independent Claims 1, 11, 12 and 21) updating, in response to detected rule violations: an identified locality; at least one target source-destination pair; and at least one rule. . . . To the extent that Kolhatkar alone is relied upon for allegedly showing updating of any sort, it falls far short of teaching or suggesting all three types of presently claimed updates.

App. Br. 15–16. The limitation at issue is "update, in response to the detected rule violations: the identified locality; the at least one target source-destination pair; and the at least one rule." The manner and implementation of such an update is neither recited nor narrowed. As the recited locality, target source-destination pair, and rule refers to rules, and graph elements themselves are abstractions of accounts and their usage, the recited update is metaphoric rather than literal. Some representational data is the implied target of such update. The nature of this representational data is similarly neither recited nor narrowed.

As the Examiner finds,

> Kolhatkar alone is not relied upon for all three types of 'updates'. Rather, "the identified locality" and "the at least one target source-destination pair" are taught by Steier. Whereas "the at least one rule" is taught by Kolhatkar.

Ans. 3. Kolhatkar in particular describes its operation as including self-learning, which inherently incorporates updates of its data as learning implies memory of changes, i.e. updates. Also, Steier describes rules that are output, and, once generated, these rules may be more succinct and easier to use, because the rules include only the characteristics relevant to the operation of the rules. This explicitly describes an update for easier use.

Steier describes analysis of source and destination nodes and transactions between them. The path between them is within the scope of the recited identified locality and the source and destination are within the scope of a target source-destination pair. As the edges may include additional data, such as the number of transactions, the average dollar value of the transactions, the total dollar value of the transactions or other such data, the information describing the identified locality and source-destination

pair are updated to include such information. Having also identified potential rule violations, the association of those particular nodes and edges forming an identified locality and source destination pair combined with the identification of such a violation are then updates in response to the rule violations.

CONCLUSIONS OF LAW

The rejection of claims 11, 12, 16, and 18–20 under 35 U.S.C. § 101 as directed to non–statutory subject matter is proper.

The rejection of claims 1, 5, 7–9, 11, 12, 16, 18, 19, and 21 under 35 U.S.C. § 103(a) as unpatentable over Steier and Kolhatkar is proper.

The rejection of claims 10 and 20 under 35 U.S.C. § 103(a) as unpatentable over Steier, Kolhatkar, and Reiter is proper.

DECISION

The rejections of claims 1, 5, 7–12, 16, and 18–21 are affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a). *See* 37 C.F.R. § 1.136(a)(1)(iv) (2011).

AFFIRMED