Knowledge-based anti-money laundering: a software agent bank application

Shijia Gao, Dongming Xu, Huaiqing Wang and Peter Green

Abstract

Purpose – Criminal elements in today's technology-driven society are using every means available at their disposal to launder the proceeds from their illegal activities. While many anti-money laundering (AML) solutions have been in place for some time within the financial community, they face the challenge to adapt to the ever-changing risk and methods in relation to money laundering (ML). This research seeks to focus on ML control and prevention, which aim to automate the monitoring and diagnosing of ML schemes in order to report suspicious activities to banks.

Design/methodology/approach – The research adopted the technology of intelligent agents to provide a more adaptive, flexible, and knowledge-based solution for AML.

Findings – Based on the analysis of monitoring, diagnosing, and reporting of ML activities occurring in electronic transactions, several types of intelligent agents are proposed and a multi-agent framework is presented for AML. Furthermore, business knowledge such as business rules and strategies are extracted from AML practice, and applied to the design of individual agents to make them act autonomously and collaboratively to fulfill the goal of ML detection.

Practical implications – The proposed multi-agent framework is a stand-alone system, which can be integrated by banks to combat ML. Although it is a uni-bank framework at present, it can be extended to multi-bank application in the future.

Originality/value – The research explores the approach of applying an intelligent agent for knowledge-based AML in an electronic transaction environment for banks. By separating business logic from the business model, such a business-rules approach can enhance the flexibility and adaptability of the agent-based AML system.

Keywords Knowledge management, Money laundering, Intelligent agents

Paper type Technical

Introduction

Since the mid-1980s, money laundering (ML) has been increasingly recognized as a significant global problem, with serious economic and social ramifications (Camdessus, 1998). Today, ML has become a key funding mechanism for international religious extremism and drug trafficking, and curtailing these illegal activities has become an important focus of governments as part of their ongoing wars on terrorism and drug abuse. Following the terrorist activity of September 11, 2001, there has been an increased focus in the United States and across the globe on the prevention of ML and terrorist financing. Increasingly, anti-money laundering (AML) systems are being implemented to combat ML. However, the traditional fixed-rule-based solutions suffer from a number of drawbacks, such as ineffective thresholds, high false positive problem, lack of pattern recognition function, and insufficient data processing capability.

In our research, we focus on ML control and prevention, which aim to automate the monitoring and diagnosing of ML schemes in order to report suspicious activities to banks. With a view to providing a knowledge-based solution for AML, we propose to apply the technology of intelligent agents to deal with the possible ML schemes in the electronic
transaction environments in a single bank. Given specific knowledge and capabilities, intelligent agents are capable of dealing with complex problems and vast amounts of information collaboratively in dynamic and unpredictable environments. Moreover, based on previous research and experimental results, some properties of intelligent agents, such as reactive and proactive behaviors, are directly applicable for tracking abnormal transactions in a systematic and goal-driven manner (Wang et al., 2002; Wang and Wang, 1997).

AML is a complex process involving many entities, where activities are delegated to a society of both autonomous and collaborative intelligent agents. Data collecting agents are responsible for collecting data of electronic transactions. Based on such data, monitoring agents may keep track on the transaction processes. When a possible ML scheme is detected, a diagnosing agent will be initiated and attempt to identify the problems. According to the output from the diagnosing agent, a reporting agent will report to the appropriate personnel. Our proposed multi-agent framework is a stand-alone system, which is integrated with the bank systems. The software agents only capture the transaction data from the bank operational system, and will not interrupt normal banking operations.

In order to achieve a knowledge-level resolution, intelligent agents are developed with specific knowledge such as business rules and business strategies to reason about business actions for ML. Business rules are extracted from AML practice, and applied to the design of individual agents to make them act autonomously to fulfill the organizational goals. By separating business logic from the business model, such a “business rules” approach can enhance the flexibility and adaptability of our agent-based AML solution.

The remainder of the paper is organized as follows. The next section briefly reviews the relevant literature on ML, AML, AML systems, and intelligent agent theory. Then the approach of applying intelligent agents into knowledge-based AML is investigated. Following this approach, we develop a multi-agent system framework for AML. The final section addresses our contribution as well as the future work.

Background

Money laundering and anti-money laundering

Money laundering (ML) is a term usually used to describe the ways in which criminals process illegal or “dirty” money derived from the proceeds of any illegal activity (e.g. the proceeds of drug-dealing, human trafficking, fraud, embezzlement, insider trading, bribery, theft or tax evasion) through a succession of transfers and deals until the source of illegally acquired funds is obscured and the money takes on the appearance of legitimate or “clean” funds or assets (HM Treasury, 2004). ML is a diverse and often complex process that need not involve cash transactions. ML basically involves three independent steps that can occur simultaneously (IFAC, 2002):

1. **Placement** – the process of transferring the proceeds from illegal activities into the financial system in such a manner as to avoid detection by financial institutions and government authorities.
2. **Layering** – the process of generating a series or layers of transactions to distance the proceeds from their illegal source and obscure the audit trail.
3. **Integration** – the unnoticed reinsertion of successfully laundered, untraceable proceeds into an economy.

The International Monetary Fund (IMF) estimates that the aggregate size of ML in the world could be somewhere between 2 and 5 percent of global gross domestic product (GDP) (FATF, 2008b). According to Celent Communications (2002), the amount of illicit funds traveling through ML channels is estimated to grow at an annual rate of 2.7 percent. However, the full magnitude of the problem is still not known with any certainty.

Recent years have witnessed a growing number of highly publicized money laundering scandals involving major international providers of diversified financial services and their correspondents in “off-shore” jurisdictions, such as Russia, other former Soviet Republics,
Latin America and the Caribbean (IFAC, 2002). In response, governments and legal authorities in various jurisdictions have issued an accelerated level of pronouncements and taken other enforcement steps focused on combating ML and related financial crime. In 1989, the Group of Seven Industrial Democracies (G-7) created a global ML watchdog organization called the Financial Action Task Force (FATF). In 1990, the FATF issued its first annual report, containing its FATF 40 Recommendations, which are a most important set of international AML standards and they have been a substantial motivation in facilitating government AML initiatives. An important element and theme of the FATF 40 Recommendations is the KnowYourCustomer (KYC) or enhanced due diligence principles. KYC guidelines require or recommend developing a keen understanding, through appropriate due diligence, of whom the true beneficial owners and parties to transactions are, the source and intended use of funds and the appropriateness and reasonableness of the business activity and pattern of transactions in the context of business (IFAC, 2002). In addition, FATF also recommended implementing Suspicious Activity Reporting (SAR) models, record keeping, and AML controls as part of overall AML regimes.

However, there are as many methods to launder money as the imagination allows, and the ML schemes being used are becoming increasingly sophisticated and complex as technology advances (CICA, 2004). Although KYC and SAR are spreading across the globe in forms ranging from best practice, “soft law” and even hard law, the money launderers are forced to change their methods to some degree. ML is becoming increasingly difficult to detect. In an effort to detect potential ML schemes, many financial institutions have deployed AML detection solutions and enterprise-wide procedural programs. These solutions work by establishing fixed rule-based thresholds by analyzing how certain established usage scenarios comply within those boundaries. Most financial institutions will establish a threshold based on a set monetary value for each transaction and detecting specific ML patterns and user scenarios that breached those thresholds. The shortcomings associated with these solutions are summarized as follows:

- They possessed an inherent inability to detect ML schemes of smaller amounts that may come in under a defined threshold limit. For instance, in investigating the financing behind 9/11 events, it was discovered that the terrorists had made frequent transactions of small sums that were below the usual cash transaction reporting thresholds (Moorman, 2004).
- The problem of false positive, which means there are transactions over a set limit that are marked as suspicious but in fact they do not represent any existing identified risk to the institution, was prevalent.
- There were no learning or generalization abilities. Although those fixed-rule-based systems have some pattern recognition capabilities, they cannot learn or generalize new patterns and they can only match patterns that they already know. As new ML schemes developed, many of these solutions were unable to adapt to uncover them, providing criminals with new avenues to circumvent detection and the law.
- There was insufficient and inconsistent checking. Transaction volumes in the financial instructions are very large and the sizes are increasing (Wicks, 2001). The current systems do not have enough capabilities to check every transaction in a comprehensive and consistent manner. Too few checks are costly in terms of undetected ML activities.
ML detection and prevention are notoriously difficult (Wicks, 2001; Horobin, 2001). Due to the complex nature of financial products, services, and ML itself, ML is dynamic and it adapts over time according to changing conditions. Patterns of behavior change as money launderers become aware of the techniques being used to combat them. Given such behavior, business knowledge about AML extracted from current up-to-date AML practices will play a critical role in achieving automation of AML. Fixed rules can be applied to mitigate against certain extreme behaviors and to enforce defined regulations. However, embedding static rule-based systems into electronic transaction environments does not provide adequate safeguards to combat ML. KPMG (Byrne, 2005) suggested a risk-based approach is the only way to identify potential ML transactions. It is therefore vital to tackle the problem using a risk-based approach, as well as the technology that adapts, so that systems can be dynamic in the way that they respond to changes in the patterns of ML.

**Intelligent agents**

The development of intelligent agents (IAs) and multi-agent systems (MASs) has recently gained popularity among IS researchers (Franklin and Graesser, 1997; Jennings, 2000). Although there is no universally accepted definition of the term “agent,” and indeed there is a good deal of ongoing debate and controversy on this very subject, the central point of agents is that they are autonomous: capable of acting independently, exhibiting control over their internal state. Wooldridge and Jennings (1995) suggest a precise description of agents; one that may be widely adopted in artificial intelligence communities as well as general computing areas. An agent is defined as a computer system that is situated in some environment, and is capable of autonomous action in that environment in order to meet its design objectives (Wooldridge and Jennings, 1995; Wooldridge, 2002). Furthermore, agents are able to act without the intervention of humans or other systems: they have control both over their own internal state, and over their behavior (Wooldridge, 1999). An intelligent agent (IA) is one that is capable of flexible autonomous action in order to meet its design objectives, where flexibility includes properties such as autonomy, social capability, reactivity, and proactivity (Wooldridge and Jennings, 1995; Wooldridge, 2002). A generic agent has a set of goals (intentions), certain capabilities to perform tasks, and some knowledge (or beliefs) about its environment. To achieve its goals, an agent needs to use its knowledge to reason about its environment and the behaviors of other agents, to generate plans and to execute these plans. A MAS consists of a group of agents, interacting with one another to collectively achieve their goals. By absorbing other agents’ knowledge and capabilities, agents can overcome their inherent bounds of intelligence (Jennings and Wooldridge, 1998).

The concept of IAs has increasingly become important in artificial intelligence, computer science, and e-commerce. In recent years, there has been considerable interest in the design of a distributed, intelligent society of agents capable of dealing with complex problems and vast amounts of information collaboratively. Since agent technology provides flexible, distributed, and intelligent solutions for business process management, researchers have proposed to design and develop numerous IA-based systems to support business processes management in dynamic and unpredictable environment (Jennings et al., 2000; Zhuge, 2003). It is proposed to use IAs for business data monitoring, in which IAs are deployed with specific domain knowledge, and they can intervene on behalf of business analysts by being able to perform limitless, error-free routine calculations and interpretation rapidly to the precise requirements of business managers (Wang et al., 2002; Wang and Wang, 1997).

Many examples of agent-based research related to knowledge management (KM) have been developed (Jennings and Wooldridge, 1996; Turban and Aronson, 1998; Shen et al., 2001). For example, Elofson et al. (1997) proposed a community of IAs to facilitate knowledge sharing in an environmental scanning process. Wu (2001) proposed the use of IAs for KM, which focused on the coordination of multi-agent supply chains and auctions. Aguire et al. (2001) proposed a multi-agent-based knowledge network. Roda et al. (2003) proposed an agent-based system designed to support the adoption of knowledge sharing practices within communities. Li et al. (2006) proposed an agent-based buddy-finding system.
methodology, and tested it in a context involving sharing musical-knowledge. When intelligent agents are applied in knowledge-based systems, they are more capable of reactive and proactive behavior, and they are equipped with social ability in the sense of cooperation, coordination and negotiation. To be more useful in complex real-world domains, the agents are flexible in terms of their problem-solving skills, communication capabilities, and utilization of internal knowledge and data.

ML is a complex and ill-structured problem. According to Bui and Lee (1999), a multi-agent framework is necessary to support a comprehensive knowledge management system faced with uncertainty, complexity, and ill-structured problems. Therefore, IA technology is a suitable approach to an intelligent AML control architecture. IAs are able to analyze all transactions and accounts, and also have corporate authority to access any data that might be relevant. The reactive behavior of agents enables them to perceive the suspicious behavior occurring in the transactions and respond in a timely fashion. The proactive behavior enables agents to uncover wrongdoing by finding suspicious patterns of behavior hidden within voluminous data, and to separate those problem patterns from normal everyday events.

**IA-supported knowledge-based anti-money laundering**

As noted before, IAs equipped with specific domain knowledge and their properties of autonomy, reactivity, proactivity, and social ability are well suited to business monitoring applications that perform limitless, error-free routine calculations and interpretation rapidly to the precise requirements of business managers. Here, we will illustrate how to apply IAs into the electronic environment to realize a knowledge-based solution for AML.

**Knowledge-based intelligent agents**

In a multi-agent system, software agents are proposed to perform some tasks autonomously on the user's behalf, which means that they can act independently of humans. It is essential to design a set of autonomous types of behaviors for the agent class, including reactive, proactive, and cooperative behavior. Both autonomous and semi-autonomous agents rely on knowledge or data which is the agent's perception or awareness of its environment. Various kinds of intelligence are supported by this kind of data. It usually concerns rules, which are the user's expression of preference of policies followed by the agent to complete its task (Caglayan and Harrison, 1997). In order to fulfill the organizational goals and objectives, business rules to conduct business activities play an essential role in governing peoples' behavior. These business rules may form an important part of the knowledge base for software agents to perform delegated tasks on the user's behalf (Liu et al., 2001). Once the rules are understood, captured and represented in the form of logic, they will serve as a basis for building intelligent agents to perform rational activities.

Business rules are a formal expression of knowledge or preference. If-then rules have become the most popular form of declarative knowledge representation used in artificial intelligence applications (Giarratano and Riley, 1998). Knowledge represented as if-then rules is easily understandable, in contrast to knowledge represented in predicate logic. Rules are declarations of the type if <condition> then <action>, that means if the <condition> is true then the <action> should be executed. The execution control of these rules is done through a separate inference mechanism which tests each rule against existing facts in a working memory, generating new facts in it – or executing some procedural code associated with the rule – when a matching occurs. This process is

"The reactive behavior of intelligent agents enables them to perceive the suspicious behavior occurring in the transactions and respond in a timely fashion."
repeated recursively until a specific goal is reached or there are not any more rules in the rule database that can be triggered.

**Business rules capture**

Rules statements are a key element in defining the intentions and the needs of the business, as well as an important type of presentation of business knowledge. In this research, we capture the business logic in the form of rules from AML practice, such as from the FATF 40 Recommendations, government legislation documents, financial institution reports, etc. These AML rules can be used by intelligent agents to monitor, diagnose, and report possible ML schemes. Two example rules for ML monitoring are:

1. IF a customer OR a person publicly associated with the customer, has a questionable background OR is on any of the Sanctions Lists, THEN this customer and associated transactions are recorded as possible money laundering.

2. IF a customer’s account has wire transfers that have no apparent business purpose to or from a country identified as a high money laundering risk or a bank secrecy or “tax haven” THEN this customer and associated transactions are recorded as possible money laundering.

**Business strategies in business rules**

Business rules specify a series of clear statements about the logic underlying a business, each of which represents a small unit of knowledge. At a high level, business rules could be classified under one or more concerns, such as controlling workflow, reducing business risk, making efficient use of resources and improve customer service (Morgan, 2002). Accordingly, while designing rules for intelligent agents to perform AML activities, we may not merely focus on those rules to control monitoring, diagnosing and reporting activities, but also consider some business strategies to improve the efficiency of AML. For instance, while the transaction monitoring agent executes validation on transaction details, it is not quite efficient to go over all the components in each transaction to ensure that details are correct before being communicated externally. Instead, this monitoring agent may focus on the validation of several critical components such as client ID, transaction type, transaction date, value data, counter party, and etc. Furthermore, sometimes special types of transactions that take specific care of that situation are more likely to be a potential ML scheme. We may consider providing additional attention to some kinds of transactions based on a risk-based approach such as:

- transactions with cash value at or above a certain figure (i.e. large amount transaction);
- transactions with a special transaction type (i.e. high-risk transaction types defined by FATF, such as wire transfer);
- transactions with a special counter party (i.e. high-risk customers and business entities, like casino owner or somebody from high-risk countries); and
- transactions of certain frequencies (i.e. high frequency transactions suggest high-risk customer behavior).

**Dynamic business rules**

Most agents rely on knowledge about the environment that has been built by the designer. Furthermore, due to the increased complexity and uncertainty in today’s environment of organizations and markets, the agent needs to be able to adapt to the dynamic world. In dynamic-rule-based agents, it usually implies the agent’s ability to automatically modify the rule base in some way, so-called dynamic business rules. Agents can derive rules from the user and environment, and then incorporate the new rules into their behaviors. Such agents need access to historical databases or logs of events, which can be analyzed for emerging trends or correlations. For example, some ML activities are related to one specific counter party or one specific transaction type. The transaction monitoring agent may find this kind of correlation after data analysis on ML history, and accordingly adjust its monitoring policy to pay more attention to the transactions related to this specific counter party or transaction type.
Multi-agent framework for anti-money laundering

After the above discussion on the application of IAs for the knowledge-based AML solution, we now develop a multi-agent framework of AML in electronic transaction environments for banks.

Deployment of intelligent agents

Before applying multi-agent technology into the AML solution, we need to decompose the process of AML into several autonomous stages, in which each agent is delegated a particular task to exhibit its goal-oriented and reactive behavior, and to cooperate with other agents to pursue their goals. The process of AML usually consists of the phases of data collecting, ML risk monitoring, behavior diagnosing, and suspicious activity reporting (FATF, 2008a) (see Figure 1).

Data collecting involves internal and external data collection. ML monitoring is composed of client profile assessment (complying with FATF’s customer identification) and a transaction risk measurement. Accordingly, the taxonomy of intelligent agents required for AML is outlined in Figure 2, in which several intelligent agent classes are applied to provide a set of AML functionalities for existing financial institutions. The requirements of the stages of the AML process (as outlined in Figure 1) are clearly evident in the categories of agents specified in the taxonomy of Figure 2. For example, the Data Collecting Agent is specialized

Figure 1 Anti-money laundering process

Figure 2 Agent hierarchy for anti-money laundering
into an internal data collecting agent and an External Data Collecting agent. The details of these agents are described in the following subsection.

**Multi-agent system architecture**

The value of any AML solution has to be based on its ability to uncover suspicious financial activities by identifying the specific individuals or organizations that may be involved (Menon and Kumar, 2005). However, given the complex nature of ML prevention controls, an automated solution cannot attach suspicion to any activity detected – it can only detect activity worthy of analyst interpretation. Human ML expertise is required to determine if that activity is suspicious and worthy of reporting. Therefore, the optimum way to implement ML prevention controls is as a synthesis of human expertise and automated intelligence. In this research, the automated system performs the detection work, raising alerts for transactions deemed suspicious (in terms of the suspicious activity report) to the humans concerned. The human analysts perform investigations into the cases that are raised.

There are two ways to develop the AML solution:

1. we can reengineer existing banking systems to support AML functions; or
2. we can develop an independent AML system to link with the existing applications through which all client and transaction data would pass during its lifecycle.

Our work is to use fundamentally the second approach by employing a financial institution’s internal resources to build software capabilities that can interact with their existing legacy systems. There are three reasons for choosing an add-on AML approach. First, our proposed AML solution can capture the data from the banking system without any interruption to normal banking operations. Second, our proposed AML solution is a stand-alone system. It can integrate flexibly to any banking legacy systems. Third, reengineering an existing banking system to support AML functions is a too complex, time-consuming, and costly. Therefore, it is more feasible to choose an add-on AML solution approach.

Based on the analysis above, the AML process diagram (see Figure 1), and the deployment of intelligent agents in the previous subsection (see Figure 2), we outline the framework of our multi-agent based AML system in Figure 3, in which a society of intelligent agents is applied to provide a set of functionalities for AML in electronic transactions.

The agents are distributed in the departments of banks involved in AML; they communicate with each other through the Internet. All of these agents work autonomously and collaboratively in the multi-agent environment. Each agent focuses on its particular task such as data collecting, monitoring, diagnosing, and reporting without inventions from outside. By drawing on other agents’ knowledge and capabilities, agents can overcome their inherent bounds of intelligence and work collaboratively to pursue their goals.

The behavior of an agent is based on an internal model of the agent consisting of a knowledge base, operational facilities, and a correspondence between the external application domains. Generally, development of an agent considers an agent knowledge base, its operational facilities and its external interface. Knowledge is required by each agent to perform its internal and external activities. It consists of knowledge for particular tasks, resource status information, information about other agents, and the like. The operational facilities execute different functions and provide collaboration with other agents;
they are the central control and action part of an agent. A dynamic rule engine is usually an important operational facility, which provides a means for applying simple, dynamic-rules-based reasoning to emergence of new facts in the agent's world and for using this reasoning capability to decide what the agent should do next. The external interface envelops an agent and provides access to it via a well-defined interface, and it is also the primary conduit for communication between agents.

The User Agent acts as an effective bridge between the user and the computer. It can make the human-computer interface more intuitive and encourage types of interactions that might be difficult to evoke with a conventional interface. In our system, this agent enables users to view the current state of the financial transactions and ML monitoring, diagnosing, and reporting processes and allows them to convey their own judgments, opinions, and arguments relative to ML detection to the rest of the bank. The agent also enables the corresponding users to issue requests to the other agents in the system. The Repository Agent plays an important role in our approach. Although there is no need for centralized storage of all knowledge regarding AML, there could be one consistent knowledge repository that maintains and integrates all information related to the monitoring and analysis tasks. In this way, the various agents that make up the system can exchange knowledge regarding entities involved and deal with ML in a collaborative manner. In our approach, the Repository Agent may contain and manage several kind of information, e.g., real time banking transaction data for monitoring, risk reports for further diagnosing, reports for suspicious activities that have been detected, etc. Such shared information about banking transactions and suspicious activities may form an important base for agents' collaboration in banking AML.

The Data Collecting Agents enable the system to collect data internally and externally. In particular, the Internal Data Collecting Agent is in charge of acquiring real-time data from existing banking systems for the client profile assessment, transaction risk measurement, and further behavior diagnosis and reporting. Several kinds of data related to possible ML schemes are required for ML prevention controls, such as client profiles, financial transaction details, account reference data, client reference data, historical statistics, etc. On the other hand, the External Data Collecting Agent retrieves open data from ML watchdog agencies, national government, and other authorities. The data includes international standards, official thresholds, watch list, legislations, etc.
Two kinds of Monitoring Agents include Client Profile Monitoring Agent and Transaction Monitoring Agent, are proposed in our system to monitor potential ML schemes on a client-by-client, transaction-by-transaction basis. Both agents comply with the global-accepted core policy for effective ML controls – KYC (KnowYourCustomer). The Client Profile Monitoring Agent is to assess a wide variety of detailed information relating to the client’s account, typically collected at the time that the account is opened. The agent provides a single view of the client profile incorporating all of the various financial relationships that the account has an affiliation with. The types of analytical activities that are part of the agent client profiling processes include, but are not limited to: watch list name screening, high risk country alerting, financial source or channels, business relationship, and political affiliation. Each client is classified into different risk profiles. And based on the client risk classification, the agent determines the frequency and the intensity of monitoring. The Transaction Monitoring Agent is to identify transactions that pose the greatest risk for potential ML activities. Transaction determined to be of a higher risk can vary from organization to organization based on their product-type lines and types of business. For instance, the risk associated with transactions from a bank would be different from those associated with an insurance agency or a securities firm. In general, the transaction risk behavior include, but are not limited to (Menon and Kuman, 2005): rapid movement of funds in or out of the account, sudden activity into a previously dormant account, frequent changes to an account, recurring transactions, hidden account relations, offsetting trades, settlement and/or standing instructions of an account, the movement of funds without a corresponding trade, and the deposit of excess collateral into an account.

Normally, if a questionable client profile or an unusual transaction is captured by the Monitoring Agents, a risk report will be issued and sent to the Diagnosing Agent for further investigation. However, an emergent suspicious activity report (SAR) could be issued to be reported to the user for instant action. When receiving the risk reports from Monitoring Agents, the Diagnosing Agent will start its diagnosing process to investigate the complex behavior that is commonly associated with ML schemes. This agent may conduct analysis on risk reports from Monitoring Agents and request any additional information if necessary to examine the cases. The agent allows financial institutions to detect wrongdoing by finding suspicious patterns of behavior that may be hidden behind large volumes of financial data.

When the Diagnosing Agent identifies unusual or suspicious behavior, a suspicious activity report (SAR) will be automatically produced and sent to the Reporting Agent. Figure 4 shows a screenshot of a SAR. Then the Reporting Agent will present and communicate a potential ML alert to the appropriate compliance personnel through the User Agent for case management investigation and action. Alternatively the Reporting Agent will automate or take a specific course of action, for example, interfering with standard operations to block a particular suspicious transaction. Cases for investigation are filtered and prioritized based on the severity of the alert. The Reporting Agent is able to support the business process to assist with suspicious case investigation. It does this by providing evidence of client activity and information, ensuring the case officer has all of the relevant customer intelligence at hand. If necessary, additional information is requested from Diagnosing Agent. This allows them to make a fact based decision and it also demonstrates regulatory due diligence in the process. The Reporting Agent also facilitates combining the automatically generated alerts with suspect manual reports, to build the case for investigation. The reporting facilities within the Reporting Agent provide a complete tracking system and audit trail for managing actions in response to detected events or suspicious behavior. Such comprehensive reporting allows the financial institutions to demonstrate compliance to the AML rules and adherence to the regulatory requirements.

Moreover, the Monitoring Agents run scheduled scans for all accounts and transactions by using the data-mining techniques (property of agent’s proactivity). The Monitoring Agents will monitor the complex suspicious customer activity and rank the customers according to degree of suspicion of ML. After the unknown patterns are understood, they are sent to the Diagnosing Agent to identify suspicious events that build over time, and to separate them from everyday events and transactions in order to target the offending behavior. In addition,
when the previous unknown complex ML schemes become known ML schemes, they will be stored in the Repository Agent for future monitoring and diagnosing.

Conclusion

This paper explores the approach of applying intelligent agents for knowledge-based AML in electronic transaction environment. A conceptual framework for a multi-agent system based on AML process is developed, in which various classes of intelligent agents are proposed to provide a set of functionalities for AML in electronic transaction environment for banks. In order to make software agents act autonomously and collaboratively to fulfill the organizational goals and objectives, business knowledge such as business rules and business strategies are extracted from AML practice, and applied to the design of individual agents. A generic structure for rule-based agents is also outlined, in which business logic is separated from business model with a view to enhance the flexibility and adaptability of such kind of rule-based system.

Following this framework, we have started to build a prototype in Java so that agents can run on heterogeneous platforms and make use of lightweight applets as temporary agents. After the implementation, a number of ML cases will be built based on the real-world cases for prototype evaluation purpose. Evaluation of the prototype consists of two parts. First, semi-structured interviews will be conducted with the AML experts to collect their feedback on the prototype. Their feedback will be used to refine the prototype. Second, a laboratory experiment(s) will be conducted to evaluate the prototype effectiveness in terms of AML decision support.

Our proposed system focuses on internal data monitoring in one bank, which lacks the capability to monitor multi-bank transactions. ML is becoming more and more complex, which includes multiple banks, financial institutions, countries, etc. How to share data and knowledge between these multiple entities is becoming an important issue. Our future work will explore such multi-entity involved AML solution.
References


(The) CICA (The Canada Institute of Chartered Accountants) (2004), Canada’s Anti-Money Laundering & Anti-Terrorist Financing Requirements, February, Toronto.


**Corresponding author**

Shijia Gao can be contacted at: c.gao@business.uq.edu.au