International Journal of Accounting Information Systems xxx (xxxx) xxx

Contents lists available at ScienceDirect

International Journal of Accounting Information Systems

journal homepage: www.elsevier.com/locate/accinf

Anti-Money Laundering: Using data visualization to identify suspicious activity

Kishore Singh [a,*], Peter Best [b]

[a] Accounting Data Analytics, Central Queensland University, Australia
[b] School of Business & Law, Central Queensland University, Australia

ARTICLE INFO

Article history:
Received 28 February 2017
Received in revised form 29 April 2019
Accepted 24 June 2019
Available online xxxx

Keywords:
Anti-Money Laundering
visualization
link analysis
money laundering symptoms

ABSTRACT

Annually, money laundering activities threaten the global economy. Proceeds of these activities may be used to fund further criminal activities and to undermine the integrity of financial systems worldwide. For these reasons, money laundering is recognized as a critical risk in many countries. There is an emerging interest from both researchers and practitioners concerning the use of software tools to enhance detection of money laundering activities. In the current economic environment, regulators struggle to stay ahead of the latest scam, and financial institutions are challenged to ensure that they can identify and stop criminal activities, while ensuring that legitimate customers are served more effectively and efficiently. Effective technological solutions are an essential element in the fight against money laundering. Improved data and analytics are key in assisting investigators to focus on suspicious activities. Continually evolving regulations, together with recent instances of money laundering violations by some of the largest financial institutions, have highlighted the need for better technology in managing anti-money laundering activities. This study explores the use of visualization techniques that may assist in efficient identification of patterns of money laundering activities. It demonstrates how link analysis may be applied in detecting suspicious bank transactions. A prototype application (AML^{2}ink) is used for proof-of-concept purposes.

© 2019 Elsevier Inc. All rights reserved.

1. Introduction

Money laundering is the process by which criminals attempt to disguise illicit assets as legitimate assets that they have a right to possess and spend (AUSTRAC, 2011). Operations are designed to take the proceeds of illegal activity, such as profits from drug trafficking, and cause them to appear to come from legitimate sources. Once illegal money has been laundered, the perpetrator is able to spend or invest the illicit income in legitimate assets. Money laundering threatens the prosperity of the global economy, undermines the integrity of financial systems and funds further criminal activity which impacts on community safety and wellbeing (ACFE, 2016).

Money laundering is a big business, however, since it is illegal and falls outside the realm of official economic statistics, any estimate is based on a combination of experience, extrapolation, and intuition. The International Monetary Fund (IMF) estimates that the aggregate level of money laundering is between 2 and 5% of the world's annual gross domestic product or approximately 1.5 trillion US dollars (FATF, 2014). In Australia this figure amounts to approximately $10–$15 billion per annum (AUSTRAC, 2011). However, the aforementioned estimates should be treated with caution. They are intended to give an estimate of the magnitude of money laundering only.

* Corresponding author.
E-mail addresses: k.h.singh@cqu.edu.au, (K. Singh), p.best@cqu.edu.au. (P. Best).

https://doi.org/10.1016/j.accinf.2019.06.001
1467-0895/© 2019 Elsevier Inc. All rights reserved.

Please cite this article as: K. Singh and P. Best, Anti-Money Laundering: Using data visualization to identify suspicious activity..., International Journal of Accounting Information Systems, https://doi.org/10.1016/j.accinf.2019.06.001

There are many ways that criminals can launder money, but the process itself consists of three stages: i) placement, ii) layering, and iii) integration. In the placement stage, the criminal introduces illegal funds into the financial system. This may be done by breaking up large amounts of cash into smaller amounts which may be deposited directly into a bank account, or by using cash to purchase monetary instruments (cashier's checks, travelers checks, money orders, prepaid cards and so on) that are collected and deposited into accounts at another location. After the funds have entered the financial system, the criminal engages in a series of conversions or movements of the funds to distance them from their source (layering stage). The funds might be channeled through the purchase and sale of investment instruments, or be transferred through a series of accounts at various banks across the globe. In some instances the transfers are concealed as payments for goods or services, thus giving them a legitimate appearance. In the final or integration stage, the funds re-enter the legitimate economy. The criminal may choose to invest the funds into real estate, luxury assets, or business ventures (ACFE, 2016; FATF, 2014; Watkins et al., 2003).

Innovative application of data visualization techniques in various fields has gained momentum in the past decade (Bolton and Hand, 2002; Chang et al., 2008; Didimo et al., 2011; Singh and Best, 2016). This paper advances the field of financial crime prevention by exploring and demonstrating the application of visualization techniques to assist in the identification of patterns of money laundering activity. The paper is organized as follows. Section 2 discusses the background and related work in anti-money laundering. Section 3 describes the methodology adopted, including task analysis, system design, implementation, and testing. Section 4 discusses the validation of the "proof of concept" prototype. Section 5 discusses the findings, contributions and limitations of the study, and finally, we offer concluding comments and future directions for research in Section 6.

2. Background and related work

Financial regulations and legislation obliges banks and financial institutions to file reports detailing large cash transactions or suspicious activity with Financial Intelligence Units (FIUs). Documents and reports filed with FIUs contain valuable information that may be useful in tracing hidden assets. Globally, the anti-money laundering and counter-terrorist financing laws in countries impose reporting and record-keeping requirements on banks and other financial institutions within their jurisdictions. Such laws require that suspicious transactions be reported to the FIUs, and these reports contain, among other things, the identity of the persons making the transactions and the amount of the transactions. They provide valuable information that may be used to: i) identify illegal activity, ii) detect the flow of illicit funds, and iii) identify leads to assets purchased with ill-gotten gains. In the United States, the Bank Secrecy Act (BSA) sets forth a system of reporting and recordkeeping requirements designed to help track large or unusual financial transactions.

The Financial Crimes Enforcement Network (FinCEN), maintains information that may be relevant to an investigation, including: i) Currency Transaction Reports (CTRs), ii) Suspicious Activity Reports (SARs), iii) Foreign Bank and Financial Account Reports (FBARs), and iv) Currency or Monetary Instrument Reports (CMIRs). In Australia, the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act) establishes the reporting obligations designed to combat money laundering or terrorism financing. The Australian Transaction Reports and Analysis Centre (AUSTRAC), regulates the AML CTF Act. In the United Kingdom, the law provides that organizations must report activity that may be linked to money laundering or terrorist financing to the National Crime Agency (NCA). In Canada, reporting obligations are imposed under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, and regulated by the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). In Germany, the Money Laundering Act requires Banks to report suspected money laundering to the FIU within the Federal Criminal Investigative Service (Bundeskriminalamt or BKA), and to the State Attorney (Staatsanwaltschaft) (ACFE, 2016; AUSTRAC, 2011; BA, 2016; Mitsilegas and Gilmore, 2007; Newman, 2007; Senator et al., 1995).

Money laundering exists in a complex chain that starts with placement of illegal funds into a legal financial system, followed by layering to conceal the funds' true origins and finally integration into a legitimate financial system (Buchanan, 2004; FATF, 2014). Due to the large amount of transactions occurring daily in a financial system, finding specific instances of money laundering becomes a non-trivial task (Lopez-Rojas and Axelsson, 2012). It is essential to support identification of suspicious activity with tangible evidence to ensure investigation by government agencies.

Bolton and Hand (2002) proposed that illegal financial transactions may be identified by flagging individuals according to perceived risk and to restrict their transactions using thresholds. Transactions exceeding predetermined thresholds require scrutiny. An undesirable consequence is that criminals adapt their behavior to avoid this control, for example, they deposit smaller amounts that are under the threshold (structuring). Hence, this control exclusively is inadequate in detecting suspicious transactions (Harvey and Magnusson, 2009). Many analysts use spreadsheets to examine large data tables. Although spreadsheets provide a detailed view of transactions, they do not offer a clear view of trends and correlations (Chang et al., 2007). Tools such as Table Lens (Seo and Shneiderman, 2002) and data sheets (Eick, 2000) provide enhanced views of large volumes of tabular data. Machine learning appears to have improved identification of suspicious transactions in comparison to simple threshold methods (Yue et al., 2007; Zhang et al., 2003). Gao and Ye (2007) developed a framework for anti-money laundering using a continuum of transactional patterns. Their continuum of transactional patterns range from "legal" to "usual," "unusual/abnormal/anomalous," "suspicious," and "illegal", where "usual" means "most probably but not necessarily legitimate" whereas "suspicious" implies "a larger likelihood to be illegal".

The need to identify patterns in transactional data suggests the use of data visualization. Visualization is a general term used to describe technologies that enable users to 'see' information in order to help them better understand and contextualize it (Singh and Best, 2016). Visual representations and interaction provides users with greater insights and understanding into large volumes of data. It builds on the human minds ability to understand complex information visually. Quality of visualizations produced

Please cite this article as: K. Singh and P. Best, Anti-Money Laundering: Using data visualization to identify suspicious activity..., International Journal of Accounting Information Systems, https://doi.org/10.1016/j.accinf.2019.06.001

depends directly on the quality of the underlying data. Visual analytics tools transform the data into representations suited to the analytical task at hand (Thomas and Cook, 2006). Early and efficient detection of anomalous activities often coincides with the analysis of complex networks (referred to as graphs in scientific literature) (Becerra-Fernandez et al., 2000). Visually representing such networks may convey useful information that helps investigators to identify relevant patterns of activities (Hawking et al., 2005). Chang et al. (2008) developed WireVis, a system for visual analysis of financial wire transactions. This system assists analysts in exploring large numbers of wire transactions and it combines textual and visual approaches. Johnson et al. (2004) presented a social network analysis approach to help detect financial crimes. They described the relationship between detecting financial crimes and the social web and demonstrated the application of social network analysis techniques to find suspicious online financial activities. Both the methodologies of Chang et al. (2008) and Johnson et al. (2004) use charts and plots, however, they make little use of graph visualizations.

Becerra-Fernandez et al. (2000) presented V4F. This system was designed to assist an analyst to easily correlate data and to discover complex networks of potentially illegal activities. The system uses graph visualizations. The Financial Crimes Enforcement Network (FINCEN) developed FAIS, a system that evaluates large cash transactions to identify potential money laundering. FAIS is built on a data analytics engine and several software modules (Senator et al., 1995). Multi-agent based simulation is another approach that may be used (Salamon, 2011). It involves the use of autonomous and interactive agents to model complex systems. Agents and their interaction with other agents, generates complex emergent behavior. Pavón et al. (2008) demonstrated the use of multi-agent based simulation to simulate social networks and to analyze social behavior. This is similar to mobile money (a platform for transferring money between users by mobile phone), that resembles a social network of connected clients where the connections are the transactions (money sent or received) and the nodes are the clients (Lopez-Rojas and Axelsson, 2012). Commercial systems that use graph visualization tools include i2 Analyst Notebook (Stewart and Rosemann, 2001), Netmap (Tracy et al., 2001) and, Xanalys Link Explorer (Watson and Schneider, 1999). These applications implement classical layout algorithms to represent relational data, like force-directed algorithms, hierarchical layout algorithms, and circular drawing algorithms (Peslak, 2005). Aigner et al. (2007) proposed a systematic view on methods for visualizing time-oriented data. They used three main criteria in their design; time, data and representation. They made three key observations; i) current visual methods are only suitable for specific applications, ii) interaction is key for analyzing time-oriented data and, iii) many prevailing methods focus only on representing the data and neglect the analytical component.

Huang et al. (2009) proposed a framework for visual analytics for stock market security. The approach is based on two visualizations: 1) Visual Surveillance of Market Performance, and 2) Behavior-Driven Visual Analysis of Trading Networks. In the first stage, the authors use a 3D tree map to monitor real-time stock market performance and to identify a particular stock that produced an unusual trading pattern. In the second stage behavior analysis of suspected traders is performed. Through visual pattern analysis, potential attackers and their attack plans are discovered. The system identifies fraud by conducting pattern recognition and matching an unusual pattern to similar others in a pattern database.

There is an emerging interest from both researchers and practitioners concerning the use of software tools to enhance public safety (Watkins et al., 2003). In the current economic environment, regulators struggle to stay ahead of the latest scam, and financial institutions are challenged to ensure that they can identify and stop criminal activities, while ensuring that legitimate customers are served more effectively and efficiently. In this competitive marketplace, success depends on creating new acquisition opportunities, closing loopholes and complying with regulatory requirements in all countries that an organization operates (Newman, 2007).

Liu et al. (2016) developed graph analysis techniques and applied them to real-world health-care datasets to look for fraud, waste and abuse activities. Health care relationships are represented using heterogeneous graphs. Anomalous individuals, relationships and communities are identified by analyzing the local and global characteristics of the graphs. The system provides two broad categories of functionalities: 1) automated screening, to reduce the data set to a small list of suspects, and 2) interactive drill-down, where the analyst can focus their investigation on a suspicious individual or activity.

Effective technological solutions are an essential element in the fight against money laundering. Didimo et al. (2014) describes the VisFAN system for the visual analysis of financial activity networks. The system is designed is to support analysts in the discovery of criminal patterns, like money laundering and fraud. It uses STRs submitted to FIUs by financial institutions and performs within- and cross-institution analysis of activity. It combines enhanced graph drawing techniques to devise novel algorithms, clustering techniques and interaction functionalities for the visual exploration of networked data-sets, together with tools for Social Network Analysis and for the automatic generation of reports.

Globally, regulators are emphasizing the importance of effective analytics as a compliance mechanism, for example, the AUSTRAC AML/CTF rules specify that reporting entities must include a transaction monitoring program in their AML/CTF program, to identify any suspicious transactions (AUSTRAC, 2016). Financial market researcher, Celent estimated that spending on anti-money laundering software globally would increase from US $335.4 million in 2006 to US$504 million in 2012 (Ray and Katkov, 2012), with this figure continuing to grow. Nearly 50% of an investigator's time is spent examining false positives, a waste of valuable resources. Improved data and analytics are essential in assisting investigators to focus more on suspicious activities and less on false positives (Newman, 2007). Furthermore, continually evolving regulations, together with recent instances of money laundering violations by some of the largest financial institutions, have highlighted the need for better technology in managing anti-money laundering activities (Ray, 2015).

The objective of this research is to demonstrate the feasibility of detecting potential money laundering activities based on visualization of financial transactions. The intention is to provide an investigator with a series of predetermined tests/analyses that visualize a subset of financial transactions (AUSTRAC, 2014). The study proposes the use of link analysis (Wasserman and Faust, 1994) as a means of

Please cite this article as: K. Singh and P. Best, Anti-Money Laundering: Using data visualization to identify suspicious activity..., International Journal of Accounting Information Systems, https://doi.org/10.1016/j.accinf.2019.06.001

visualizing bank transactions affecting an entity in order to detect anomalous transaction patterns which may be consistent with money laundering. This is demonstrated and tested using data obtained from the bank transactions of a large entity (*specific information is withheld for confidentiality reasons*). Feedback from audit firms, a bank and information systems auditors is obtained to assist in evaluating this approach.

3. Data visualization methodology

This study proposes the use of link analysis to visualize bank transactions affecting an entity thereby allowing potential money laundering activity to be detected. A prototype application (AML^{2}ink) has been developed and is documented in this paper to allow validation of this strategy. The prototype development approach involves the following phases: task analysis, system design, implementation, and testing (Tory and Möller, 2004).

Task analysis identifies: the problem that the system is required to solve; functions that need to be incorporated into the system to solve these problems; user requirements for the target visualizations; and any applicable limitations. Results of task analysis drive the design process in which specifications for data, processes and interfaces are planned. The design is implemented using a prototype, that is, a proof of concept intended to demonstrate the feasibility of implementation in practice. Finally, testing is performed to evaluate the systems functionality and to ensure that it meets its specified purpose. Industry feedback is also obtained to determine 'fit for purpose'.

3.1. Task analysis

Money laundering may involve a multitude of transactions, potentially, by separate individuals, into multiple accounts with different owners at different banks or financial institutions. Laundering of money involves three phases: placement, layering and integration. Money may be deposited into various bank accounts (placement). Transactions may be structured to avoid detection by reporting rules. Multiple stages of transfers may be used to disguise true origin and ultimate destination (layering). Money may be transferred among accounts and in and out of the country (Fig. 1). In some instances the transfers are concealed as payments for goods or services, thus giving them a legitimate appearance. In the final stage (integration), the money re-enters the legitimate economy (AUSTRAC, 2011; Goldberg and Wong, 1998; Newman, 2007). In an attempt to combat money laundering, FIU's require reporting of cash transactions in excess of a specified amount, for example $10,000. Additionally, related transactions in which the aggregate amount exceeds the limit are also monitored and reported by bank officials (AUSTRAC, 2016; Goldberg and Wong, 1998).

Detailed record-keeping creates an audit trail, however, the volume of transactions is large. Approaches that reduce the burden of excessive information may improve the effectiveness of identifying suspicious activities and contribute to the overall anti-money laundering effort (Singh and Best, 2016). Several descriptive and predictive statistical methods exist to analyze transactions with consistent or unusual relationships among data (Bolton and Hand, 2002; Ko et al., 2016). These are grouped into supervised and unsupervised methods. Supervised methods use a database of known "signatures" to construct a model which yields a suspicion coefficient for new cases. Traditional statistical methods (Hand, 1981), neural networks (Webb, 2003) and tree-based classification methods (Breiman et al., 1984) may be used. Link analysis (Wasserman and Faust, 1994) establishes relationships among fraudsters using social network methods. Unsupervised methods are used when there are no previous sets of legitimate and fraudulent observations. A combination of profiling and outlier detection may be used. (Bolton and Hand, 2002).

Money laundering obscures the source, ownership or use of funds obtained from illicit means. The detection of these illicit activities present difficulties not encountered in other financial networks (Bolton and Hand, 2002). Finding structural relationships among transactions that reveal the network of organizations and individuals involved in these transactions, requires an innovative approach. The use of link analysis for the detection of money laundering is proposed and demonstrated in this study.

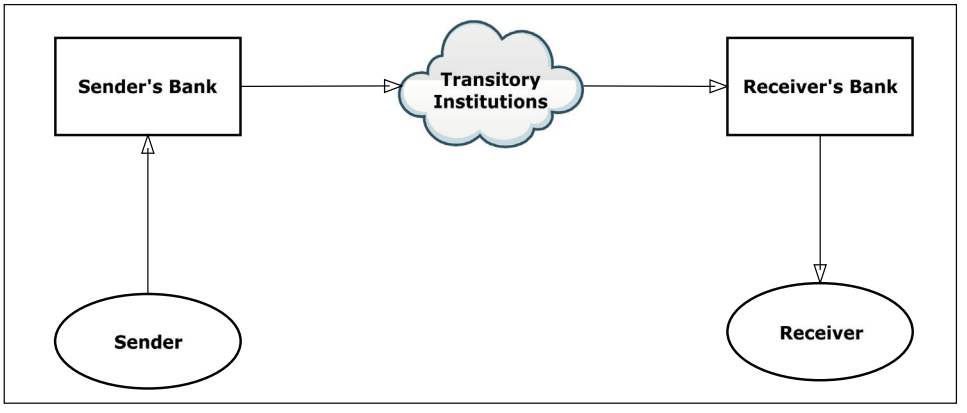


Fig. 1. Money flow through banking system.

Please cite this article as: K. Singh and P. Best, Anti-Money Laundering: Using data visualization to identify suspicious activity..., International Journal of Accounting Information Systems, https://doi.org/10.1016/j.accinf.2019.06.001

FIUs (AUSTRAC, FinCEN, FINTRAC, and so on) provide comprehensive lists of symptoms of potential suspicious activities relating to money laundering. The following list (AUSTRAC, 2014) is the basis of this study:

1. The transaction was inconsistent with the customer's profile.
2. Cash deposited domestically with the funds subsequently withdrawn from ATMs offshore.
3. Depositing multiple large amounts of cash and receiving multiple checks drawn on that account.
4. Elaborate movement of funds through different accounts.
5. Frequent early repayments of loans.
6. Funds transferred to a charity fund.
7. High volume of transactions within a short period.
8. Investment funds sent to 'interesting' countries.
9. Large sums credited into accounts from 'interesting' countries.
10. Large cash deposits into company accounts.
11. Large amounts of cash from unexplained sources.
12. Multiple transactions of a similar nature on the same day in different locations.
13. Obtained loan and repaid balance in cash.
14. Structuring cash deposits/withdrawals.
15. Transfers from company accounts to private betting accounts.
16. Unusually large transfer of money from an individual to a business.
17. Unexplained income inconsistent with economic situation.
18. 'U-turn' transactions occurring with funds being transferred out of Australia and then portions of those funds being returned.
19. Use of internet banking to frequently access Australian-based accounts internationally.

3.2. System design

Under FATF Recommendation 20, banks and financial institutions file reports detailing suspicious activities or large cash transactions with FIUs (FATF, 2012). These consist of suspicious activity reports (SARs), and currency transaction reports (CTRs), while a smaller number are cash and monetary instruments reports (CMIRs) that are filed by anyone entering or leaving a country with currency or negotiable instruments above a specified threshold (AUSTRAC, 2014; USGPO, 1970). These audit trails serve to capture limited "footprints" of many money laundering operations (Goldberg and Wong, 1998).

Money laundering exploits a web of disguised relationships. Unravelling this complex network of relationships is suited to visualization methods, particularly, link analysis. These relationships include the methods of placing money, its movement in the financial system, and the organizational entities and their owners involved in the process. Furthermore, certain entities may play a transitory role within the network, for example, a shell corporation being used to receive and distribute money. Link analysis may enable investigators to infer ownership and relationships, for example common or joint ownership of businesses, effortlessly.

In this study, link analysis is proposed to create visual representations of data to track the movement of money, demonstrate complex relationships, and discover patterns and trends that may require further investigation (Singh and Best, 2016; Watkins et al., 2003). Link analysis is characterized by a series of nodes and links. A node is shown as a circle, polygon, or some other graphical shape, and an edge is a line or curve connecting the nodes. Nodes are places in two-dimensional space, and edges represent relationships between the nodes (Singh and Best, 2016). Link analysis is effective in identifying relationships with several degrees of separation which is particularly useful in tracking the placement, layering, and integration of money as it moves around unexpected sources. Within the context of this study, a node represents a bank account and a link represents a transaction flow. Furthermore, target accounts are depicted as yellow nodes and destination accounts as cyan nodes. CR cash flows are shown in blue, and DR flows are shown in red.

Node-link visualizations are particularly useful to represent the transfer of funds between bank accounts. Nodes representing bank accounts may be the source or the receiver of a funds transfer. At times, funds received may be later transferred to other accounts or back to the source account (referred to as a 'u-turn' transaction). It is also valuable to 'follow the money' by visually observing funds transferred through a number of accounts to their ultimate destination account(s). These capabilities are provided by graphs composed of nodes and links, and distinguish node-link visualizations from other types of visualizations, including matrix-based methods, which lack these capabilities.

In developing automated AML techniques, only those symptoms that can be detected automatically are considered. For obvious reasons, any symptom that relies upon subjective interpretation by a bank employee or which requires direct contact with the client cannot be used for automatic detection purposes. In practice, the symptoms suitable for automated AML detection may be split into three subsets:

1. Those that can be detected based on data available on usual account activity statements.
2. Those where detection requires correlation that might potentially violate the bank's data policies.
3. Those where detection requires data that are not directly available from the bank's information system, but are available from other publicly accessible sources, for example, list of high-risk money laundering countries.

Please cite this article as: K. Singh and P. Best, Anti-Money Laundering: Using data visualization to identify suspicious activity..., International Journal of Accounting Information Systems, https://doi.org/10.1016/j.accinf.2019.06.001

The following symptoms of money laundering have been selected for inclusion in the prototype system design (AUSTRAC, 2014):

1. High volume of transactions within a short period/Structuring cash deposits or withdrawals.
2. 'U-turn' transactions.
3. Funds transfer involving banks in 'interesting' countries.
4. Payments of loans by external parties.

The node-link diagrams to be developed will show summary transaction flows between an entity's bank accounts and those of other parties for a specified period of time to detect high volumes of transactions and potential structuring. Nodes representing bank accounts in 'interesting' countries will be highlighted using color. Distinguishing debit and credit transaction flows will allow easy detection of 'U-turn' transactions. Transaction flows into and out of loan accounts will reveal payments from parties outside of the entity.

3.3. Implementation

Certain detection strategies may be directly applied to individual transactions in a bank's information system, for example: i) funds transfers involving source or destination bank accounts in 'interesting' countries; or ii) cash operations exceeding a predefined threshold. Other detection strategies analyze transaction patterns over time and rely on bank accounts serving well-defined purposes, such as: receiving payments from customers and paying vendors. It is expected that the transaction flows involving bank accounts of an entity not engaged in money laundering could be quite different from those of an entity that is so engaged. Once a pattern or signature is established for a "normal" entity, i.e. one with no money laundering, it may be used to investigate activities in other entities. Key issues to take into consideration include: account balance at successive dates, inbound and/or outbound transfer amounts, and identities of transfer source/destination accounts. Events that occur repeatedly at regular intervals may be suspicious and justify further investigation.

The prototype AML^{2}ink demonstrates how bank transactions can be visualized using link analysis to determine the accounts involved in a transaction, and the properties of transactions, such as amounts and 'interesting' countries. It also identifies subtle indications of suspicious behavior, for example, transactions of more than $10,000, and multiple transactions below $10,000.

The process begins with bank account transaction data being imported, cleansed and pre-processed into a standard format prior to being processed by AML^{2}ink. Next, SQL queries process data from the primary tables, using the rules defined in Section 3.2. The results are placed in a series of temporary tables which become the source data for visualizations (Singh and Best, 2016). AML^{2}ink performs the necessary computations and generates DOT code (a graph description language) which is used to render the visual elements. The DOT code is submitted to GraphViz, which renders and produces the visualizations (Fig. 2).

Graphviz was selected to produce the visualizations as the authors required a tool that could be used in non-interactive mode. Graphviz is only used to produce the visualizations. The DOT code is generated by a SQL procedure. The DOT code is passed to a Graphviz process which returns the appropriate image file that is displayed to the end-user. Furthermore, Graphviz is open source software and has the benefit of reduced costs when compared to commercial software packages (*a possible benefit may be increased uptake in the visualization approach*[1]).

Graphviz consists of a series of drawing programs such as dot, neato, twopi, circo, fdp, and sfdp. AML^{2}ink implements twopi as its principal drawing program. The radial layout algorithm represented by twopi is conceptually the simplest in Graphviz. It provides the most visually appealing graphs suitable for use by forensic investigators and for inclusion in reports or publications. It follows the algorithm described by Wills (1999). It takes a node specified as the center of the layout and the root of the generated spanning tree. The remaining nodes are placed on a series of concentric circles about the center, the circle used corresponding to the graph-theoretic distance from the node to the center. Thus, for example, all of the neighbors of the center node are placed on the first circle around the center (DiBattista, 1997). All nodes distance 1 from a node on the first circle, are placed on the second circle; and so on. The algorithm allocates angular slices to each branch of the induced spanning tree to guarantee enough space for the tree on each ring.

In DOT there are three types of objects: graphs, nodes and edges. Graphs may be undirected or directed. Layout programs in Graphviz take descriptions of graphs written in DOT, and render them into visualizations.

For each graph produced by Graphviz, detailed syntax is required to specify the type of graph, the attributes of each node, and the attributes of each edge. It is impractical for an investigator to produce this syntax manually. AML^{2}ink automates the generation of this syntax, producing a line of syntax for the overall graph including a specification whether nodes may overlap, a line of syntax for each source node specifying its shape, label (e.g. Bank-State-Branch [BSB] and account number), font, and color, a line of syntax for each destination node, and a line of syntax for each edge specifying its label (e.g. total amount, number of transactions), font, color and width.

[1] The authors interviewed data analytics teams in a large national bank and two large international audit firms. These organizations indicated that they were not using commercial visualization software products due to the high costs involved. They were seeking lower cost alternatives.

Please cite this article as: K. Singh and P. Best, Anti-Money Laundering: Using data visualization to identify suspicious activity..., International Journal of Accounting Information Systems, https://doi.org/10.1016/j.accinf.2019.06.001

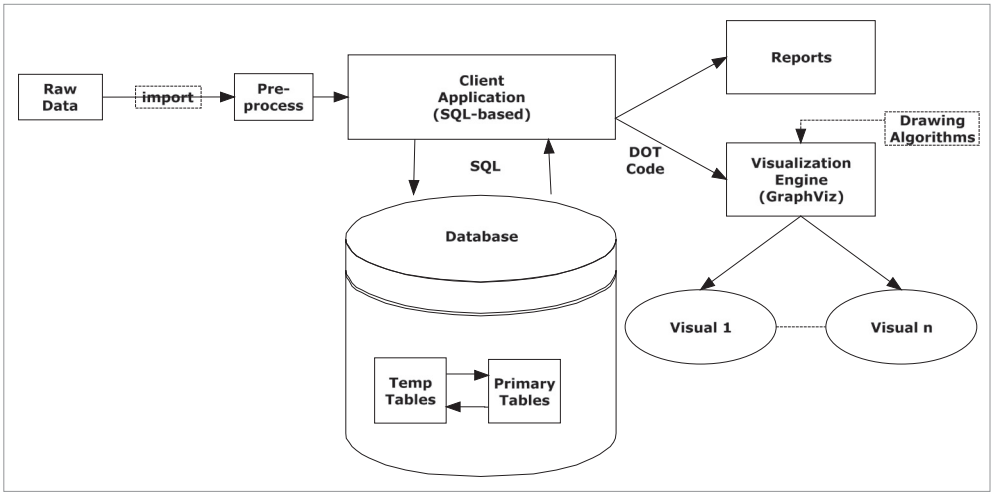


Fig. 2. System architecture.

3.4. Testing

In order to assess the usefulness of the system a sanitized data set containing transactions over a two-year period (2014 to 2016) was used. For privacy and proprietary reasons, account numbers and other information has been obscured to protect the identity and privacy of client information (Lopez-Rojas and Axelsson, 2012).

The experiment uses test data obtained from the bank transactions of a large entity (*specific information is withheld for confidentiality reasons*). The test data is limited in volume to demonstrate the application of data visualization to money laundering detection. The data consists of data observations with the following attributes:

- Target_BSB
- Target_Account
- Dest_BSB
- Dest_Account
- Num
- Sumamt
- DRCR

In this context, a target (Target_BSB + Target_Account) is a bank account of the target entity. Cash flows can be DR (outflows) or CR (inflows) transfers to a target. A destination (Dest_BSB + Dest_Account) is the account of a customer (with CR transactions) or a vendor/employee (with DR Transactions). These data observations represent the summation of individual transactions between a start-date and an end-date. The number of cash flows (Num) and the sum of the amounts (Sumamt) between the target and destination are generated for both inflows and outflows. The purpose of using summation data for a period of interest (for example, 2 weeks) is to allow detection of high volumes of transactions with customers or vendors and examination of cash flows to detect structuring of cash flows to avoid threshold monitoring (for example, methods aimed at detecting transactions exceeding $10,000). Accordingly, this analysis of data can be performed on a rolling cycle, for example, weekly.

In this experiment, the entity is assumed to have four target bank accounts (Table 1):

Cash receipts from customers are credited to account “999-991 999999992”. Cash is then transferred to accounts “999-991 999999991” and “999-991 999999993”, out of which payments are made to vendors and employees respectively. Account “999-991 999999991” is also used to make payments on the loan account “999-991 999999994”.

Table 1
Target bank accounts of the entity.

BSB	Account	Purpose of account
999-991	999999992	Receipt of cash inflows from customers
999-991	999999991	Payment of vendors, including the loan account
999-991	999999993	Payment of employees or vendors
999-991	999999994	Loan account

Please cite this article as: K. Singh and P. Best, Anti-Money Laundering: Using data visualization to identify suspicious activity..., International Journal of Accounting Information Systems, https://doi.org/10.1016/j.accinf.2019.06.001

ARTICLE IN PRESS

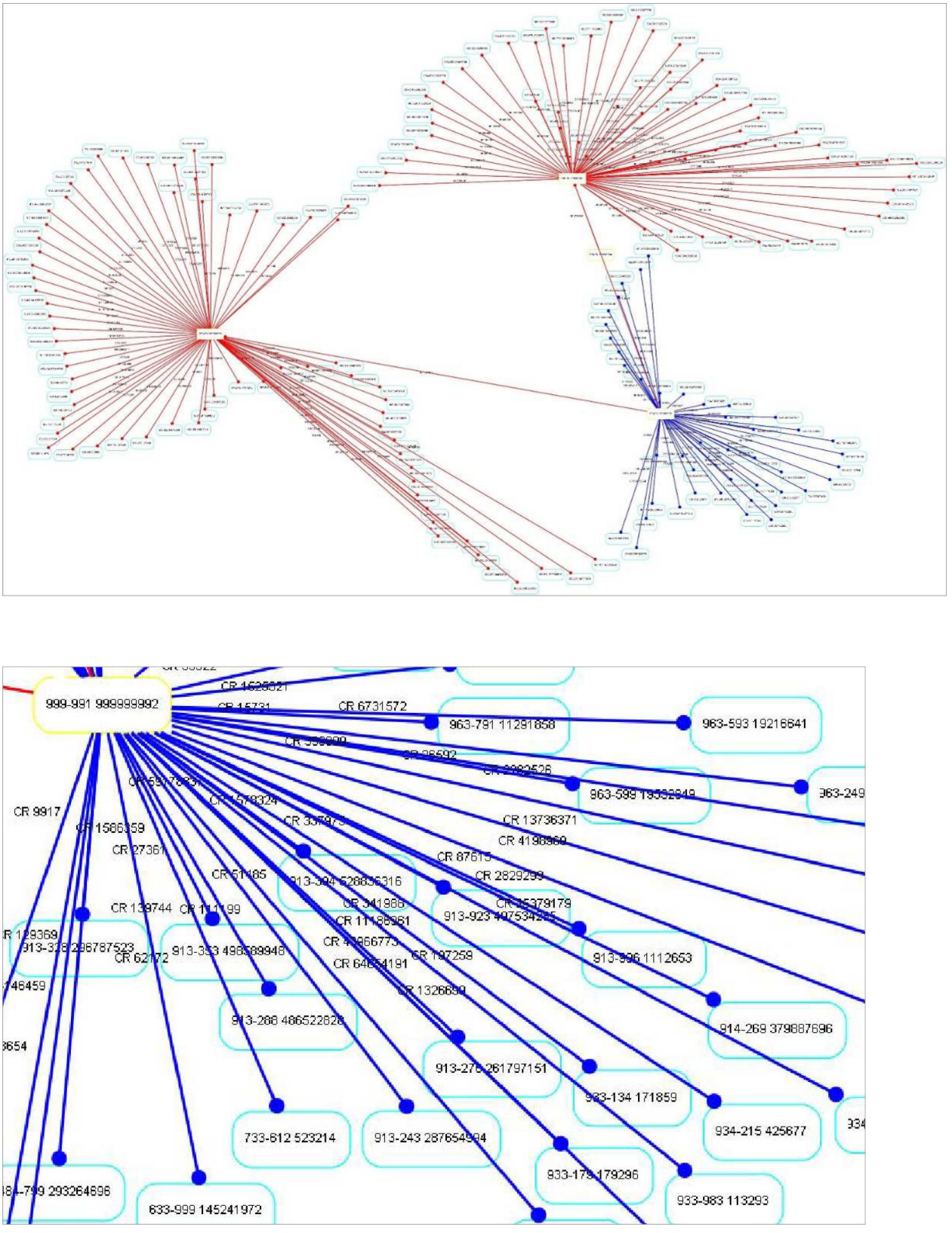


Fig. 3. Relationship among target accounts. a: Expanded view of relationship among target accounts.

Please cite this article as: K. Singh and P. Best, Anti-Money Laundering: Using data visualization to identify suspicious activity..., International Journal of Accounting Information Systems, https://doi.org/10.1016/j.accinf.2019.06.001

3.4.1. Relationship among accounts

Phase 01 of this experiment generates a directed graph for the initial test data. Fig. 3 and a provide a visualization of the above relationships among the target accounts. Targets accounts are depicted as yellow nodes and destination accounts as cyan nodes. CR cash flows are shown in blue, and DR flows are shown in red. The links have labels showing the DR/CR nature and the sum of the amounts (Sumamt). The graphs are produced as jpeg files, allowing the investigator to zoom in on large and complex graphs for more detailed review (Fig. 3a).

3.4.2. U-turn cash flows

U-turn cash flows are bi-directional flows between the target accounts and destination accounts. Such flows are unusual because they occur when an external party to the entity is both a customer (with cash inflows) of the entity and a vendor or employee (with cash outflows). It is usual for such accounts to be classified as contra-accounts and balances are offset, resulting in a net inflow or outflow, but not both.

Fig. 4 and a show the visualization of Phase 02 of this experiment where u-turn cash flows are depicted. This u-turn case involving account "913-393 483845787" is easily detected in the graph as a cash inflow to a target account apparently coming from a vendor receiving outflows from a target account.

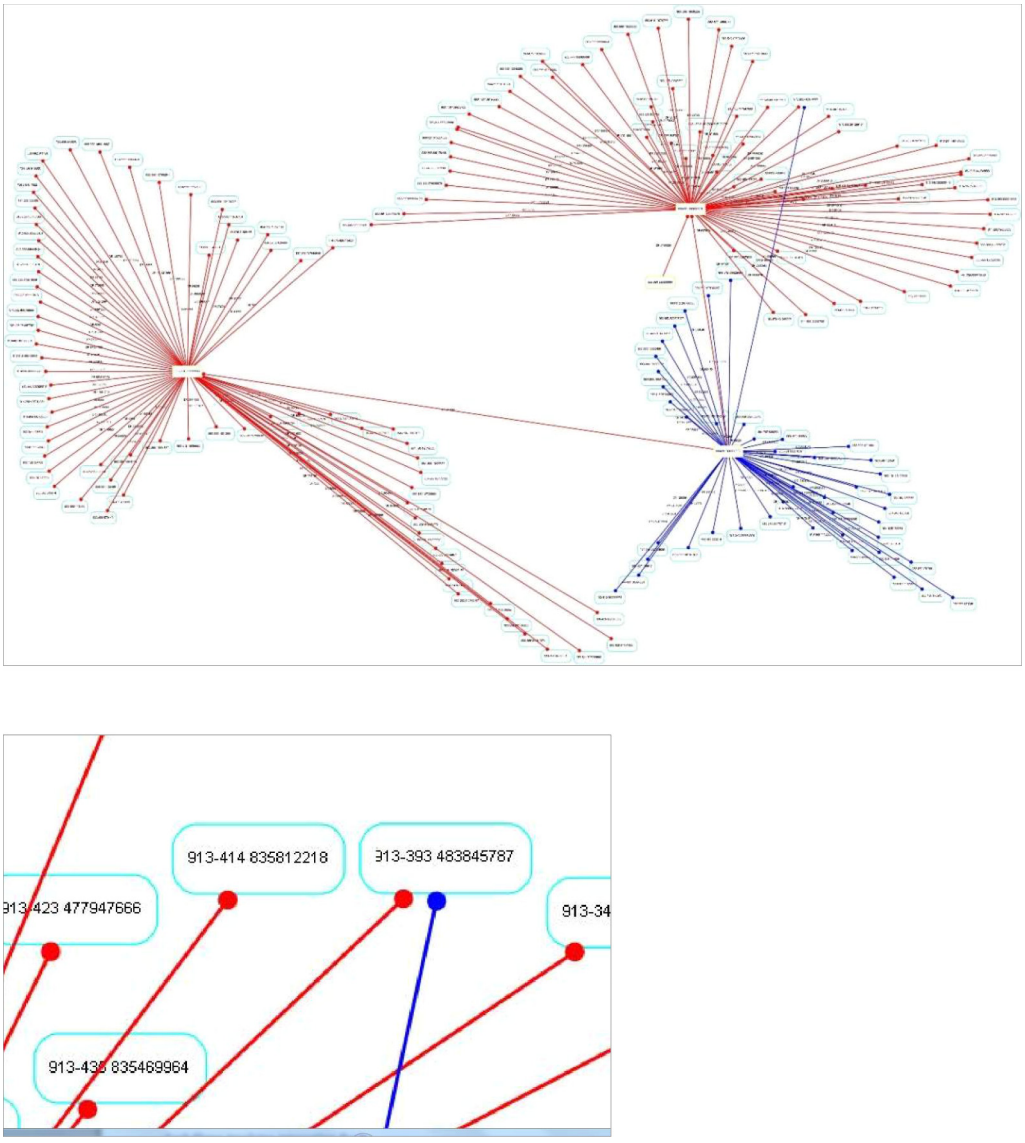
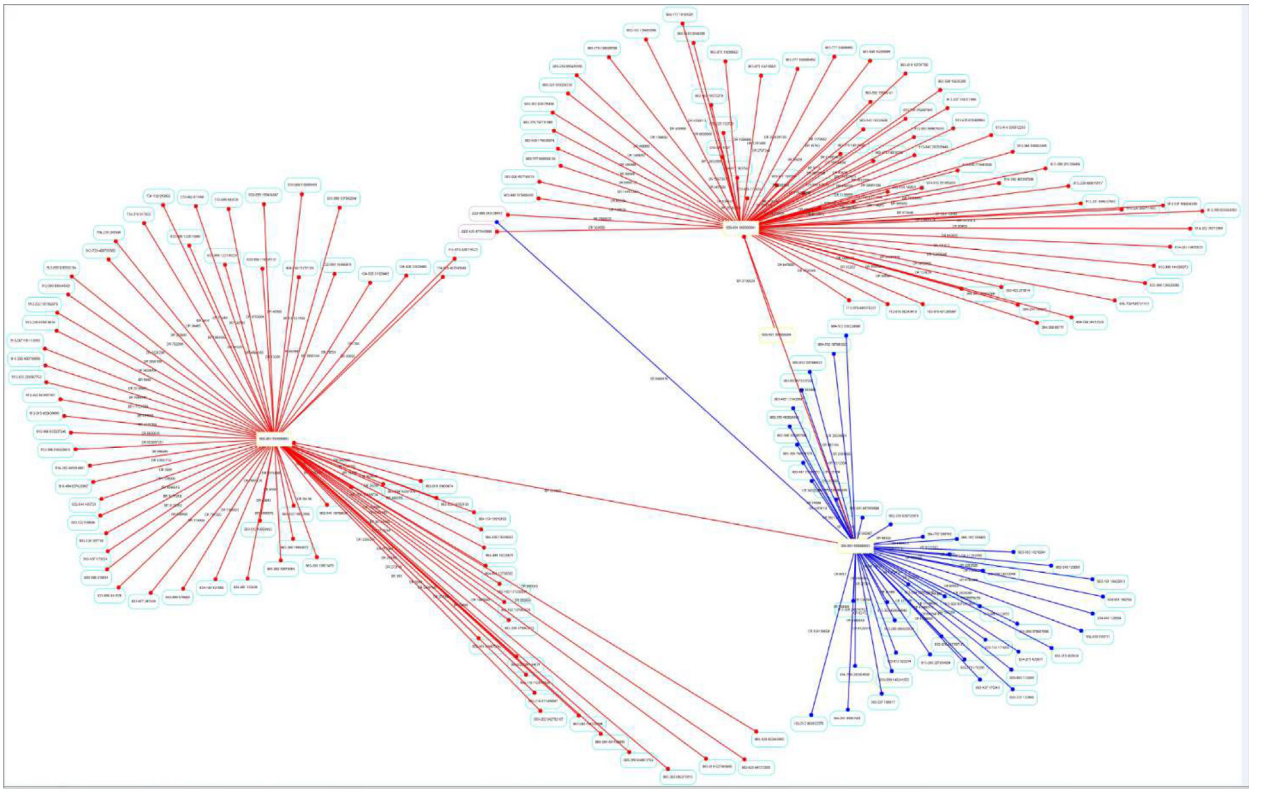


Fig. 4. U-turn cash flows. a: Expanded view of U-turn cash flows.

Please cite this article as: K. Singh and P. Best, Anti-Money Laundering: Using data visualization to identify suspicious activity..., International Journal of Accounting Information Systems, https://doi.org/10.1016/j.accinf.2019.06.001

3.4.3. Cash flows involving interesting banks

Inflows or outflows involving BSBs of interest can easily be detected and revealed in the graph using color. In Fig. 5 and a, the graph produced by Phase 03 of this experiment shows the destinations of interest using the color violet. Account "ZZZ-888 243138411" is an overseas bank account belonging to a vendor. Account "ZZZ-423 477947666" is an account used by an entity which is both a vendor and a customer (with u-turn transactions). This simple technique is used to alert the investigator to this threat.



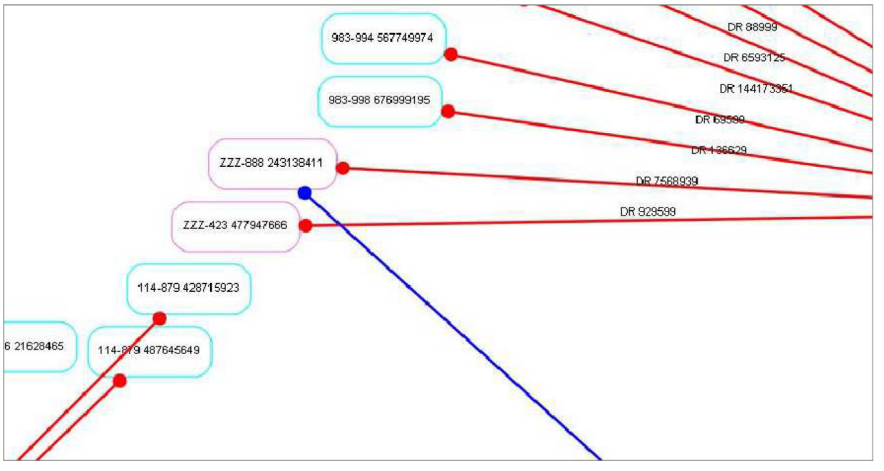


Fig. 5. Cash flows involving interesting banks. a: Expanded view of cash flows involving interesting banks.

Please cite this article as: K. Singh and P. Best, Anti-Money Laundering: Using data visualization to identify suspicious activity..., International Journal of Accounting Information Systems, https://doi.org/10.1016/j.accinf.2019.06.001

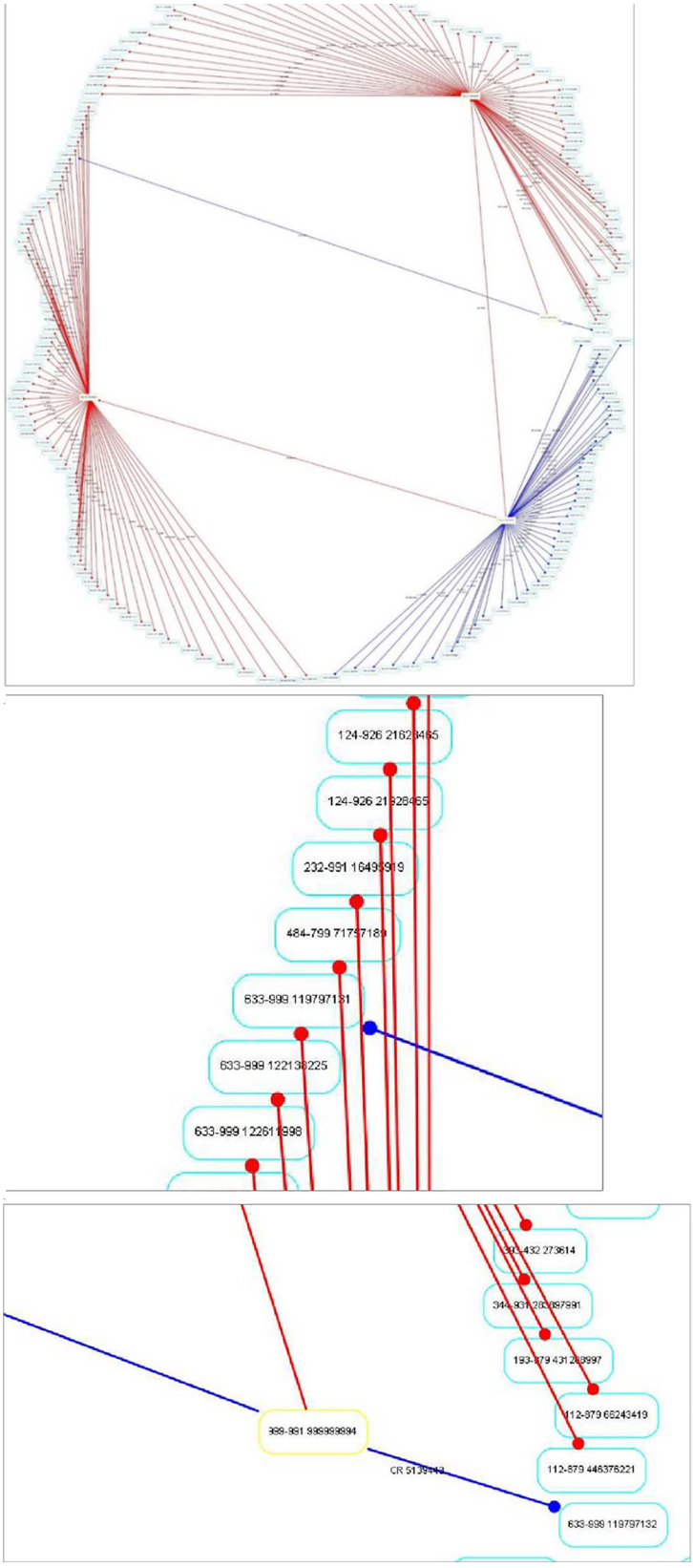
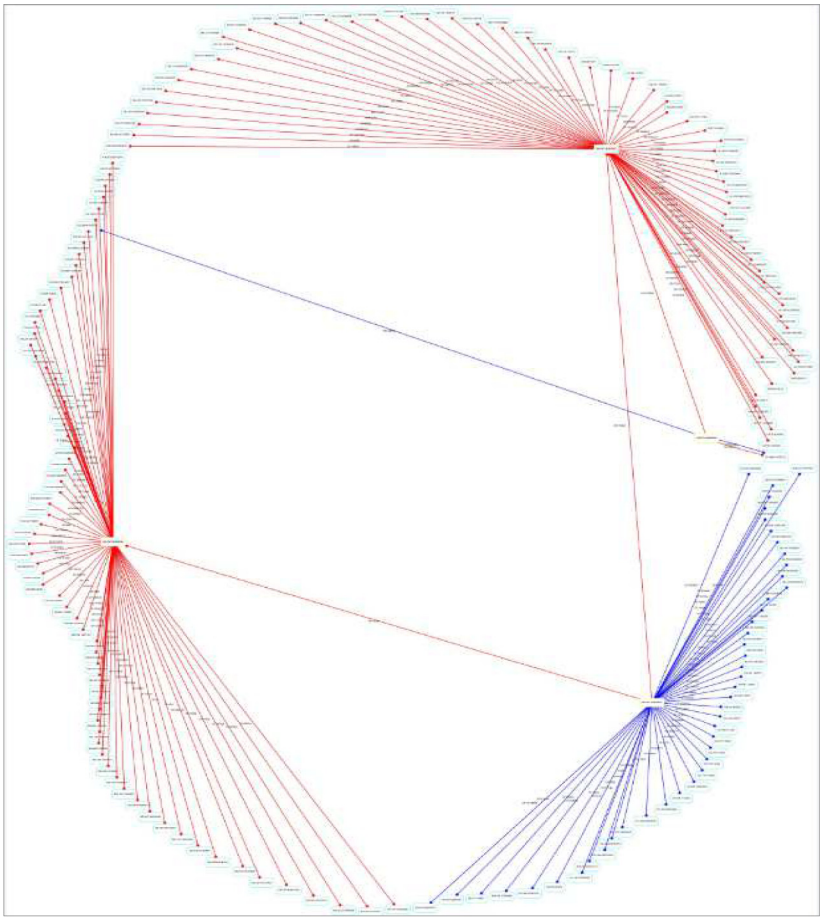


Fig. 6. Loan payback. a: Expanded view of loan payback. b: Expanded view of loan payback.

Please cite this article as: K. Singh and P. Best, Anti-Money Laundering: Using data visualization to identify suspicious activity..., International Journal of Accounting Information Systems, https://doi.org/10.1016/j.accinf.2019.06.001

3.4.4. Loan payback

Phase 04 of the experiment provides a visualization that includes the repayment of the loan by external parties. In this case, the loan account is being paid by one of the vendors using account "633-999 119797131", and by an additional source using account "633-999 119797132". This is easily detected in Fig. 6, a and b.



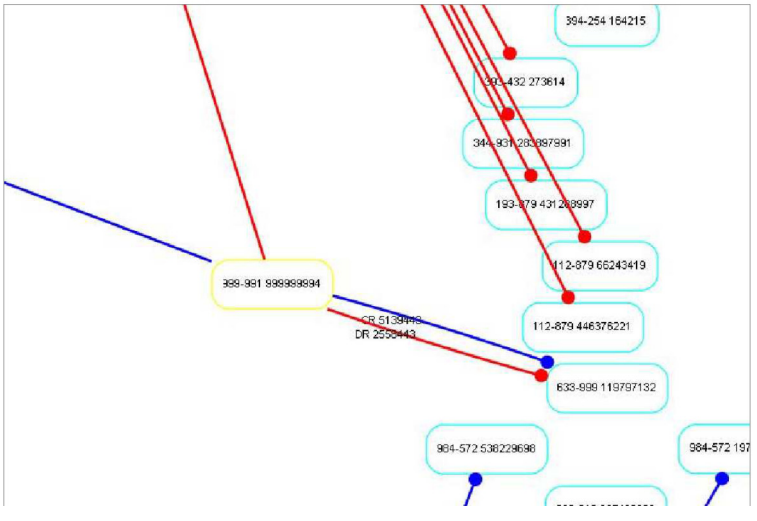


Fig. 7. U-turn transactions involving the loan account. a: Expanded view of u-turn transactions involving the loan account.

Please cite this article as: K. Singh and P. Best, Anti-Money Laundering: Using data visualization to identify suspicious activity..., International Journal of Accounting Information Systems, https://doi.org/10.1016/j.accinf.2019.06.001

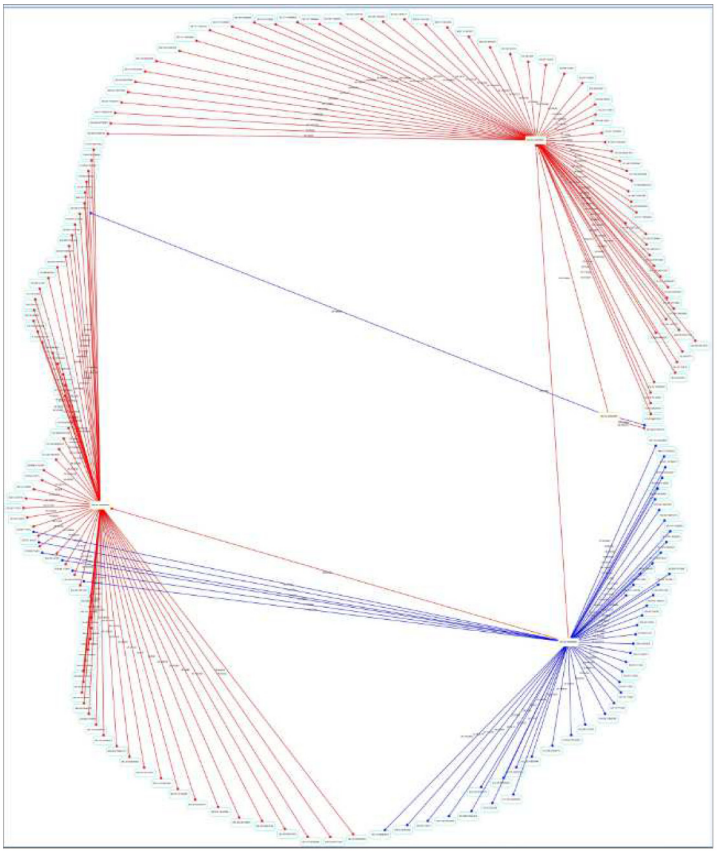
3.4.5. Further analyses

Fig. 7 and a highlight account "633-999 119797132" to which cash has been transferred directly from the loan account, after cash has been credited to the loan account from that source. This is a further case of a u-turn transaction, but involving a loan account.

The investigator is alerted to elaborate movement of funds as a key symptom of money laundering.

Fig. 8 and a illustrate multiple cases of u-turn transactions involving vendors.

Where the investigator's suspicion is aroused concerning an account (for example, one involved with u-turn transactions), further bank data can be extracted and incorporated into the visualization to "follow the money". Fig. 9 and a follow the cash flows of account "913-393 483845787". In this case, there are further u-turn transactions with account "913-277 261797151" and then with "913-299 261299464".



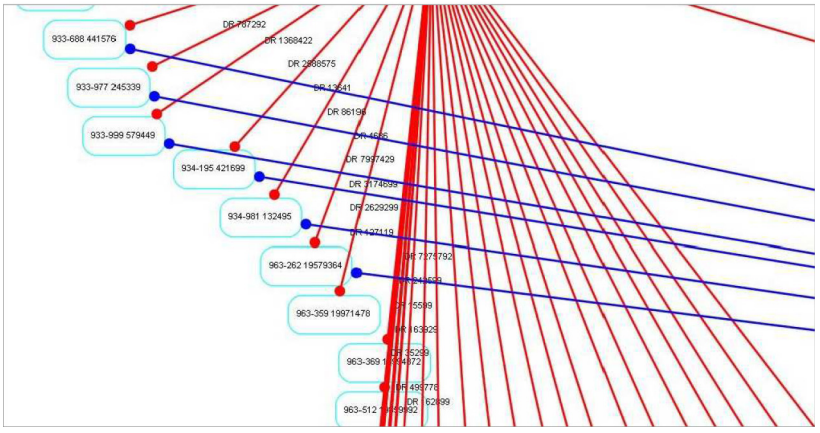
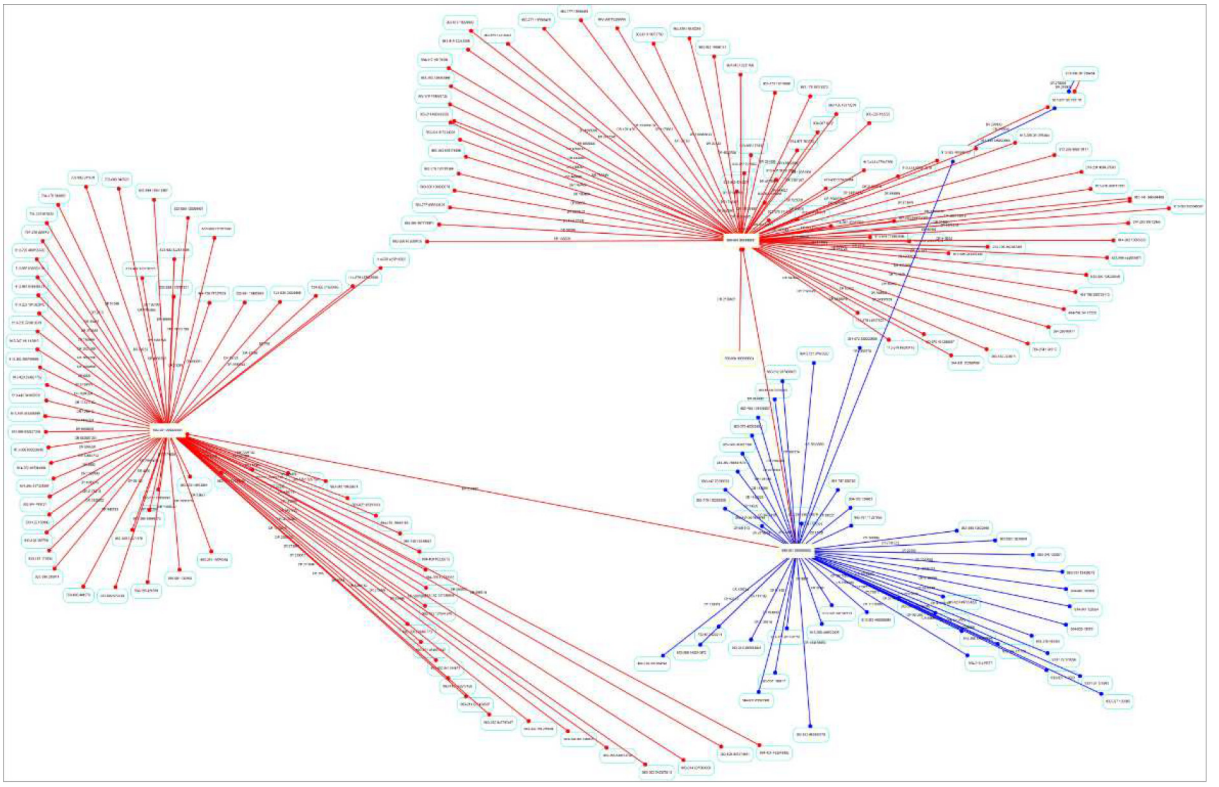


Fig. 8. Multiple u-turn transactions involving vendors. a: Expanded view of multiple u-turn transactions involving vendors.

Please cite this article as: K. Singh and P. Best, Anti-Money Laundering: Using data visualization to identify suspicious activity..., International Journal of Accounting Information Systems, https://doi.org/10.1016/j.accinf.2019.06.001



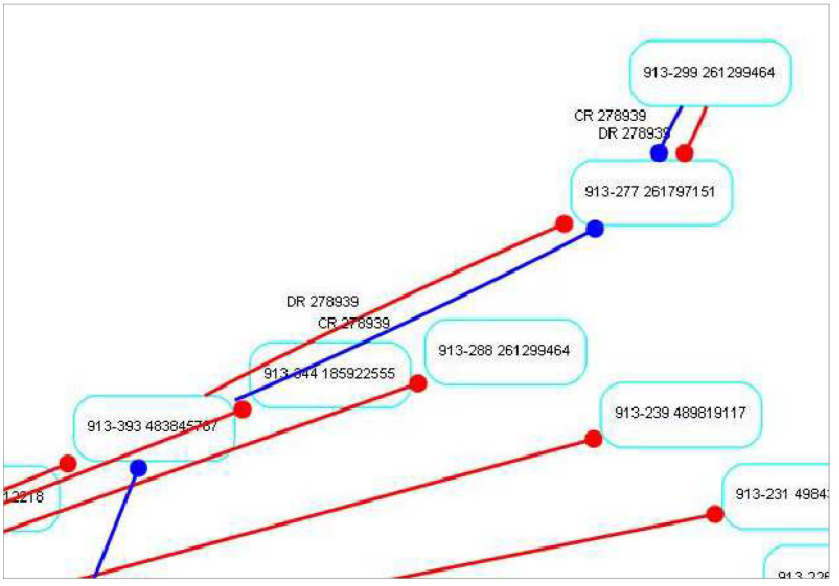


Fig. 9. a: Following the money. b: Expanded view of following the money.

4. 'Proof of concept' and validation

The objective of this study is to propose the application of link analysis to visualize banking transactions affecting an entity and thereby assist in the detection of transactions and activities potentially related to money laundering. The prototype application AML^{2}ink demonstrates how this strategy can be implemented, though it is only a 'proof of concept' tool, not a commercial application for use by auditors and other end-users. This prototype was verified/tested using sample data to determine whether it

Please cite this article as: K. Singh and P. Best, Anti-Money Laundering: Using data visualization to identify suspicious activity..., International Journal of Accounting Information Systems, https://doi.org/10.1016/j.accinf.2019.06.001

Table 2
Importance of developing/acquiring improved analytics/visualization tools for money laundering detection.

Importance of analytics/visualization tools	Mean	Variance	Median
Audit firms	5.5	0.5	5.5
Bank	7.0	0.0	7.0
Information systems auditors	5.7	1.2	6.0

meets specifications. Other methods of verification may include code examination, walkthroughs and other techniques (USDoHHS, 1997).

There has been some debate in the literature about the challenge of evaluating the usability of proposed systems (Ellis and Dix, 2006; Greenberg and Buxton, 2008; Lieberman, 2003). A proposed system should be useful to users and the user interface presumably should be usable by users (Davis, 1989). The prototype application AML^{2}ink is merely a demonstration of the application of link analysis rather than a final product. Evaluating the user interface poses a number of difficulties, including controlling for the respondent's expertise/experience, cognitive style, color preferences, and measurement scales (Lieberman, 2003). There is no attempt to evaluate the user interface in this paper.

However, the strategy of applying link analysis to money laundering detection must be validated. Validation is concerned with whether such a strategy fulfils its specific intended purpose and meets the needs of the user, i.e. the usefulness of the strategy. In this paper, validation is achieved by obtaining independent reviews from relevant organizations and professionals.

The validation process involved a presentation to the following parties to gain evidence that the strategy of applying link analysis and visualization to the detection of money laundering was an effective approach:

- Forensic teams of two large international audit firms.
- Anti-money laundering team of a national bank.
- Information systems audit professionals constituting a panel of (27) experts.

Feedback was requested on:

- The importance of developing/acquiring analytics/visualization tools to assist in the detection of suspicious transactions and potential money laundering.
- Ease of understanding of link analysis and associated visualizations.
- The functionality of such a visualization tool and effectiveness for its purpose.
- Any further suggested improvements to the concept.

Following an in-person presentation and demonstration, participants were asked respond to questions using a Likert scale of 1 to 7, with 1 being 'Strongly disagree' and 7 being 'Strongly agree'. A summary of the responses received is presented below.

4.1. Importance

Respondents recognized the importance of developing or acquiring improved analytics/visualization tools to assist in money laundering detection. This was seen as a priority area for the bank given its reporting obligations and potential penalties. Current approaches involve manual reviews of reports, running queries on tables, rule-based applications that cannot be modified, and filtering. See Table 2.

4.2. Ease of understanding

Respondents found the link analysis graphs quite comprehendible. See Table 3.

4.3. Functionality and ease of use

The totals of the debit and credit cash flows for the specified period under examination were used as annotations on the links between accounts. Respondents found that the link analysis graphs were useful for aggregation of data. See Table 4.

Respondents generally considered that the graphs contained adequate data. Comments were received about the need to access underlying data to pursue any suspicious cash flows. Further data is also needed to allow distinguishing the source of transactions,

Table 3
Ease of understanding.

Ease of understanding	Mean	Variance	Median
Audit firms	6.5	0.5	6.5
Bank	7.0	0.0	7.0
Information systems auditors	5.2	1.5	5.0

Please cite this article as: K. Singh and P. Best, Anti-Money Laundering: Using data visualization to identify suspicious activity..., International Journal of Accounting Information Systems, https://doi.org/10.1016/j.accinf.2019.06.001

Table 4
Aggregation of data.

Useful to aggregate large volumes of data	Mean	Variance	Median
Audit firms	5.5	0.5	5.5
Bank	6.0	0.0	6.0
Information systems auditors	5.4	0.9	5.0

such as automated teller machine, electronic funds transfer or Internet banking, and distinguishing the owner of accounts – individuals or businesses. See Table 5.

Respondents found that the graphs were effective for detecting the specified patterns of transaction behavior, namely:

1. High volume of transactions within a short period/Structuring cash deposits or withdrawals.
2. 'U-turn' transactions.
3. Funds transfer involving banks in 'interesting' countries.
4. Payments of loans by external parties.

Further development is necessary to incorporate the detection of additional patterns of activity, such as transactions that are inconsistent with the entity's profile, and early repayment of loans. Refer to Table 6.

Respondents found that link analysis graphs and visualizations promised increased effectiveness in detection of money laundering. See Table 7. However, considerable further development is needed to capitalize on the opportunities presented by this approach and make such tools available in a commercial form.

4.4. Further comments and issues

Respondents were asked to provided additional comments and raise further relevant issues.

The link analysis graphs were considered easy to understand. The color coding of debit and credit cash flows, with annotations on the links were considered very useful.

Respondents stressed the importance of having tools requiring little technical expertise on the part of the user. The generation of syntax for the visualization software must be automated. It also must be a simple process to import data in a specified format, and then generate the visualizations. However, some technical expertise is necessary to extend the functionality of the link analysis to detect further patterns of transaction activity and functionality not incorporated in the prototype.

The visualizations must also be able to be saved, exported and printed.

Users must be able to interrogate the graphs easily, by zooming in, and then being able to drill-down on various bases to subsets of the graphs, and also the underlying data. This is critical to allow investigation of unusual patterns.

The feedback from this validation process will be useful in revising the concept presented in this paper.

5. Discussion, contribution and limitations

Given the magnitude of money laundering globally, it is critical to detect money laundering as early as possible to limit such activity, and comply with FIU reporting obligations. Yet the nature of 'suspicious' matters is not well-defined. Accordingly, a range of tools have been developed to assist in the detection of money laundering, but each have their limitations.

This paper explores the application of data visualization to assist investigators to 'see' bank transaction data for a target entity and use their senses to visually detect specific symptoms and other unusual patterns of cash flows between accounts. The main relevant symptoms explored are:

1. High volume of transactions within a short period/Structuring cash deposits or withdrawals.
2. 'U-turn' transactions.
3. Funds transfer involving banks in 'interesting' countries.
4. Payments of loans by external parties.

This paper demonstrates the value of being able to see the data to quickly and easily detect unusual funds flows of funds involving an entity. It is expected that bank transaction graphs for entities in the same industry sector and of the same size are likely to be quite similar. It is therefore feasible to develop a classification scheme for types of entities and sizes of entities to

Table 5
Adequate data.

Contain adequate information	Mean	Variance	Median
Audit firms	6.0	0.0	6.0
Bank	5.0	0.0	5.0
Information systems auditors	5.5	1.2	5.0

Please cite this article as: K. Singh and P. Best, Anti-Money Laundering: Using data visualization to identify suspicious activity..., International Journal of Accounting Information Systems, https://doi.org/10.1016/j.accinf.2019.06.001

Table 6
Effective for exploration of data.

Enable effective exploration of data	Mean	Variance	Median
Audit firms	5.0	0.0	5.0
Bank	5.0	0.0	5.0
Information systems auditors	5.2	1.5	5.0

allow the investigator to quickly detect unusual graphs warranting further investigation. It would also be useful to detect changes in bank transaction activity for a given entity over time, i.e. detect transactions that are inconsistent with the customer's profile.

This paper contributes to the academic literature on money laundering detection using data visualization techniques. This research has certain limitations which must be acknowledged. This study advances the field of financial crime prevention by exploring and demonstrating the application of visualization techniques to assist in the identification of money laundering activity. It demonstrates the concept being proposed with currently available open-source visualization software. This data visualization application requires access to bank transaction data for the entity. An auditor of an entity can use this tool to assess the risk of money laundering by the entity. However, they are restricted to transactions involving the entity and cannot "follow the money" to determine what networks of accounts exist beyond the entity. A bank investigator, charged with detecting and reporting suspicious matters to the FIU, does not have this restriction, and can probe suspicious transaction flows across entities. They, however, though are restricted to analyzing the data held in the bank's database.

Link analysis graphs are visualized as node-link diagrams. Although node-link diagrams provide an intuitive way to represent graphs, over-lapping nodes and visual clutter quickly become a problem when graphs comprised of a large number of nodes and edges are visualized (Von Landesberger et al., 2011). In this study, graphs provide a very high level view of bank transaction flows. Larger entities may have thousands of customers and/or vendors which may generate very large and cluttered graphs. In such cases, it may be necessary for the investigator to analyze separately a number of subsets of the data in more detail. When addressing visual clutter in node-link diagrams, one may focus on the nodes, the edges, or both. In this paper the choice was to focus on the representation of the edges, since visual clutter in node-link diagrams is generally the direct result of edge congestion. Furthermore, since node positions often have a clearly defined meaning, for example, in case of nodes depicting source bank accounts, it is not always possible to modify node positions to reduce visual clutter. We therefore consider the complexity of graphs with a large number of edges to be a limitation that should be addressed in subsequent research.

Feedback from respondents raised a number of limitations of the prototype demonstration of the link analysis concept. These included the need for additional data, such as transaction source and entity type, the ability to drill-down on activity for further investigation, the ability to print or export output, and the ability to extend the range of patterns of activity that the user may wish to pursue.

6. Conclusion

Money laundering is big business. The International Monetary Fund (IMF) estimates that the aggregate level of money laundering is between 2 and 5% of the world's gross domestic product or approximately 1.5 trillion US dollars. In Australia this figure amounts to approximately $10–$15 billion per annum. Money laundering threatens global prosperity, undermines the integrity of financial systems and funds criminal activity which impacts on community safety and wellbeing. Research in AML has concentrated on: i) fighting against the crime of money laundering; ii) anti-money laundering regulation; and iii) monitoring of suspicious behavior with the help of computer technology. To combat crimes such as drug trafficking, terrorist financing and so on, anti-money laundering remains the focus of global research. Emphasis is placed on the practical aspects of improving the effectiveness of processes for combating money laundering. The ability to recognize suspicious behavior, which is dependent on the computer technology, is a key focus of research in the discipline.

This study demonstrated the feasibility of detecting money laundering activities based on visualization of monetary transactions. A prototype application (AML^{2}ink) was developed to explore visualization techniques for identifying suspicious money transactions. The intention was to provide an investigator with a series of predetermined tests or analyses that visualize a subset of transactions. The study capitalized on mechanisms that provide cognitive support for efficient identification of suspicious activities. The model was tested using data obtained from the bank transactions of a large entity and validated through feedback from professionals. This research highlights the effectiveness of using visualization to identify suspicious money laundering activities. We demonstrated the use of data visualization techniques which may enhance an investigator's ability to "see" patterns and

Table 7
Effectiveness compare with other tools.

Effective compared with other tools	Mean	Variance	Median
Audit firms	5.0	0.0	5.0
Bank	6.0	0.0	6.0
Information systems auditors	5.2	1.5	5.0

Please cite this article as: K. Singh and P. Best, Anti-Money Laundering: Using data visualization to identify suspicious activity..., International Journal of Accounting Information Systems, https://doi.org/10.1016/j.accinf.2019.06.001

efficiently target suspicious ones. The feasibility of applying low-cost, open-source software to implement such techniques was also demonstrated.

Statement of authorship

This work is not currently submitted for publication or published elsewhere.

References

ACFE, 2016. Fraud Examiners Manual International Edition.
Aigner, W., Miksch, S., Müller, W., Schumann, H., Tominski, C., 2007. Visualizing time-oriented data—a systematic view. Comput. Graph. 31 (3), 401–409.
AUSTRAC, 2011. Money Laundering in Australia 2011. Australian Transaction Reports and Analysis Centre http://www.austrac.gov.au/publications/corporate-publications-and-reports/money-laundering-australia-2011 Accessed: 18/01/2017.
AUSTRAC, 2014. Money Laundering Methodologies. AUSTRAC, Commonwealth of Australia http://www.austrac.gov.au/typologies-2008-methodologies Accessed: 30/1/2017.
AUSTRAC, 2016. AML/CTF Countermeasures. AUSTRAC, Commonwealth of Australia http://www.austrac.gov.au/businesses/obligations-and-compliance/countermeasures Accessed: 30/1/2017.
BA, 2016. Anti-Money Laundering Tutorials by Country. Edcomm Group http://bankersacademy.com/resources/free-tutorials Accessed: 23/01/2017.
Becerra-Fernandez, I., Murphy, K.E., Simon, S.J., 2000. Enterprise resource planning: integrating ERP in the business school curriculum. Commun. ACM 43 (4), 39–41.
Bolton, R.J., Hand, D.J., 2002. Statistical fraud detection: a review. Stat. Sci. 17 (3), 235–249 Institute of Mathematical Statistics.
Breiman, L., Friedman, J., Stone, C.J., Olshen, R.A., 1984. Classification and Regression Trees. CRC press.
Buchanan, B., 2004. Money laundering—a global obstacle. Res. Int. Bus. Financ. 18 (1), 115–127.
Chang, R., Ghoniem, M., Kosara, R., Ribarsky, W., Jing, Y., Suma, E., Ziemkiewicz, C., Kern, D., Sudjianto, A., 2007. WireVis: visualization of categorical, time-varying data from financial transactions. Visual Analytics Science and Technology, 2007. VAST 2007. IEEE Symposium on.
Chang, R., Lee, A., Ghoniem, M., Kosara, R., Ribarsky, W., Yang, J., Suma, E., Ziemkiewicz, C., Kern, D., Sudjianto, A., 2008. Scalable and interactive visual analysis of financial wire transactions for fraud detection. Inf. Vis. 7 (1), 63–76.
Davis, F.D., 1989. Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Q. 319–340.
DiBattista, G., 1997. Graph Drawing: 5th International Symposium, GD'97, Rome, Italy, September 18–20, 1997. Proceedings. Springer Science & Business Media.
Didimo, W., Liotta, G., Montecchiani, F., Palladino, P., 2011. An Advanced Network Visualization System for Financial Crime Detection. Pacific Visualization Symposium. 2011. *IEEE*. IEEE, PacificVis.
Didimo, W., Liotta, G., Montecchiani, F., 2014. Network visualization for financial crime detection. J. Vis. Lang. Comput. 25 (4), 433–451.
Eick, S.G., 2000. Visual discovery and analysis. IEEE Trans. Vis. Comput. Graph. 6 (1), 44–58.
Ellis, G., Dix, A., 2006. An explorative analysis of user evaluation studies in information visualisation. Proceedings of the 2006 AVI Workshop on Beyond Time and Errors: Novel Evaluation Methods for Information Visualization. ACM.
FATF, 2012. International Standards on Combating Money Laundering and The Financing of Terrorism & Proliferation Paris. France, FATF.
FATF, 2014. Money Laundering. Financial Action Task Force http://www.fatf-gafi.org/faq/moneylaundering/ Accessed: 20/01/2017.
Gao, Z., Ye, M., 2007. A framework for data mining-based anti-money laundering research. J. Money Laund. Control 10 (2), 170–179.
Goldberg, H.G., Wong, R.W., 1998. Restructuring Transactional Data for Link Analysis in the FinCEN AI System. AAAI Fall Symposium.
Greenberg, S., Buxton, B., 2008. Usability evaluation considered harmful (some of the time). Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM.
Hand, D.J., 1981. Discrimination and classification. Wiley Series in Probability and Mathematical Statistics. 1981. Wiley, Chichester.
Harvey, J., Magnusson, D., 2009. The costs of implementing the anti-money laundering regulations in Sweden. J. Money Laund. Control 12 (2), 101–112.
Hawking, P., McCarthy, B., Stein, A., 2005. Integrating ERP's second wave into higher education curriculum. PACIS 2005 Proceedings, p. 83.
Huang, M.L., Liang, J., Nguyen, Q.V., 2009. A Visualization Approach for Frauds Detection in Financial Market.
Johnson, T., Lorents, A.C., Morgan, J., Ozmun, J., 2004. A customized ERP/SAP model for business curriculum integration. J. Inf. Syst. Educ. 15 (3), 245–254.
Ko, S., Cho, I., Afzal, S., Yau, C., Chae, J., Malik, A., Beck, K., Jang, Y., Ribarsky, W., Ebert, D.S., 2016. A Survey on Visual Analysis Approaches for Financial Data. Computer Graphics Forum. Wiley Online Library.
Lieberman, H., 2003. The Tyranny of Evaluation. CHI Fringe.
Liu, J., Bier, E., Wilson, A., Guerra-Gomez, J.A., Honda, T., Sricharan, K., Gilpin, L., Davies, D., 2016. Graph analysis for detecting fraud, waste, and abuse in health-care data. (Report). AI Mag. 37 (2), 33.
Lopez-Rojas, E.A., Axelsson, S., 2012. Multi agent based simulation (mabs) of financial transactions for anti money laundering (aml). Nordic Conference on Secure IT Systems. Blekinge Institute of Technology.
Mitsilegas, V., Gilmore, B., 2007. The EU legislative framework against money laundering and terrorist finance: a critical analysis in the light of evolving global standards. Int. Comp. Law Q. 56 (01), 119–140.
Newman, L., 2007. Making the most of anti-money laundering systems. J. Superannuat. Manag. 1 (2), 31.
Pavón, J., Arroyo, M., Hassan, S., Sansores, C., 2008. Agent-based modelling and simulation for the analysis of social patterns. Pattern Recogn. Lett. 29 (8), 1039–1048.
Peslak, A.R., 2005. A twelve-step, multiple course approach to teaching enterprise resource planning. J. Inf. Syst. Educ. 16 (2), 147.
Ray, A., 2015. Emerging Solutions in Anti-Money Laundering Technology. Celent http://celent.com/reports/emerging-solutions-anti-money-laundering-technology Accessed: 29/01/2017.
Ray, A., Katkov, N., 2012. Evaluating the Enterprise-Wide Compliance Vendors: Solutions for Anti-Money Laundering and Anti-Fraud. Celent http://celent.com/reports/evaluating-enterprise-wide-compliance-vendors-solutions-anti-money-laundering-and-anti-fraud Accessed: 29/01/2017.
Salamon, T., 2011. Design of Agent-Based Models. Eva & Tomas Bruckner Publishing.
Senator, T.E., Goldberg, H.G., Wooton, J., Cottini, M.A., Khan, A.U., Klinger, C.D., Llamas, W.M., Marrone, M.P., Wong, R.W., 1995. Financial crimes enforcement network AI system (FAIS) identifying potential money laundering from reports of large cash transactions. AI Mag. 16 (4), 21.
Seo, J., Shneiderman, B., 2002. Interactively exploring hierarchical clustering results [gene identification]. Computer 35 (7), 80–86.
Singh, K., Best, P., 2016. Interactive visual analysis of anomalous accounts payable transactions in SAP enterprise systems. Manag. Audit. J. 31 (1), 35–63.
Stewart, G., Rosemann, M., 2001. Industry-oriented design of ERP-related curriculum-an Australian initiative. Bus. Process. Manag. J. 7 (3), 234–242.
Thomas, J.J., Cook, K.A., 2006. A visual analytics agenda. IEEE Comput. Graph. Appl. 26 (1), 10–13.
Tory, M., Möller, T., 2004. Human factors in visualization research. IEEE Trans. Vis. Comput. Graph. 10 (1), 72–84.
Tracy, S., Stewart, G., Boykin, R., Najm, M., Rosemann, M., Carpinetti, L., 2001. SAP Student Marketplace for the Advancement of Research and Teaching (SAP Smart). AMCIS 2001 Proceedings. p. 195.
USDoHHS, 1997. General Principles of Software Validation; Final Guidance for Industry and FDA Staff. Center for Devices and Radiological Health.
USGPO, 1970. The Currency and Foreign Transactions Reporting Act of 1970. United States Government Printing Office https://www.fincen.gov/resources/statutes-regulations/fincens-mandate-congress Accessed: 01/02/2017.
Von Landesberger, T., Kuijper, A., Schreck, T., Kohlhammer, J., Van Wijk, J.J., Fekete, J.D., Fellner, D.W., 2011. Visual analysis of large graphs: state-of-the-art and future research challenges. Comput. Graphics Forum 30 (6), 1719–1749.
Wasserman, S., Faust, K., 1994. Social Network Analysis: Methods and Applications. Cambridge university press.

Please cite this article as: K. Singh and P. Best, Anti-Money Laundering: Using data visualization to identify suspicious activity..., International Journal of Accounting Information Systems, https://doi.org/10.1016/j.accinf.2019.06.001