International Conference on Business Management & Information Systems, 2013

Computer-aided Financial Fraud Detection: Promise and Applicability in Monitoring Financial Transaction Fraud

Georgios Samakovitis and Stelios Kapetanakis[1]

School of Computing and Mathematical Sciences, University of Greenwich, London, United Kingdom
[1] School of Computing, Engineering and Mathematics, University of Brighton, Brighton, United Kingdom
E-mail: g.samakovitis@gre.ac.uk; s.kapetanakis@brighton.ac.uk

ABSTRACT

Anti-money Laundering (AML) and Financial Fraud Detection (FFD) have been receiving increasing attention in the past few years, especially in light of the global financial crisis. Closer systems integration and a number of latest steep technological developments in areas like Big Data; High Frequency Trading; e-payments; and mobile payment systems, to name a few, are now promising enhanced risk management through superior decision support for the global financial industry. At the same time, however, resident regulatory frameworks, national and international, appear to lack the connectivity and flexibility required to support integrated AML and FFD approaches. This is strongly testified by the disparate technological approaches to FFD across different Financial Institutions and their reluctance to share practice within the industry.

Focusing on Financial Transaction Fraud, this paper draws on the authors' past research work which presented a prototype system that uses a workflow approach to identify abnormal financial transactions and applies Artificial Intelligence for classification. That work has shown successful applicability at short scale experiments, limited by the wide concern that information sharing should be achieved within the broader sector in order to achieve improved results. Drawing from there, this paper proposes that extending that approach across transaction infrastructure will deliver higher quality intelligent monitoring against Financial Transaction Fraud.

Following from that, we argue that the necessary technological maturity does exist to support full-scale operable FFD systems working on large disparate datasets. We then discuss the evidence in favour of the view that such systems can only be realised in the presence of wider regulatory consensus. There is, therefore, the need for a framework within which the technical infrastructure, business architecture and regulatory rules will harness that technological capability to deliver superior fraud prevention.

The paper first reviews computer-aided techniques and approaches for FFD available to the financial sector and discusses the business value of their application. It then addresses the main impediments for their full-scale applicability and uses an analytical framework for assessing their significance, in technological, business-specific and regulatory terms. A brief account of the authors' workflow-based approach is then provided and its capabilities are outlined.

In light of the above analysis, the paper proposes a techno-economic framework that will facilitate delivery of unified knowledge from large and disparate data sets of financial transactions. That, we propose, will augment fraud reduction capabilities and contribute to significantly lower associated costs.

Keywords: Financial fraud detection, Anti-money laundering, Transaction monitoring, Artificial intelligence

INTRODUCTION

Current consensus in Industry and Public Policy cycles is that Financial Fraud is, today more than ever, an acute problem facing the Financial Services Sector globally. Not least because of its impact on banks' revenue and trust profile, the detection of Financial Fraud (henceforth FFD) has been moving up the agendas of Financial Services firms, regulatory authorities and technology providers alike [23, 24].

On the one hand, Financial Institutions are driven by compliance requirements under significant regulatory pressure (as testified by the recent fines imposed on major banks on grounds of non-compliance [23]), as well as pressure coming from their shareholder for cost reduction, operational efficiency and risk management [3, 4]. On the other hand, national and international agendas on crime prevention and security [23, 14, 24] begin to synch heavily with regulators' interests in seeking further linkages between Financial Fraud and Money Laundering (ML), not least because of the former is now becoming a well-recognised source for the latter, while, in turn, ML is widely identified as the key vehicle for Terrorist Financing [25, 26]. On top of that, new technology-driven payment and remittance vehicles such as Bitcoins, e-currencies, or other means of exchange (conventional or less-so) and their potential linkage to activities such as Piracy at Sea or wider models of terrorist financing [1, 3] are all changing the Conventional Wisdom as to what Financial Fraud constitutes and how it may be accommodated by money exchange platforms within or outside the existing banking system. On the same grounds, it is argued that the linkage between FF and ML offers ample economic justification for organised crime to use 'clever' forms of Financial Fraud as an attractive vehicle [11].

Despite that pronounced importance, a unified technological approach to FFD does not appear to exist amongst practitioners in the Financial Services; in a direct analogy to the Paradox of Practice [7] we contend that despite the existence of suitable mature technologies and techniques which promise feasible intelligent monitoring at larger-than-ever scale, intelligent FFD is far from reality; conversely, adopted solutions are largely rule-based, hence not making use of learning capabilities of available algorithms [12, 13].

In this work, we start from reviewing the current state of play in intelligent approaches for automated transaction monitoring and then briefly discuss the authors' current contribution to the field [9, 10], which emphasises on scalability and the potential for handling large and diverse data sets. Drawing on these particular attributes, we discuss the value of the *collective intelligence* that can be leveraged using that approach through shared infrastructure. That, in turn, leads to the contention that a suitable co-ordination of technical and policy actions is required to fully enhance the performance of related Decision Support Systems and deliver the technological potential of Intelligent Financial Fraud Detection and Deterrence. We ultimately propose how this co-ordination may be supported with the use of an Actor-based analytical framework [7]. We believe that this stakeholder-centred approach will help tune-in the contribution of different actors in redesigning anti-fraud processes and taking more informed practical steps in the future.

LITERATURE REVIEW

Financial Fraud has increasingly become an acute problem across the global industry. Accounting for annual losses of £38bn in 2011 in the UK alone, the cost of fraud has risen to £73bn in 2012 [17, 14, 18]. In global terms, in 2009 only fraud-related losses reached $2,75trn [19], reflecting an approximate 4.5% of total expenditure [20]. Given its economic impact, the problem of Financial Fraud provides a significant scope for Decision Support optimisation. Because of the nature of electronic money transfer, accurate labelling of financial transactions as genuine or fraudulent is paramount in ensuring customer trust, especially in light of the prevalence of user-driven electronic banking [7]. The authors' previous work [15] suggested that misidentified fraud instances (false positives) are equally detrimental to customer trust as are unidentified instances of original fraud (false negatives). This adds significantly to the precision requirements of FFD processes and systems, and partly hints to the current reluctance to adopt unified industry-wide approaches.

Despite the aforementioned reported economic importance of fraud [17, 14, 18, 19], no explicit FFD framework is widely recommended in the literature. Transaction-handling entities (such as banks and financial services providers) address the problem at the firm level, while authorities and independent bodies (such as the FSA, SOCA, BAI, SFO, NFA, FCA, among others) only address cases of large-impact financial fraud, typically linked to wider criminal activity [17, 18]. Occasionally Financial Institutions are seen to use bespoke rule-based monitoring systems to address the problem [21, 22]; however, the main approach to fraud involving small amounts is mainly addressed through fraud protection insurance. Indications therefore exist that no robust and reliable Decision Support is available to facilitate fraud identification across the board.

Useful contributions to classifying the literature on FFD types and existing approaches in Data Mining & Artificial Intelligence to address Financial Fraud were provided by Ngai et al. [16] where techniques such as Clustering, Classification, Prediction, Outlier Detection, Regression and Visualisation approaches, among others, populate the wider Computer Science literature.

AN INTELLIGENT FFD APPROACH

Financial organisations choose to deal individually with the problem of financial fraud since most of the information derives from their clients' data. Therefore, an approach to tackle this problem could be to collect data anonymously from various sources. Such a policy should ensure firstly the integrity/anonymity of data as well as be able to deal with disperse and multivariate data origin sources. For the latter the current technological progress in the area of persistence could be useful if been subject to a number of modifications. The latest advances tackle the speed, volume and velocity limitations of traditional relational SQL databases [28] and work with unstructured schemas, close to the natural format of the data source. The current operational spectrum can show a number of No-SQL [27, 28] solutions that can deal effectively with large and very large volumes of data, both in acceptable time windows and multivariate in terms of the production sources. Advances such as the effective slicing and dicing of Map – Reduce in accordance with Business Intelligence Cube solutions can be rather effective in working with diverse datasets. Additionally, the enforcement of distributed and aggregated solutions leads to more scalable approaches that seem centralised-free and scalable enough to meet the current needs of the financial sector.

Such an approach if adopted by the Financial Services Sector and Financial authorities could lead to transaction monitoring at national and potentially international level, defining a different perspective in fraud identification. FFD can largely benefit from that since a new definition is given in transaction transparency and trace control regardless of the data origin while keeping vendor and client anonymity at the same time.

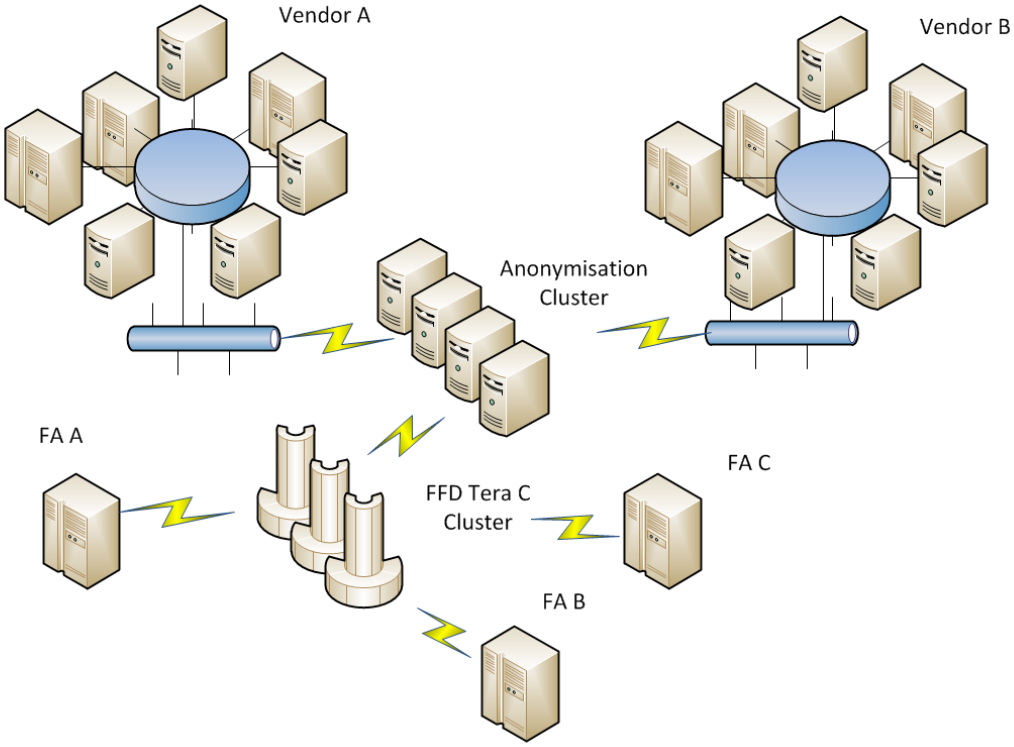

Fig. 1: FIs along with FAs Connected via an Anonymity Transaction Network for the Monitoring of the Latter

Figure 1 illustrates how an imposed layer of anonymity among FI data could lead to effective monitoring from FAs at scalable level. Such an approach could be suggested at preliminary level in order to test its efficiency, enhanced on demand according to a present agenda and enforced subject to results. Previous research of the authors [9, 15] has shown that business processes have several layers that could be used for monitoring purposes. Starting from the workflow orchestration, intelligent monitoring can be enhanced with the rule set needed for latter pattern extraction. Moving to the execution of workflow, there can be several levels of abstraction that reveal resemblance among transactions, thus improving fraud identification. The constant retro-feed from FIs can lead to new pattern recognition(s) which will be re-used in the creation of an ideal pattern pool for general reference.

THE ANALYTICAL FRAMEWORK: SEEKING 'COLLECTIVE INTELLIGENCE' WITH THE USE OF AN ACTOR-BASED APPROACH

In the previous section, we demonstrated a technological approach that is suited to augment Decision Support for identifying Financial Fraud through intelligent monitoring of transaction streams, viewed as workflows. While the system in its full scale implementation is yet to be delivered, its successful proof-of-concept demonstrated fully functionality and ability to aggregate disparate and heterogeneous data sources. Technical functionality is therefore available to support the desired *collective intelligence*.

Drawing from that, we now look further into how that technical feasibility can realistically be accommodated by the actual operational frameworks. The reasons why this is a challenge, are primarily related to:

1. The sensitive nature of transaction data which renders the use of open platforms unusable for their sharing;
2. Overlapping and often conflicting jurisdictions of financial institutions, regulators and other relevant authorities on the data to be used in the system;
3. The fact that existing infrastructure for handling FF is largely proprietary and thus tailored to individual needs and tied to the legacy systems of each financial institution;
4. The conflicting interests of involved parties in adopting a commonly acceptable FFD platform or approach;
5. Ultimately, the debate as to whether there is a need for establishing ownership of the resulting *collective intelligence* and, if so, the question as to which entity (regulator, national or supra-national authority, business or public consortium etc.) would own that intelligence.

The need for using a systematic analysis to place the problem in the context described above is dealt with through the use of the Actor-based Informed Grounded Theory [7, 8] an approach that was developed to make sense of how technological investment decisions are performed in UK banks.

The Actor-based Informed Grounded Theory argues that the problem of FFD has the shape and expression it currently has, *not in spite of but because of* the Actors who have addressed it in the past as well as now. This is a Social Construction-driven approach, which supports any potential shift in how the problem's importance shifts across Policy Agendas through the years. Furthermore, according to this approach, any consensus about what the FFD problem is and how it should be addressed is driven by the educational background and professional training of the expert individuals and groups who investigated it. Those may be Practitioners or Observers, and their interests and views grow, live and evolve within a Community of Conventional Wisdom. The approach is diagrammatically represented in Figure 2 below.

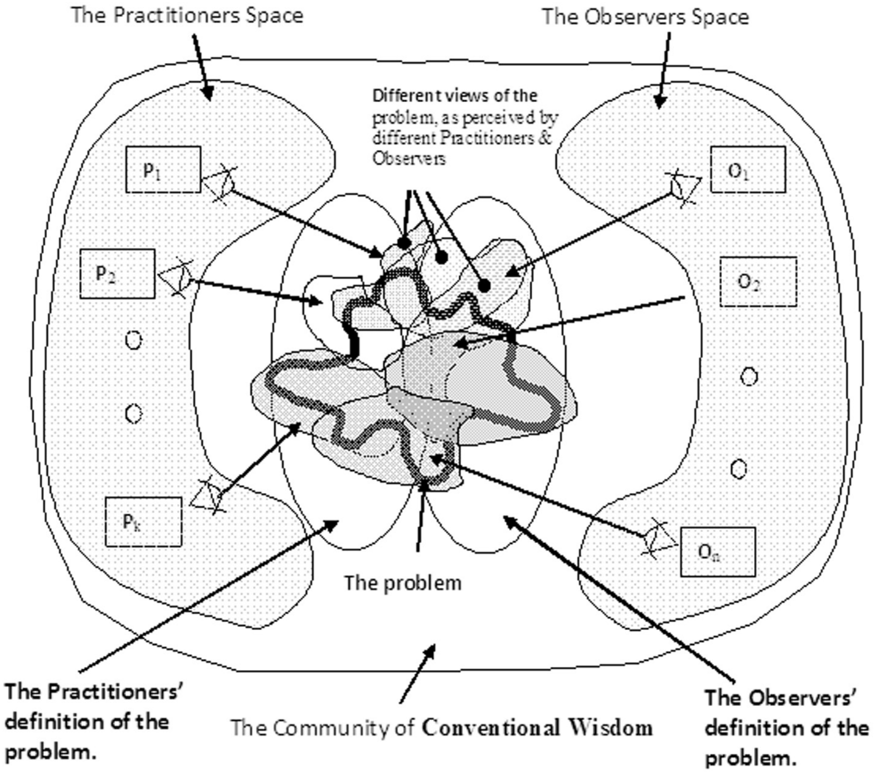
The Practitioners Space
The Observers Space
Different views of the problem, as perceived by different Practitioners & Observers
P1
P2
O
O
Pk
O1
O2
O
O
On
The problem
The Practitioners' definition of the problem.
The Community of Conventional Wisdom
The Observers' definition of the problem.

Fig. 2: The Actor-based IGT Model for Explaining the Social Construction of the FFD problem. The problem (marked by the thick line) is constructed through the perceived realities of each expert group of Practitioners or Observers and within the Community of Conventional Wisdom. Notice that the final 'shape' of the problem does not pre-exist. It is negotiated and reached through the interaction of Practitioners, Observers and the Community

The way that the framework can support an analytical approach to FFD is by facilitating an analytical model that actively takes account of interests; a pure Stakeholder Analysis (see [5, 6], among others) is not preferred here, as the relevant stakeholder grids[1] used tend to pre-assign values to the importance of stakeholders , thus embodying assumptions that are established as conventions. The Actor-based approach, on the other hand, offers the additional opportunity for involving Actors' expertise and background.

In our Actor-based analysis the following parties are identified and categorised as *Observers* or *Practitioners*. In this analysis, Observers are interested parties with direct interests to the problem of FFD who, however, maintain indirect involvement in the practice of achieving fraud detection in its technical sense. Observers in our analysis include:

[1] Typically, stakeholder analysis approaches adopt portfolio tools, typically names Stakeholder Grids, which map stakeholder attributes such as power, impact and interest against each other to enhance our understanding of a situation or problem.

1. Universities and Academic Researchers from a multitude of disciplines, such as Finance & Accounting, Banking, Economics, Public Policy, Law, Information Systems, Computer Science (including Artificial Intelligence and Data Mining); these aim to promote specific research aims through academic publication and through attracting public or private research funding.
2. Commercial and other Market Research entities, such as consultancy firms, seeking the delivery of market intelligence (in the form of reports or knowledge services) as a marketable product for the Financial Services industry.
3. Regulatory Authorities, national or international, aiming to ring-fence broader societal and economic interests; secure balanced operation of the financial infrastructure; and provide against abuse of that infrastructure for criminal purposes.

On the other hand, Practitioners are these interested parties whose direct mission is to practically solve the problem of FFD as part of their business strategy. Our analysis identified Practitioners to be:

1. Financial Institutions, which are interested in serving their business model while ensuring regulatory compliance with Anti-Money Laundering Rules;
2. Technology providers and vendors, which aim to develop technical solutions for Financial Services firms to automate or otherwise facilitate FFD.

The above categorisation may go further to identify sub-sections of each class of Actors; however, for the purposes of this paper, it is only used as a basis for discussing the involved interests.

IDENTIFYING PERTINENT INTERESTS

Having identified the key Actor classes, the discussion draws on the landscape around FFD on the basis of how Actors' interests are interlinked. That discussion will lead to the conclusions where the necessity for integrating technical solutions with policy frameworks is stressed.

To begin with, the interests of Universities and academic disciplines are represented and the research bodies avail themselves in the form of tools and approaches that are potentially usable in the industry. Interestingly, rarely are these approaches directly used in the industry; this, however, may come as no surprise since the specificities of proprietary systems (software and hardware architectures, legacy data management systems) do not allow for direct use.

On the other hand, the interest of the Financial Services industry on FFD is largely driven by compliance and regulation that dictates tighter Anti-Money Laundering controls, while at the same time there is significant pressure for controlling any related operating costs. On aggregate, the interests of Financial Services firms appear to lie in:

1. ensuring compliance in order to withstand regulatory audit;
2. minimising the costs of compliance (potentially through intelligent FFD support);
3. improving their risk profile as deemed important for regulators, auditors, shareholders and customers;
4. avoiding loss of business while still projecting corporate social responsibility in the industry.

Interests of technology providers and vendors are, however, different: attending to the service provision model, IT systems providers address the problem with a focus on sales and pursue establishment of their product suites across firms in the sector. Naturally, technology vendors have little interest in regulatory requirements as their main concern as these may introduce unnecessary restrictions and costs. Finally, because they often attend to license-based models, they often are incompatible to each other and offer a significant extent for customisation, as this is what generates the bulk of their income.

Finally, regulatory authorities and policy-makers have a totally different agenda, not least because or their non-for-profit character. Their interest is that of ensuring against illicit profiteering, ring-fencing security and the interests of the state, serving tax collection efficiency, among other things, all within a framework that fosters healthy and untethered competition in the industry and does not reduce customer confidence on the economy. On the other hand, policy makers abound across industries and across fields and problem areas, as public policy and regulation grows organically: regulatory bodies and approaches are disparate across national jurisdictions and industries, which makes the combined problem of FFD, Anti-Money Laundering and Terrorist Financing further complex in regulatory policy terms. Furthermore, Financial Services regulators are not exclusively concerned with fraud and have to act in compliance with other bodies and authorities. The challenges for regulators introduced from the above mainly focus on:

(1) agreeing and sharing jurisdiction at national level while maintaining response speed and efficiency;
(2) supporting the sharing of data without failing jurisdiction requirements;
(3) ensuring coordination between them in order to materialise tangible or intangible gains for the state and the public;
(4) maintaining and defending a standard of risk profile across the industry.

The above discussion of Actors' interests provides an interesting and challenging landscape where technologies derived from applied academic research, vendor-driven technical solutions and bespoke proprietary approaches can only offer partial answers to Intelligent Financial Transaction Fraud, when operating in isolation. As explained in our Intelligent FFD approach, the desired optimal collective intelligence can be delivered through shared infrastructure (Figure 1). This poses, however, the open question of ownership of the derived collective intelligence, which calls for further consideration.

CONCLUSIONS AND FURTHER WORK

This work has advocated for the necessity for systems integration, data sharing and co-ordination between industry and policy actors in the Financial Services world to achieve effective Intelligent Financial Fraud Detection and Deterrence. In so doing, it has demonstrated that this effort can only be optimised through developing *collective intelligence* across the industry; such an effort, the argument goes, is fraught with difficulty mainly because of (i) the confidential nature of the transaction data that would need to be shared; (ii) the competitive nature if the Financial Services industry where sharing of best practice is challenging; (iii) disparity of data sources and channels, which makes this an uneconomical exercise; (iv) disparity of interests between Financial institutions and regulatory authorities.

To overcome the obstacles, this article provided a framework to systematically record and analyse the role of Actors or interested parties in addressing the problem, ultimately aiming to contribute to informed consensus on both technological and policy-related facets of Intelligent Financial Fraud Detection and Deterrence.

In technology terms, we suggested an intelligent, workflow-centred solution that was developed as part of the authors' research in 2011-12 and updated to accommodate scalability and the capability for handling large and diverse data sets, while maintaining data anonymity; emphasis was placed on the system architecture that supports the aim of *collective intelligence* required to optimise the quality of delivered benefits. It is therefore contended that at least one technological solution can be made available to support this model.

In terms of policy, in turn, focus was placed on underlining the necessary conditions for practical implementation of that technological approach. That, we argued, can be served by surfacing the roles and – often disparate – interests of expert groups and individuals called Actors.

By doing so, we come closer to addressing an open debate about whether and how the *collective intelligence* that results from our proposed approach can be governed to deliver superior results for Financial Institutions and wider socio-economic benefits.

REFERENCES

[1] Stokes, R.: Virtual Money Laundering: the case of Bitcoin and Linden Dollars, Information and Communication Technology Law, Vol. 21, No. 3, pp. 221-236 (2012).

[2] Bronk, C., Monk, C., and Villasenor, J.: The Dark Side of Cyber Finance, Survival: Global Politics and Strategy, Vol. 54, No. 2, pp. 129-142 (2012).

[3] Milimo, M.: AML Around the World: Money Laundering in the High Seas, ACAMS Today, Vol. 8, No. 1, January/February (2009).

[4] White Paper: Anti-Money Laundering Risk Assessment & Customer Due Diligence, Association of Certified Anti-Money Laundering Specialists (2013).

[5] Brugha, R. and Varvasovszky, Z.: Stakeholder Analysis: A Review, Health Policy and Planning, Vol. 15, No. 3, pp. 239-246, (2000).

[6] Bryson, J.M.: What to do when Stakeholders Matter, Public Management Review, Vol. 6, No. 1, pp. 21-53, (2004).

[7] Samakovitis, G.: Technology Investment decision making: An Integrated analysis in UK Internet Banking, PhD Thesis, The University of Edinburgh (2006).

[8] Samakovitis, G. and Fleck, J.: Practitioners, Observers and the Community of Received Wisdom: The Actor-based Approach to Technological Investment Decisions, In: 13th European Conference on Information Technology Evaluation, Genoa, Italy, pp. 28-29 (2006).

[9] Kapetanakis, S.: Intelligent Monitoring of Business Processes using Case-based Reasoning, PhD Thesis, The University of Greenwich (2012).

[10] Kapetanakis, S., Petridis, M., Knight, B., Ma, J., Bacon, L.: A case based reasoning approach for the monitoring of business workflows. In: Bichindaritz, I., Montani, S. (eds.) 18th International Conference on Case-Based Reasoning, ICCBR 2010, LNCS (LNAI), vol. 6176, pp. 390–405. Springer, Heidelberg (2010).

[11] Bennett, N. and Dilloway, S.: Investigating the Convergence of Money Launderingn and Terrorist Financing, ACAMS AML and Financial Crime Conference, Amsterdam, 19-20 June (2013).

[12] Ford, C., L.: Principles-Based Securities Regulation in the Wake of the Global Financial Crisis McGill Law Journal 55 (2010).

[13] Crawford, L., Lont, D., Scott, T.: The effect of more rules-based guidance on expense disclosure under International Financial Reporting Standards. Accounting & Finance (2013).

[14] National Fraud Authority: Annual Fraud Indicator 2013, https://www.gov.uk/government/publications/annual-fraud-indicator--2 , last accessed 15 Sep 2013.

[15] Kapetanakis, S., Samakovitis, G., Gunasekera, B. and Petridis, M.: Monitoring Financial Transaction Fraud with the use of Case-based Reasoning, Seventeenth UK Workshop on Case-Based Reasoning (UKCBR 2012) 11th December 2012, Cambridge, UK (2012).

[16] Ngai, E.W.T., Hu, Y., Wong, Y.H. Chen, Y. Sun,X.: The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature, Decision Support Systems, Volume 50, Issue 3, pp. 559-569 (2011).

[17] Ash, D.: The UK fraud landscape for financial services, Computer Fraud & Security, Volume 2011, Issue 4, pp. 16-18 (2011).

[18] National Fraud Authority, Annual Fraud Indicator, January 2012, http://www.homeoffice.gov.uk/publications/agencies-public-bodies/nfa/annual-fraud-indicator/annual-fraud-indicator-2011?view=Binary , last accessed 10 Oct 2012.

[19] The Global Financial Cost of Fraud, Finance Week, 16 November 2009, http://www.financeweek.co.uk/topic/global-financial-cost-fraud , last accessed 10 Oct 2012.

[20] The Financial Cost of Fraud, Centre for Counter-Fraud Studies, University of Portsmouth, 2011, http://pkfemail.co.uk/ukassets/images/460/Downloadfiles/The Financial Cost of Fraud_WEB.pdf, last accessed 4 Oct 2012.

[21] Edge, M. E., & Sampaio, P. R. F.: A survey of signature based methods for financial fraud detection. Computers & Security, Volume 28, Issue 6, pp. 381–394 (2009).

[22] Edge, M. E., & Sampaio, P. R. F.: The design of FFML: A rule-based policy modeling language for proactive fraud management in financial data streams, Expert Systems with Applications, Volume 39 pp. 9966–9985 (2012).

[23] Anti-Money Laundering Annual Report 2012/13, Financial Conduct Authority, http://www.fca.org.uk/your-fca/documents/anti-money-laundering-report , accessed 30-7-2013.

[24] Fraud The Facts 2013, Financial Fraud Action UK, http://www.financialfraudaction.org.uk/Fraud-the-Facts-2013.asp , accessed 22-7-2013.

[25] Keene, S.D.: Threat Finance: Disconnecting the Lifeline of Organised Crime and Terrorism, Gower, London (2012).

[26] Hopton, D.: Money Laundering: A Consice Guide for all Business (2nd Ed.), Gower, London (2009).

[27] White Paper: NoSQL in the Enterprise, Datastax (2013).

[28] Padhy, R. P., Patra, M. R., Satapathy S. C.:RDBMS to NoSQL: Reviewing Some Next-Generation Non-Relational Database's, International Journal of Advanced Engineering Science and Technologies, Vol. 11, No. 1. (2011).