IJCSN International Journal of Computer Science and Network, Volume 4, Issue 2, April 2015
ISSN (Online) : 2277-5420 www.IJCSN.org
Impact Factor: 0.417

Anti Money Laundering Overall Customer Identification Schema & Data Concern

[1] Evis DRINI MBA, [2] Dr. Rovena BAHITI

[1] PhD student, National Commercial Bank of Albania
Tirana, 1000, Albania

[2] National Computer Security Agency (ALCIRT)
Tirana, 1000, Albania

Abstract - One of the main obligations resulting from AML directive is: Customer due diligence (CDD). Financial and Credit Institutions face the obligation to recognize AML customers and report their data accordingly. Knowing that these data already exists in some identified Data Bases such as: Civil State Offices, National Registration Centers, Ministries etc, then there is no need of creating multiple Data Bases for the same Customer Identification data, but there is the need of creating a data connection / exchange between these parties. The AML reporting is an obligatory EU directive and a country specific in force law obligation, so Public Institutions that posses Customer Identification Data Bases should cooperate with Financial Institutions to facilitate the process of Customer Identification thus enhancing the accuracy of data reported and Improving Customer Serving from these Financial Institutions. The intention of this research is to give an overview of the existing parties involved in Customer Identification, and listing the Pros and Cons of establishing a data communication between these parties.

Keywords - *AML, Customer Identification, Customer Due Diligence.*

1. Introduction

Financial and Credit Institutions face the obligation to recognize AML customers and report their data accordingly to the European Directives for AML[I] and Albanian in force law No:9917 dated on: 19-May-2008. Financial institutions should verify their customer/non customer identification data electronically in reliable sources like governmental lists, Identity Theft Complaint data base established by Federal Trade Commission [II] and other reliable sources [III]. In the customer relationship, the identification procedure is mandatory and the main condition to fulfill when creating a financial relation, but there are lots of cases when the Individual is not a customer of the financial institution like: Third parties, Financial representatives, Authorized person etc. and there will still exists a financial transaction performed between. In such cases, when the primary objective is serving to the client, the identification issue rises. There is no customer relationship between the parties, the financial institution and the non-customer, but there exists a financial transaction and a reporting obligation. In such cases the financial institution should collect and store whole identification data in order to use them in AML reporting if needed. These identification data actually exists in the Civil State Offices, and if they are provided to the financial institution, it will lead to fast-serving to non-customers and correct AML reporting.

To the financial institution, it is more important building a business relationship then reporting to the AML, so collecting and storing identification data for non-customers it is an added cost and time consuming. Furthermore not every non-customer should be reported to the AML and this check can be performed only at the end of the business day. The reporting requires only those non-customers that pass the threshold of 1 mil cash transactions within 72 hours. As the identification data already exists in public institutions there should be a data connection between these data bases and the financial institutions systems. This scenario requires additive data controls to insure the data security and privacy.

2. Customer Identification Schema

2.1 Where Are Stored The Identification Data?

Each individual has its own record of data identification in the Civil State Office data base. The Unique key is set

based on the SSN – social security number that is also available in every Identification Document.
PEP (political exposed persons) – list, are stored in the Interior Ministry and these kind of persons gets a special identification on financial services.

When the individual becomes a customer in a financial institution, its identification data are also stored in this data base together with the Document number and additional data like: Father-name and Address (these data are not printed on the Document but are mandatory in AML reporting). When a non-customer requires a financial service, the financial institution is not obliged by law to store the detailed data identification but is obliged to report all detailed identification data only if the customer should be reported to the AML. Not knowing since the first moment if the non-customer will be or not reported to the AML, the financial institution faces the problem how to handle such identification.

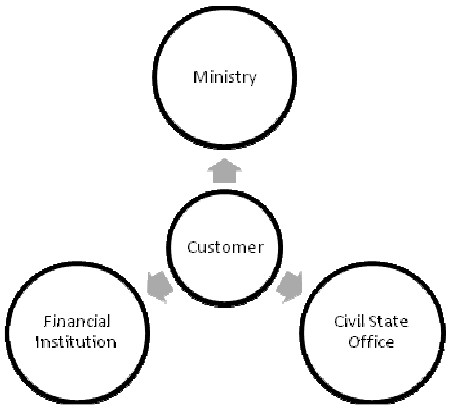

Fig. 1 Actual Identification Data flow.

One simple solution is to store identification data for non-customer the same way as storing for customers, but it delays the time of serving to these clients and adds costs of data entering and storage as well. This methods leads to the following pros and cons:

1. It is time consuming
2. Data redundancy
3. Data recurrence
4. Adds costs of data inputting/authorizing and checking
5. Adds extra costs of data storage and maintenance
6. Does not serve to the primary goal of "doing business not reporting "
7. Adds cost of queuing
8. Results in customer disappointment and annoyance
9. Causes a risky future for the business relationship
10. Overall economic cost

Some advantages of this method will be:

1. If the non-customer should be reported to AML, then all the identification data are stored in the system of the financial institution.
2. No security / privacy concern when exchanging data.

2.2 Exchanging Identification Data

If the financial institutions will be provided with a connection (web service) to get the identification data from the public institutions it will ease the process of non customer identification. The access on these data should be restricted to insure the proper usage and customer privacy.

When the identification data is needed then the "key data" should be used to make the search in this connection. As every document has its unique number and SSN printed on it, they can be used in the search method. To make it more accurate the Name and Last-name should be part of the search code. So searching in the data base of a public institution from the financial institution staff will be possible only if knowing the SSN and Name and Surname of the individual, thus insuring the search is performed only when possessing an Identification Document.

The SSN is a primary key in the public institution data base, but the financial institution identifies its customers with its own customer-number, thus the SSN should be a foreign key in the financial institution data base in order to insure the relation.

Mandatory search-fields:
- SSN
- Name
- Surname

This precondition will prevent the misuse of the rights of using public institution identification data. In addition the privacy of the non-customers is protected as well and the AML reporting needs are fulfilled.

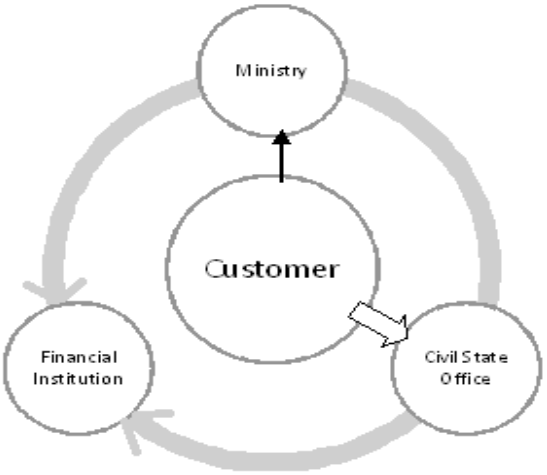

Fig. 2 Proposed Identification Data flow.

The inputting and storing data for non-customer is now replaced with a search in the web-service, resulting in a faster way of serving to the non-customer. The missing data such as Father-name and Address may be retrieved from the web-service only if the non-customer should be reported to the AML (process that is performed at the end of the business day).

3. Conclusions

Setting a data connection between financial institutions and public institutions like Civil State Offices and Ministries to ease the non customer identification process, will lead to benefits for all the parties involved.

References

[1] Commission Of The European Communities. Brussels, 30.6.2009. Commission Staff Working Paper - Compliance with the anti-money laundering directive by cross-border banking groups at group level [Electronic version] Retrieved March 17, 2013 on the website http://ec.europa.eu/internal_market/company/docs/financial-crime/compli_cbb_en.pdf

[2] http://cryptome.org/fincen022610.pdf

[3] http://www.rbnz.govt.nz/regulation_and_supervision/anti-money_laundering/guidance_and_publications/5506190.pdf

Evis DRINI has graduated the Faculty of Economic Business Informatics, Tirana University in 2007. She holds a post graduation master diploma in MBA Entrepreneurship from 2011 and is actually enrolled in PhD school in the same Faculty. She joined the Faculty of Economic staff as teaching assistant in 2008-2009 on the management of information systems subject. Having an experience of more than 7 years working as SW development, reporting and analysis in the banking sector, she currently holds the title of Senior Specialist (from 2011) on IT-department at National Commercial Bank of Albania. She is the author of 4 journal articles and conference papers in the field of information systems management, Anti Money Laundering and business informatics related fields. Her work focuses on the analysis and development of banking software applications and reporting issues.

Prof. Asoc. Dr. Rovena BAHITI has graduated the Faculty of Economic, Tirana University in 1998. She holds a PhD diploma in Economics from 2006 and she had gone through all didactic positions since 1999 when she joined the staff of the Faculty of Economic, teaching assistant in 1999, senior lecturer in 2006 and assistant professor in 2011. For several years she was full Professor of Business Informatics within the Department of Statistics and Applied Informatics at Faculty of Economic, Tirana University. Now she is the Director of National Computer Security Agency (ALCIRT). She is the author of more than 30 journal articles and conference papers in the field of management information system and other economic and informatics related fields. Her work focuses on the management of IT project and information systems.