An Anti-Money Laundering Methodology: Financial Regulations, Information Security and Digital Forensics Working Together

Denys A. Flores*
National Polytechnic School
Quito, Ecuador
denys.flores@epn.edu.ec

Olga Angelopoulou and Richard J. Self
University of Derby
Derby, U.K.
{o.angelopoulou, r.j.self}@derby.ac.uk

Abstract

Analysing large amounts of financial information within databases can be hardly accomplished when dealing with money laundering. The main reason is the lack of digital forensics and proper database analysis procedures within the anti-money laundering strategies of financial institutions. Also, analysing single or grouped financial events related to money laundering is difficult when the Know-Your-Customer Policies in these institutions are not enforced, or even used as evidentiary instruments to gather digital evidence and track suspicious customers through the whole investigation life cycle. Even though the relevant data sources to get information from can be identified and used to create Suspicious Activity Reports, they need to be protected from money laundering events, and by these means, prevent their confiscation. Hence, in this article, we propose a methodology for combining digital forensics and database analysis in order to enhance money laundering detection. Additionally, in order to tackle the lack of synergy between the KYC policies and Information Security requirements, we enhance our previous model by analysing the FATF recommendations, the Basel Frameworks along with the BS ISO/IEC 27001, 27002 and 27037 standards in order to incorporate some of their best-practices into a methodology for money laundering detection model to deliver a set of requirements and activities for customer verification and financial evidence extraction before, during, and after a suspicious activity takes place.

Keywords: digital forensics, information security, money laundering, FATF, database analysis

1 Introduction

Digital forensics is the science which aims to identify, preserve, collect, validate, analyse, interpret, document and present digital evidence stored in electronic sources [3]. Thus, digital forensics applies in the reconstruction of events during criminal investigations, or anticipates unauthorised actions [24]. There is an attempt of the utilisation of digital forensics principles in money laundering detection. Flores, et al. (2012) demonstrated that these techniques can be used for supporting the investigation of money laundering cases along with the application of internal controls to track illegal operations [16]. Since using conventional digital forensic tools to analyse large financial databases may not be possible (Wright, 2009), we already proposed that digital forensic practices and database analysis approaches should be considered to assist the establishment of Know-Your-Customer 'KYC' policies, and the collection of reliable financial evidence in order to effectively produce Suspicious Activity Reports 'SARs' (FATF, 2001).

Journal of Internet Services and Information Security (JISIS), volume: 3, number: 1/2, pp. 101-114

*Corresponding author: Department of Informatics and Computer Sciences (DICC) Faculty of Systems Engineering National Polytechnic School Ladron de Guevara E11-25 y Andalucía Quito, Ecuador, Tel: +593-2-2-507-144 (ext. 2664), Web: ec.linkedin.com/in/denysflores/

In our current research we identified anti-money laundering recommendations proposed by the Financial Action Task Force [15], [14] [1] and the Basel frameworks [2] to help financial institutions to secure their transactions by means of an adequate measure of capital and liquidity. These recommendations and frameworks lack of both Computer Forensic Practices and Information Security considerations. The initial aim of this work was to develop a methodology to forensically identify, collect, analyse and present financial evidence. However, it did not define which kind of financial information data sources should be secured to get reliable evidence from, and what kind of customer information should be collected and revised in order to not only detect money laundering activities, but also ensure the customer information accuracy to ensure traceability and strong linkage between the obtained digital evidence and the KYC policies.

Therefore, considering that information is an important asset that needs to be protected [19], money laundering-related information has to be properly managed by incorporating the FATF recommendations about KYC policies, and the Minimum Capital Requirements outlined in the Basel frameworks so that only the relevant data sources can be identified and secured. As a result, admissible and reliable digital evidence can be identified, collected, acquired, and preserved, considering the BS ISO/IEC 27001, 27002 and 27035 standards.

Hence, in section 2, a brief summary of the FATF recommendations is provided. Then, in section 3, the importance of identifying and protecting capital assets is explained along with the need of regulating customer financial activities. Section 4 outlines the research methodology in order to present and justify the combination of financial requirements, information security, and digital forensic practices. It is followed by section 5, where the key features of our proposed methodology for money laundering investigation are discussed. It includes the fundamentals of our existing work in order to; first, understand the current selection of relevant financial data sources, and later justify the implementation of information security controls to protect and validate customer information. Finally, conclusions about this research are given.

2 Summary of the Financial Action Task Force Recommendations

In 1990, the FATF issued 40 Recommendations [14] in order to help financial institutions to implement anti-money laundering methods and techniques to refrain the misuse of financial systems to launder drug money. Then, further revisions in 1996, 2003, and 2004 helped to reflect the evolving money laundering typologies in these recommendations, including terrorism financing which are fully covered and discussed in the FATF IX special recommendations [13].

In summary, the FATF 40 Recommendations and FATF 9 Special Recommendations are focused in the following areas:

- Strengthening the Legal Systems by urging countries to sanction money laundering and its predicate offences, confiscate unlawful assets related to these offences, and ensure that relevant evidence is obtained to apply civil or criminal liability to the offenders [13](rec.III; 1- 4)
- Adoption of measures to prevent money laundering and terrorism financing by implementing Know-Your-Customer Policies (KYC) to keep track of politically exposed persons, cross-border transactions and non-face to face business relationships [13](rec.II,IX; 5-12)
- Monitoring and Reporting suspicious transactions via Suspicious Activity Reports (SARs) when funds are suspicious of being proceedings of money laundering [13](rec.IV; 13-16)

[1] The Financial Action Task Force is an inter-governmental body whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing [13].
[2] Basel Frameworks published by the Bank of International Settlements.

- Establishing protections to prevent financial relationships with banks with no physical representation in the country (aka. shell banks) as well as making sure to apply the recommendations to non-financial businesses and professions which may be vulnerable to money laundering [13](rec.VIII; 17-20)
- Making sure that these recommendations are fully applied in the country, including the branches and subsidiaries of local banks located abroad [14](rec. 21-22)
- Regulation and Supervision of financial operations within financial institutions and non-financial businesses and professions such as casinos, real states agents, jewels dealers, lawyers, among others [13] (rec. VI; 23-25)
- Establishing a financial intelligence unit (FIU) in the country to receive, analyse and disseminate SARs, the results of which can assist law enforcement authorities in further investigations [14] (rec. 26-32)
- Making sure legal persons are aware and prevented from misuse of their financial assets for money laundering purposes [14](rec. 33-34)
- Establishing communication channels for international cooperation, including mutual legal assistance and extradition [13] (rec. V; 36-40)
- Keeping track of wire transfers, including all the relevant information of the originator name through the whole payment chain [13] (rec. VII)

Understanding the FATF Recommendations is important to develop an understanding of the main goal the Information Security strategy in our money laundering detection methodology aims to fulfil.

3 The Importance of Protecting Relevant Capital Assets and regulating Customer Financial Activities

3.1 Identifying and Protecting Capital Assets

The BIS [3] has suggested that any financial institution should properly identify and measure its sources of Core and Supplementary Capital, along with liquidity sources due to the fact that they constitute minimum capital requirements for the proper operation of any financial institution [4](p.6, 14).

First, Core Capital, Equity Capital or Tier 1 Capital [4](s.49 (i-iii)), is a key capital element comprised of Regulatory Capital and Risk-Weighted Assets, which are useful to identify and measure the sources of capital, and assess their risk respectively [4](p.12). In fact, this allows protecting them from unexpected financial exposures by identifying which core capital sources are and define methods to protect them.

Second, Undisclosed Reserves of Capital, Supplementary Capital, or Tier 2 Capital is the capital reflected in the profit and loss account, so it has to be considered as a minimum capital requirement in terms of financial transparency. Particularly, measuring this form of capital enables to identify the possible financial losses not yet identified [4](s. 49; iv, vii - x).

Third, measuring liquidity is important in order to identify the concentration of funding per funding source in order to prevent liquidity collusions [6](s. 151). As a matter of fact, measuring liquidity enables to secure the liquidity capacity of any financial institution so that it can be able to face economic stress during critical events [6](s.1).

[3]The Bank of International Settlements assists central banks in their pursuit of monetary and financial stability, to foster international cooperation in those areas and to act as a bank for central banks.

Finally, considering that any assets or property should be confiscated when directly or indirectly related to either money laundering, or terrorism financing [14](rec. 3, 13, 38; lit. III), the minimum sources of capital should be identified and protected in order to not only prevent the injection of unlawful capital assets, but also to identify the financial risk if they are confiscated due to money laundering activities.

Hence, the importance of identifying, measuring and protecting the minimum capital requirements has to be considered to prevent them to be confiscated if found related to money laundering events. In fact, the consequences of it may impact the financial institution's normal operation since these represent important funding sources to guarantee the normal operation of any bank, or financial institution.

3.2 Regulating Customer Financial Activities

Initial research demonstrated that KYC policies are important to reveal unlawful activities related to money laundering [16]. However, the main goal in our current research was to effectively apply and use KYC polices as an evidentiary instrument, not only as a mere internal policy to just comply with the FATF recommendations. Therefore, the examinations of FATF recommendations and the Basel Frameworks demonstrated key regulations about customers which can be used to get accurate evidence about unlawful activities. Consequently, our existing methodology was enhanced by considering the validation of customer identification data, and ensuring the traceability of their activities before, during, and after any financial transaction takes place [14](rec. 5).

The identification and verification of existing customers, new customers, casual customers and beneficial owners must be supported by copies or records of official and reliable documents before a financial event [14](rec. 5(a), (d); 10). Additionally, in case of politically exposed persons beyond the controls already mentioned, conducting enhanced monitoring of activities and business relations [14](rec.6(b), (d)) is required to assess operational risk. Such assessment has to be done considering market risk, and identifying risk exposure groups [4] due to the fact that money laundering risk related to business lines [4] has been omitted when analysing money laundering operations [2]. This consideration in our model is explained as follows:

a) Since the operational risk is closely related to the business lines (prop. 1),
operational risk $\rightarrow$ business line identification (1)
b) And these can be also linked to money laundering risk (prop. 2);
money laundering risk $\rightarrow$ business line identification (2)
c) Then, operational risk implies money laundering risk identification (prop. 3):
if (1) $\rightarrow$ (2) $\rightsquigarrow$ operational risk $\longleftrightarrow$ money laundering risk (3)

Therefore, identifying business lines through operational risk assessment is important not only to link money laundering risk identification with the business lines, but also to identify which financial data sources are in charge of managing the interactions among customer transactions and business lines operations.

Then, during any financial event, as in establishing business relationships or conducting transactions, records of identity data must be kept along with transaction validation, and personal information verification [14](p.5). Thus, validating transactions is important in order to identify suspicious transactions or patterns that may be linked to money laundering.

Furthermore, after any financial event, information must be kept for at least five years along with customer identification data and all the necessary transactional records in order to evaluate and determine

[4] A business line or line-of-business is a product or set of products which are vital for running the enterprise's core business because these generate profit. LOB's are usually run by computer applications which are large programs related to financial databases.

to either finish the relationship with a suspicious customer, or make a Suspicious Activity Report 'SAR' [13](lit. IV; rec. 10, 5), if required.

The assessment of Market Risk should be considered not only to monitor customer's business activity before and during a financial event [14](rec. 5 (d)), but also to justify SARs by providing evidence which links potential money laundering activities with market behaviour and business lines operations. The analysis of a single or a group of exposures, as part of the market risk assessment strategy [5](s.27, p.15) in money laundering risk can be associated to risk concentration sets [15](p.17). Thus, regulating customer behaviour before, during and after a financial event allows to promptly report money laundering suspicions [15](p.25) supported by market movement evidence related to the business profile of a suspicious customer, and the impact of such actions in the business lines as well as minimum capital requirements.

4 Brief Explanation of the Research Methodology for Incorporating Financial and Information Security Requirements into the Money Laundering Detection Model

The initial money laundering detection model [16] could not use a real transactional database because accessing this type of information is generally restricted and classified in all financial institutions. Therefore, in order to enhance it, we required a strategy which can be useful to create a general knowledge baseline to define strategies for money laundering detection in spite of not having direct access to real transactional data, or current money laundering procedures.

The enhanced version of our model should be able to incorporate valuable considerations for detecting money laundering. This is a complicated procedure, considering that it requires investigating the offences along with the financial events related to this form of crime [21].

Thus, as money laundering investigations require considering financial requirements and customer behaviour, the developments from our initial model must ensure that financial data sources provide reliable digital evidence to be collected in the evidence repository (Flores, et al., 2012). In addition, a knowledge baseline for money laundering detection has to be developed to enhance the previous model, whereas the information sources should provide valuable practices to be considered acceptable knowledge in the field [29] (p. 101).

Our current research analysed the Basel Frameworks, the FATF recommendations, the BS ISO/IEC 27001, 27002 and 27035 standards, because they provide the best-practices to enhance our previous money laundering model not only to ensure that valuable considerations are delivered, but also to obtain reliable digital evidence from secure financial data sources. As a consequence, money laundering events can be investigated and related to relevant financial events [21] in order to produce admissible SARs with reliable customer verification.

5 Key Features and Enhancements to the Money Laundering Detection Model

Financial requirements need to be included in order to identify the relevant financial data sources to get evidence from, and establish the requirements to identify and validate customer activities and their information in a secure manner. In the next sections, the key features of the preliminary model and its enhancements are explained, so that a more accurate money laundering investigation can be performed using the Top-Down Approach [16].

5.1 Key Features of Our Previous Model

Initially, we proposed a money laundering detection model to handle digital evidence before, during and after a suspicious activity takes place [17], stressing the importance of understanding, analysing, evaluating and reporting such suspicions. Moreover, considering database log files as digital evidence [16] suggested and demonstrated the way of extracting them by selectively imaging the relevant logs for money laundering investigations, and by this means, not only preventing them from being corrupted, but also ensuring their integrity. Additionally, our previous research showed that it is very important to develop thresholds inside transactional databases, using stored procedures [22], in order to support the KYC policies, and align the detection process with the organisational goals [25], as shown in Sample Code 1:

```
delimiter $$
    USE `sample_database`$$
    CREATE PROCEDURE `backup_transactions_csv` (IN amount DECIMAL, IN start_date DATETIME, IN
    end_date DATETIME)
    BEGIN
     SET @threshold = amount;
     SELECT * FROM `sample_database`.`tb_db_transact_log`
          WHERE `tb_db_transact_log`.`trans_amnt`
          >= @threshold AND trans_datetime BETWEEN start_date AND end_date
    INTO OUTFILE '/home/root/Documents/MySql
          Forensic Logs/backup.csv'
          FIELDS TERMINATED BY ','
          OPTIONALLY ENCLOSED BY '"'
          LINES TERMINATED BY '\n';
    END
$$
```

Sample Code 1. Using store procedures in MySQL Server to define pre-defined thresholds according to *KYC policies*

This, however, requires the identification of potential data sources which may provide transactional information to reveal unlawful activities against the KYC policies.
Thus, our initial assumption was that, as digital evidence storages can be different data sources [10], these potential data sources should be managed and controlled either in digital transactional archives; e.g., spreadsheets, or in computer databases; e.g., accounting databases. However, the whole set of data sources will not be needed, but only the relevant data in transactional archives and computer databases related to financial transactions: Let be:

$$\text{(4) } T = \{\forall\, x | x \text{ is a dataset within transactional archives}\}$$
$$\text{And } C = \{\forall\, x' | x' \text{ is a dataset within computer databases}\}$$
$$\text{(5) Then } T \bigcup C = R$$
$$\text{Where}$$
$$\text{(6) } R = \{\forall\, x, x' \mid x \wedge x' \text{ are datasets related to financial transactions}$$

Then, once the evidential data sources in (6) are identified [9], they can be consolidated into digital repositories by adopting the Top-Down Approach [16] in which relevant pieces of data are identified, extracted, transformed and loaded [5] into them. These repositories may be just one de-normalised database table [6] or history table $footnote A table named `tb_db_transact_log' is used in Sample Code 1 as digital repository.$(see Figure 1), which is important for preserving transactional events for further forensic analysis [11].

[5]Extract, transform and load (ETL) is a process in data warehousing to extract information from operational or archive systems, transforming it to meet business needs, and loading it into the end target [12]
[6]De-normalization is the process to optimise the read performance of a database by adding or grouping redundant data [27].

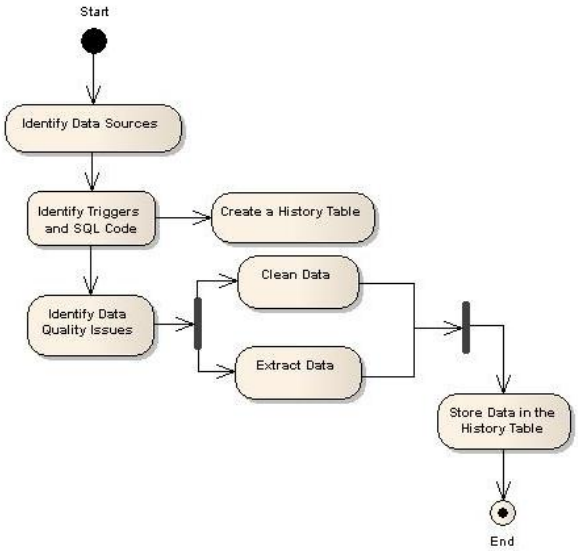

Figure 1: Top Acquiring Evidence Stored in Data Sources.

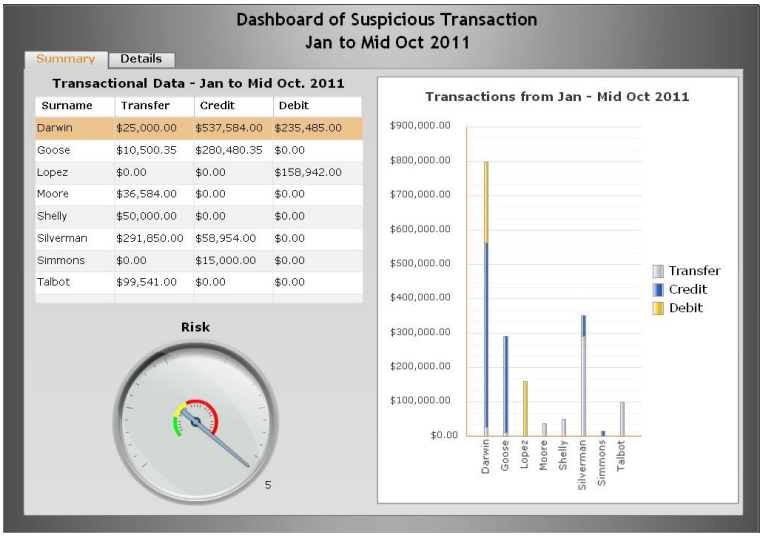

Figure 2: Dashboard of Suspicious Money Laundering Transactions

```
-- Backup Jan11 - Mar11
DELIMITER $$
USE `forensics`$$
CALL backup_transactions_csv(10000.00, '2011-01-01', '2011-03-01');
```

Sample Code 2. Creating CSV files in MySQL Server as suspicious database logs from Jan. to Mar. 2011, where transactions are greater or equal than USD$ 10,000. 00, matching pre-defined thresholds in *KYC policies*

By using Sample Code 1, customised database logs can be created, and stored as plain text. These plain-text files can be considered evidence, and extracted automatically as many times as needed in order to prove that internal policies have been violated [22]. For instance, a database log can be created when a transaction is greater than or equal to USD 10,000.00 which may be considered suspicious within a specified period of time (see Sample Code 2)

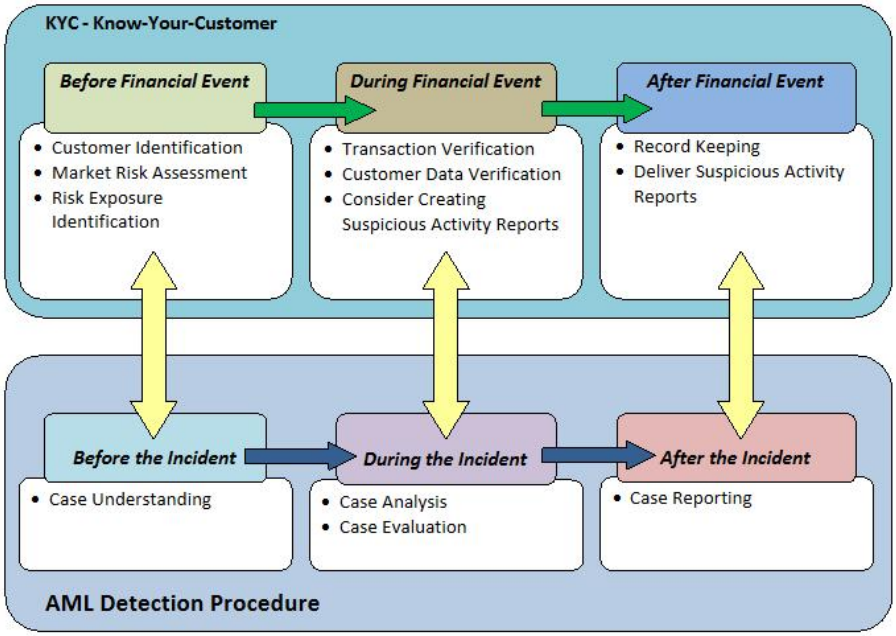

Figure 3: Enhancements to the Previous Model by Aligning KYC Policies, Financial Data source Protection and the Previous Digital Forensic Practices, Before, During and After a Suspicious Event

When any suspicious event is detected, the customized database logs can be examined and selectively imaged [10] to avoid evidence corruption and manipulation [1], while the normal database server operation is preserved. As a consequence, evidence can be used to create enhanced SARs [16] using BI Dashboards (see Figure 2).

Nonetheless, even though evidence data sources can be identified, analysed and used to report suspicious money laundering activities, the types of financial sources were not defined in our previous model. Also, even though the previous model helped dealing with money laundering digital evidence once it is consolidated from different sources, it was not possible to ensure that these sources meet security requirements to avoid that pre-processed customer digital evidence can be tainted.

The financial sources and information security requirements have been considered in the enhanced model.

5.2 Enhancing the Initial Model

In order to identify the way in which our previous model can be enhanced, it was necessary to define a knowledge baseline [29] that detects financial sources, and protects them from being tainted by applying information security control requirements in customer information (see Figure 3).

a) Identifying Financial Sources is important because later research, based in the Basel Frameworks [4][5][6], and the FATF Recommendations [13][14][15], showed that these sources have to be prevented from being used as money laundering targets. In fact, as stated by the FATF [14] (rec. 3, 13, 38; lit. III), all assets or property, including the mentioned ones, should be confiscated when directly or indirectly related to money laundering. The financial sources that should be protected from being confiscated due to money laundering activities are shown in Table 1:

Table 1. Financial Sources to be Protected from Money Laundering Activities

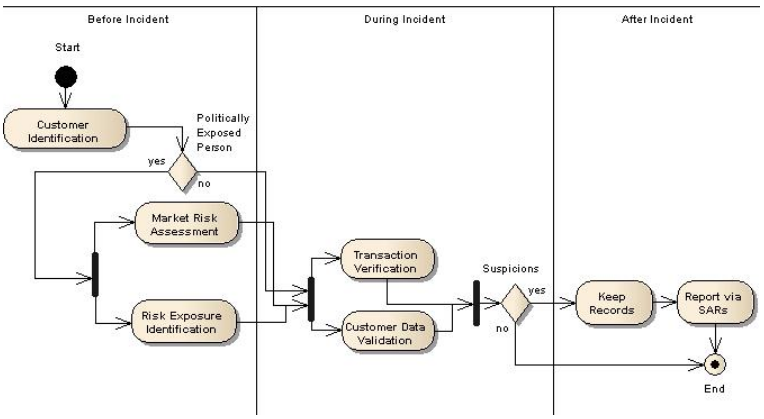

Figure 4: Know-Your Customer Policies Workflow

Financial Source	Description
Core Capital	*Core Capital, Equity Capital or Tier 1 Capital* is the capital visible in published accounts, and a common key element to all banking systems in order to assess the minimum capital requirements (BIS, 2006, s.49 (i)-(iii))
Supplementary Capital	*Undisclosed Reserves of Capital, Supplementary Capital, or Tier 2 Capital* is the capital which, in spite of not being publicly disclosed, it is reflected in the *profit and loss account*, so it has to be considered as a *minimum capital requirement* in terms of transparency (BIS, 2006, s.49 (iv)).
Liquidity Sources	*Liquidity* are comprised of all funding sources, whose withdrawal, or in this context, its confiscation, could trigger liquidity problems (BIS, 2010, s. 151)

The financial sources or minimum capital requirements as outlined in table 1, have to be protected from money laundering events because they are required to allow financial institutions to operate [4](p.6,14). However, neither the FATF Recommendations, nor the Basel Frameworks provide a process to secure the data sources related to them, which may cause that evidence is tainted before creating the digital repositories of money laundering-related evidence.

b) Protecting relevant financial sources is important to address information security when dealing with external parties before giving them access to assets [19](s.6.2). In our detection procedure [16], these external parties are customers; therefore, reliable controls are required to be implemented to manage information for customer identification, customer data validation, and customer recording before, during, and after any financial incident (see Figure 4). As a result, customer information can be considered reliable enough to produce SARs, and avoid evidence to be tainted, solving the lack of security considerations in the FATF recommendations, and Basel Frameworks.

5.3 Before Any Financial Incident

Before any financial event, literally after identifying the financial data sources, and creating the evidence repository [16], a procedure for identification and verification of existing customers, new customers, casual customers and beneficial owners must be established, and supported by reliable documentation [14](rec. 5(a), (d); 10) so that evidence can be prevented from being tainted or forged. This customer information handling procedure must be supported by document and record control requirements as well as security controls when dealing with external parties in order that employees in charge of money laundering investigations can know what exactly they should be looking at before a money laundering incident takes place. First of all, document and record control requirements are useful to track management actions and their relationship with internal policies [18] (s. 4.3.1). In Table 2, the proposed documentation and record requirements for money laundering detection are detailed.

In regards to security controls when dealing with external parties, conducting enhanced monitoring activities of customers' business relations [14](rec.6(b), (d)) are important to assess the market risk and identify exposure customer groups.

a) Market Risk Assessment is important in order to monitor the relationship between customer business activities and Market Risk; especially, if these customers are politically exposed persons [14](rec. 6(c)). Therefore, monitoring activities of customer's business activity, risk profile and source of funds [14](rec. 5(d)) can be enhanced in order to justify Suspicious Activity Reports by providing evidence which links potential money laundering activities with Market Risk assessment information.

b) Risk Exposure Group Identification is advisable to identify the Risk Concentration [5](s. 27, p.15) related to a single or a group of money laundering exposures [15](p.17) such as non-resident customers, private banking relationships, arrangements involving personal assets, and relationships with shareholder companies.

In accordance to digital forensic practises, documenting and verifying customer information is important so that money laundering evidence can be prevented from being tainted or forged. Moreover, assessing market risk, and identifying risk concentration sets allows enhancing the monitoring of customer's financial activities; especially, if they are politically exposed persons. Consequently, SARs can be produced, and supported by reliable documentation and transactional records. Also, implementing these considerations within the KYC policies allows identifying risk concentrations per each segment of the market [5](s. 32, p.16), enhancing the overall risk exposure assessment by considering the correlated risk factors that may arise from market risks [5](s. 28, p.15-16).

Table 2. Documentation and Record Requirements

Requirement	Characteristics
Document Requirements (BS ISO/IEC, 2005, s. 4.3.1)	- Document the KYC policies - Document the procedures and controls to support the KYC policies - Document the Methodologies for Market Risk Assessment and Risk Exposure Group Identification
Control of Documents (BS ISO/IEC, 2005, s. 4.3.2)	- Establish and document a procedure for controlling supporting documentation considering: - Document Adequacy Approval prior use - Review and Update of Documents - Document Re-approval - History of Changes to reflect past and current versions - Availability of the current versions of documents on demand - Document readability, identification, transference, storage, distribution, disposal - Identification of documents of external origin - Prevent obsolete document usage
Control of Records (BS ISO/IEC, 2005, s. 4.3.3)	- Establish records to provide evidence of conformity regarding KYC policies - Record protection and control - Consider legal and business requirements when producing records - Ensure record identification, readability, availability, and retrievability - Implement and document controls to identify, store, protect, retrieve, track retention time and dispose records

5.4 During any financial event

Digital evidence is considered relevant and sufficient after having converted general aggregation levels of information into specific relevant pieces of evidence, following the Top-Down Approach [16]. In fact, the model proposed in [16], defines this approach as a strategy for the analysis of large transactional data sets [20](s. 5.2(b)), due to the fact that database servers are considered mission-critical devices [20](s. 7.1.3.3).

During the investigation of a suspicious financial event, all the methods, tools, and steps used and followed must be documented so that their repeatability can be ensured at any stage of the investigation (BS ISO/IEC, 2011b, s. 5.3.3). Furthermore, documenting the overall investigation allows justifying the

actions taken [20](s. 5.3.5) to detect money laundering events whilst facing evaluations by independent assessors, or authorised counterparties [20](s. 5.3.2).

Finally, during the course of any financial event like establishing business relationships or conducting transactions, customer information has to be verified to ensure its accuracy, and support the identification of suspicious transactions or patterns that may be linked to money laundering [15](p.15) such as:

- Transactions are above the designated threshold (USD 15,000)
- Transactions are frequently suspicious; i.e., when several operations seem to be linked
- Wire transfers are occasional and suspicious when customer information (name, address and account number) is incomplete [13](lit. VII)
- Transactions are under suspicions of money laundering or terrorist financing, regardless of any exemptions
- There are suspicions regarding the accuracy or adequacy of previously obtained customer identification data

Therefore, if any transaction matches any of the previous criteria, these suspicions should be reported for later investigation by means of SARs [15](p.25), which must be supported by relevant and sufficient evidence obtained in the Top-Down Analysis. Also, all the steps, tools, and methods used must be documented so that the repeatability of the process can be ensured, in case of external parties require the validation of the findings and activities reported in the SARs.

5.5 After any financial event

Once the financial event finishes, besides evaluating the evidence using the information extracted from the financial data sources [16], all the related information must be kept for at least five years along with customer identification data and all the necessary transactional records [14](rec. 10) in order to determine:

- Whether or not carrying on with further financial event with such customer; e.g. opening an account, establishing business relationships, or performing other transactions [14] (rec. 5)
- Make a SAR in relation to that customer [13](lit. IV) under suspicions or demonstrated events related to money laundering

Thus, keeping records and financial information after any financial event allows reconstructing individual transactions (including the amounts and types of currency involved) to provide evidence of criminal activity, which can be swiftly provided under requests from the competent authorities. The process of incorporating customer verification procedures, and identifying the data sources related to minimum capital requirements enhances the existing model by preventing digital evidence to be tainted before it can be consolidated in evidence repositories. Our model is improved by protecting minimum capital requirements through the analysis of market risk and the identification of risk exposure groups. In fact, this is important to prevent unlawful capital to be injected in the financial system, the consequence of which may be the confiscation of all the related capital inside any financial institution. Furthermore, incorporating these best practices in the previous model [16] enables a more accurate detection of money laundering because evidence is not only collected, but also tracked before, during, and after any financial event by using document and record controls to ensure that violations to the KYC policies are linked to the most relevant evidence available. This clarifies the reported findings in the SARs which can be replicated at any time by any counterpart to verify the accuracy of the conclusions.

6 Conclusion

Whilst our previous research [16] defined a model to forensically identify, collect, analyse and present financial evidence, it this article we have explored financial and information security best practices in order to enhance the initial proposal by identifying financial information data sources that should be secured to prevent money laundering activities. In addition, even though our initial aim structured the process of getting financial evidence related to KYC polices, it did not identify which kind of customer information should be analysed, and how it should be handled during the investigation life cycle. However, one result of our current research is the clear identification and validation of customer information, as instructed by the FATF recommendations so that KYC policies can be used as an evidentiary instrument to collect and revise not only customer information, but also suspicious transactions related to money laundering events.

Also, our proposed work aims to deliver straightforward and practical steps to be applied within financial institutions of any size and purpose. Furthermore, it strives for delivering a set of practices which, on top of complying with the FATF recommendations and the Basel Frameworks, can be tuned and set according to the BS ISO/IEC 27001, 27002 and 27037 standards. Consequently, information assets [19] related to minimum capital requirements [4] can be protected from confiscation due to money laundering activities by closely monitoring customer financial activities using the document and record control requirements [18] as well as the financial controls outlined in our methodology. In contrast, although excellent automated tools for money laundering detection are currently in the market, for instance Oracle Financial Services Behaviour Detection Platform [23], SAS Money Laundering Detection [28] and BOSCH Money Laundering Detection System [7], they cannot ensure an adequate handling of digital evidence. Our approach, is not a plug-and-play solution, but an information security and digital forensics-based model for money laundering detection. Beneath the financial and technical requirements for its implementation, is the awareness of the whole financial institution to prevent database logs to be tainted in order to prevent, monitor, detect and report unlawful activities related to money laundering in the most secure and reliable manner possible.

Summing up, with our methodology, money laundering investigations can be supported not only by digital financial evidence, but also by documentary evidence which reflects both customer information and suspicious financial activities. Actually, this methodology is thought to be applied in the Ecuadorean financial system due to the fact that this country has been black listed due to money laundering risk in financial operations [8]. Our methodology may be the first in the country to propose aligning information security, financial requirements, and digital forensics to support an internal anti-money laundering strategy. Nonetheless, a long path is still ahead to overcome challenges like the underestimation of digital forensic practices within organisations [16], which increases the time in which our proposal can be validated in the short term, mainly due to the cost of deploying the strategy in the whole Ecuadorean financial system, and the technical requirements to align information assets with the process of consolidating the relevant financial information into a single transactional repository of suspicious transactions.

7 Acknowledgments

The authors acknowledge the support of the Ecuadorian Ministry of the Interior and the Central Bank of Ecuador for providing vital information to conduct this research.

References

[1] Association of Chief Police Officers. Good Practice Guide for Computer-Based Electronic Evidence. 7Safe

Information Security, 2011. http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf.

[2] F. S. Authority. Review of Firms' Implementation of a Risk Based Approach to Anti-Money Laundering (AML), 2008. http://www.fsa.gov.uk/pubs/other/jmlsg_guidance.pdf.

[3] V. Bhat, P. Rao, R. Abhilash, P. Shenoy, K. Venugopal, and L. Patnaik. A novel data generation approach for digital forensic application in data mining. In *Proc. of the 2nd International Conference on Machine Learning and Computing (ICMLC'10), Bangalore, India*, pages 86–90. IEEE, February 2010.

[4] BIS. Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework - Comprehensive Version. Bank for International Settlements, December 2006. http://www.bis.org/publ/bcbs128.pdf.

[5] BIS. Enhancements to the Basel II Framework. Bank for International Settlements, July 2009. http://www.bis.org/publ/bcbs157.pdf.

[6] BIS. Basel III: International Framework for Liquidity Risk Measurement, Standards and Monitoring. Bank for International Settlements, December 2010. http://www.bis.org/publ/bcbs188.pdf.

[7] BOSCH. Anti-Money Laundering. http://www.bosch-si.com/solutions/compliance/anti-money-laundering/compliance-software-anti-money-laundering.html, 2012.

[8] E. Brockner. Ecuador Blacklisted for Money Laundering. International Relations and Security Network, April 2010. http://www.isn.ethz.ch/isn/Digital-Library/Articles/Detail//?lng=en&id=114501.

[9] W. C. Forensics and Data Access Auditing. SANS Blog, 2009. http://computer-forensics.sans.org/blog/2009/03/15/forensics-and-data-access-auditing.

[10] M. I. Cohen, D. Bilby, and G. Caronni. Distributed forensics and incident response in the enterprise. *The International Journal of Digital Forensics & Incident Response*, 8:101–110, 2011.

[11] C. Database. Security information management software filters and prioritizes data. ThomasNet Industrial News, March 2011.

[12] ETL-Tools-Info. Definitions and Concepts of the ETL Process, 2012. http://etl-tools.info/en/bi/etl_process.htm.

[13] Financial Action Task Force. Fatf ix special recommendations (incorporating all subsequent amendments until february 2008). FATF Standards, October 2001. http://www.fatf-gafi.org/.

[14] Financial Action Task Force. Fatf 40 recommendations (incorporating all subsequent amendments until october 2004). FATF Standards, October 2003. http://www.fatf-gafi.org/.

[15] Financial Action Task Force. Methodology for Assessing Compliance with the FATF 40 Recommendations and the FATF 9 Special Recommendations (Updated as of February 2009). FATF Reference Document, February 2004. http://www.fatf-gafi.org/media/fatf/documents/reports/methodology.pdf.

[16] D. A. Flores, O. Angelopoulou, and R. J. Self. Combining Digital Forensic Practices and Database Analysis as an Anti-Money Laundering Strategy for Financial Institutions. In *Proc. of the the 3rd International Conference on Emerging Intelligent Data and Web Technologies (EIDWT'12), Bucharest, Romania*, pages 218–224. IEEE, September 2012.

[17] C. Grobler, C. Louwrens, and S. Von Solms. A framework to guide the implementation of proactive digital forensics in organizations. In *Proc. of the 2010 International Conference on Availability, Reliability and Security (ARES'10), Krakow, Poland*, pages 677–682. IEEE, February 2010.

[18] ISO 27001. Information Technology-Security Techniques-Information Security Management Systems-Requirements. BS ISO/IEC 27001:2005, 2005. https://bsol.bsigroup.com/.

[19] ISO 27002. Information Technology-Security Techniques-Code of Practicefor Information Security Management. BS ISO/IEC 27002:2005, 2007. https://bsol.bsigroup.com/.

[20] ISO 27037. Information Technology-Security Techniques-Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence-Draft International Standard (DIS). BS ISO/IEC 27037:2011, 2011. https://bsol.bsigroup.com/.

[21] M. J. *Money Laundering: A Guide for Criminal Investigators*. CRC Press Taylor & Francis, 3 edition, Decemer 2011.

[22] P. Kieseberg, S. Schrittwieser, M. Mulazzani, M. Huber, and E. Weippl. Trees Cannot Lie: Using Data Structures for Forensics Purposes. In *Proc. of the 2011 European Intelligence and Security Informatics Conference (EISIC'11), Athens, Greece*, pages 282–285. IEEE, September 2011.

[23] Oracle Financial Services Behaviour Detection Platform. Oracle Financial Services Behaviour Detection Platform. `http://www.oracle.com/us/industries/financial-services/046853.html`, 2012.

[24] G. Palmer and C. Mitre. A Road Map for Digital Forensic Research. Technical Report DTR-T001-01 FINAL, August 2001.

[25] P. K. Panigrahi. A framework for discovering internal financial fraud using analytics. In *Proc. of the 2011 International Conference on Communication Systems and Network Technologies (CSNT'11), SMVDU, Katra, Jammu, India*, pages 323–327. IEEE, June 2011.

[26] K. Pavlou and R. T. Snodgrass. Forensic analysis of database tampering. *ACM Transactions on Database Systems*, 33(30), December 2008.

[27] K. E. Pavlou and R. T. Snodgrass. A framework for systematic database denormalization. *Global Journal of Computer Science and Technology*, 9(4):44–52, 2009.

[28] SAS Anti-Money Laundering. SAS Anti-Money Laundering. `http://www.sas.com/industry/financial-services/banking/anti-money-laundering/index.html`, 2012.

[29] M. Saunders, P. Lewis, and A. Thornhill. *Research Methods for Business Students*. Pearson Education Ltd.., 4 edition, 2007.

Denys A. Flores is a Computer Systems Engineer with an MSc. in Computer Forensics. He has a strong background in software development and business intelligence. Currently, he works in the Department of Informatics and Computer Sciences of the National Polytechnic School of Ecuador, and is involved in large IT security projects for the Ecuadorean government. His research interests are money laundering detection, digital forensics, network security, e-discovery and cyber ethics.

Olga Angelopoulou is a lecturer in Digital Forensics at the University of Derby. She obtained a doctorate in Computing with the title: 'Analysis of Digital Evidence in Identity Theft Investigations' from the University of Glamorgan. Her research interests include Digital Forensics, Identity Theft, Online Fraud, Digital Investigation Methodologies and Online Social Networking.

Richard J Self supervises a wide range of undergraduate and postgraduate dissertations and has supervised several PhD students including topics such as e-learning, knowledge management and management practices in local government in the Middle East. His research interests are focussed in two directions; towards the pedagogy relating to the development of transferable and employability skills and the practical use of information technology in a wide range of contexts which are focussed towards understanding the contexts in which IT can make a difference and those in which it fails to deliver the planned results. A current key area is to develop a project to evaluate the phenomenon of TechnoStress and TechnoTrust and the relationship to Corporate Governance.