Indian Journal of Finance and Banking; Vol. 4, No. 2; 2020
ISSN 2574-6081 E-ISSN 2574-609X
Published by CRIBFB, USA

A Framework to Score the Risk Associated with Suspicious Money Laundering Activity and Social Media Profile

Dillip Kumar Parida
Research Scholar
K. L. U. Business School, K. L. University
Greenfields, Vaddeswaram
Guntur District, Andhra Pradesh, India
E-mail:dillip_parida@hotmaill.com

D. Prasanna Kumar *PhD*
Associate Professor
K. L. U. Business School, K. L. University
Greenfields, Vaddeswaram
Guntur District, Andhra Pradesh, India
E-mail:dr.prasanna@kluniversity.in

Received: May 27, 2020 Accepted: June 30, 2020 Online Published: July 15, 2020

doi: 10.46281/ijfb.v4i2.662 URL: https://doi.org/10.46281/ijfb.v4i2.662

Abstract

Money laundering has immense entailments. The criminal who possesses black money and wants to mask it as legitimate must fabricate the source to look genuine. It makes the crime organized and more systematic to break the financial system. The existing AML (Anti Money Laundering) solutions and its design based on the creation of a transaction profile. Most of the leading AML software focuses on financial transactions and rarely focuses on linked suspicious individual's social media profiles. Social networking is one of the most popular platforms to interact with others and millions of users use these platforms to communicate with each other from around the world. At the same time, the web has plenty of social and demographic information to create an accurate profile that aims to construct a legitimate profile. This paper consolidates the fragmented discussion from several articles and provides a detailed view of fraud profile identification. Practical insights are identified from various AML solutions and summarized from an extensive literature review. The risk scoring framework and definitions of filters can be widened to include more parameters for effective alert generation. In this paper, we propose an approach and risk scoring framework to assess customer profiles that drive the suspicious profile or transactions based on social media attributes.

Keywords: Anti Money Laundering, Social Media profile, Financial Fraud, Fraud Detection, Money Laundering Detection, Risk profile scoring, Anomaly Detection.

1. Introduction

Money laundering is the process of criminal proceeds for the secrecy of their illicit source of money. Money laundering helps to enjoy the profit without the stake of their illegal resource. Money laundering is described as "the process by which the proceeds of crime and the true ownership of those proceeds are concealed or made opaque so that the proceeds appear to come from a legitimate source" (Johnston & Abbott, 2005).The widespread technology and wired transfers help the money laundering activity by layering the transactions. The organized criminals seek to make investments in the 'legitimate' economy, by investing in the legal business and real estate (Kruisbergen, Kleemans, & Kouwenberg, 2015).With the advancement of technologies and integration of financial systems, it provides multiple ways for the drug traffickers, terrorist groups, and smugglers to expand their operation and launder the money. The Identification of the money laundering activity is too difficult and complex due to the large volume of transactions globally. To identify and prevevfnt this activity many financial institutions installed software to track the illegal wired transfer. Now robust anti-money laundering solutions are developed to combat financial crime. The technology helps to combat the money launder based on risk profile and alert system. But the major Anti Money Laundering software focuses on financial transactions and limited to banking transactions. Money launders constantly devising new and innovative ways to launder money. It has become a major concern to combat money launderers with effective new measurements. Hence prevention of Money Laundering, detection of back money placement in the economy, and control of these illicit activities are crucial for a stable economy and safeguard financial institutions.

Social Media sites such as Facebook, Linkedin, and Tweeter can be utilized as an investigative tool to identify and vet individuals and businesses, determine connections between counterparties and discover criminal involvement (Glass, 2018).To combat this situation, the Anti-money laundering framework needs to be more robust and a combination of transaction profiles with a social media profile may provide additional capability to detect money launderers. This new methodology can identify the patterns in social media activities that could indicate a suspicious profile. If the data is not consistent across social media platforms then it triggers a suspicious alert about the credibility of the user for further assessment.

We find that a better view of risk profiles can be created with the help of social media attributes. Scoring of these parameters may help to detect the credibility of a user based on social media entities and attributes present in the network. The relationships can be built with the social network entities and degree of centrality to find the association. A lot of research has been done in this area but not much regarding anti-money laundering. The objective of the proposed solution is to identify the suspicious customer and create a complete 360-degree view of a customer profile that provides evidence to categorize the risk category based on social media events.

This research paper explores the possibilities for Anti Money laundering application to include suspicious social media profile detection and its scoring framework to categorize risk categories. We analyzed real-world AML systems and social media platforms that can be used as an investigative tool by utilizing Facebook, LinkedIn, and Tweeter to identify and appraise individuals and businesses. The major contributions of this research paper are (a.) A framework to include social media events as one of the criteria and (b.) Risk scoring model to provide a risk score based on predefining criteria.

2. AML Risk views for Financial and Social Media Profile

Every day we have millions of transactions in the financial industry. Transactions can be identified associated with risk and analyzed to remove the potential threat. Risk views give a data profile with the possibility of money launder activity. Social media contains a plethora of information and evidence of keywords that may be associated with money laundering. The social media data can be mined to get meaningful information regarding suspicious transactions. Social media could be rich sources of data that leads to a suspicious profile or event which is more prone to money laundering. Using text analytics on social media data for profiling may detect a suspicious user in social media concerning money laundering.

Table I. Money Laundering Events

Financial and Transactional Events	Social Media Profile Network Events
▪ Cash Transactions (high frequency and value) ▪ Sudden high-value transactions in the dormant account ▪ Accounts with High Turnover ▪ Instruments with High Volatility ▪ Transactions without descriptions ▪ Sending and receiving high volume transactions out of the country ▪ Multiple transfers in multiple accounts ▪ Purchasing of remittance in cash just below threshold limits ▪ Multiple accounts with same name and addresses	▪ The profile has nothing in common such as friends or even a professional interest ▪ Profile Network connections are random ▪ Offensive or sensitive content on the profile ▪ Lack of complete information in profiles ▪ Data mismatching in different platform and profiles

Even though the researchers presented a few strategies and approaches for identifying Fake profiles, however, it is as yet a hard challenge. For instance, some AI calculations are proposed for identifying suspicious financial transactions, however, it does not give the complete proof to recognize all counterfeit transactions. Utilizing accurate Social profile identification process can be an additional parameter to the financial transaction to understand the complete view of the user profile and its associated transactions.

3. Profile and Characteristics

Understanding the risk profile enables the financial institutions to apply appropriate risk management processes and solutions to the AML compliance solution to mitigate risk.

- **Characteristic:** A distinguishable behavior related to the financial transaction of the account holder. (e.g. unusual cash transaction pattern)

- **Profile:** Profile created with a standard set of mostly defined by the characteristic of the transaction (e.g. online transaction) and social media profile. The solution will also have a standard set of behavioral rules about customer segments and their typical behavior.
    - A profile is based upon the transactions and it may contain no of occurrences or value of the transaction.
    - A profile is based upon the consistency of data across social media platforms.
    - A Social media profile that linked to any other suspicious profile.
    - Any of the social media profile attributes has a noise keyword that relates to illegal activity, Money laundering, or crime.
    - When the transaction (financial and social) imported and profile created, the system compared the profile with its historical records/profile.
    - The combination of the rules and the customer Segments to identify instances or patterns that are abnormal or suspicious behavior.
    - The defined rules or behavior combine to assign a risk to the profile and the alert generated with a risk score.
    - The risk score is derived from an algorithm using the sum and weightings of the associated risks.

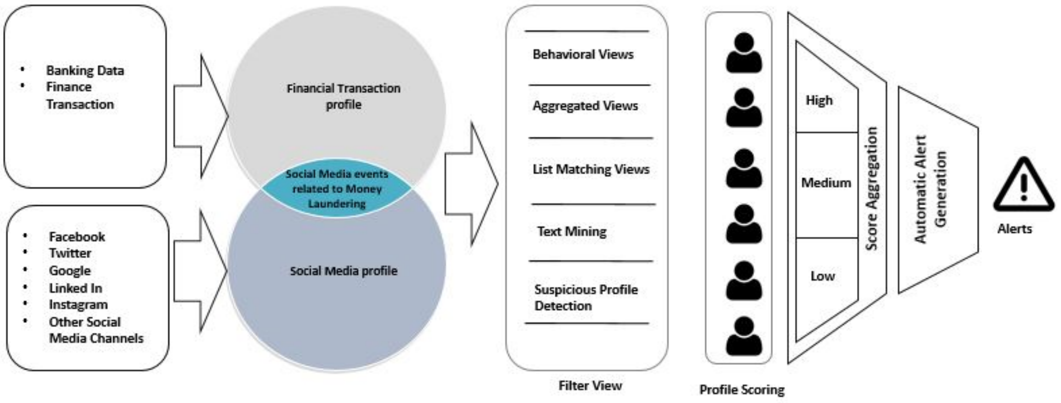

Figure1. Risk Filter process and stages

4. Risk scoring model on Filter View

The combination of financial transaction view and social media profiles created a pool of information that combines structured and unstructured data. If any data that looks suspicious in financial transactions can be profiled in the social media category. That will give a more detailed view of other aspects to get an insight into data concerning suspicious transactions.

4.1 Risk Scoring Model Framework

Risk rating involves the categorization of individual profile based on social and financial parameters, into a series of graduating categories based on types of risk. A primary function of a risk rating model is to assist in the creation of the KYC profile. As well, risk ratings assist management in predicting changes in the social and financial portfolio quality and its impact on the current KYC Framework of the financial institution. The risk rating can lead to a proactive response to the potential threat and a wider choice of reactive action to track money laundering. Risk ratings should be determined based on individual institution's policy and government regulations. Continuous monitoring of exiting profiles required as a part of the profile review process.

The following sample risk rating model can be enhanced and developed concerning organization policy. The model may be modified as appropriate to meet the specific needs of individual institutions.

Each transaction is evaluated under five risk filter components. Behavior, Aggregated, list matching, Key AML noise phrase, and suspicious profile detection. Risk Scores used for ratings are based on an evaluation of individual transactions and aggregated also. The maximum individual risk component score and the overall score are mentioned below.

4.2 Risk Filter Components

Risk filter components (Risk Assessment Filter) refer to the screening of transactions, events, information related to the customer. This screening can be classified into five different categories based on the nature of information and source systems. The classified filters are associated with risk percentage (Weight) to prioritize features for alert generation. The weight can be changed based on the priority and organization's money laundering policy.

Risk Assessment Score is calculated for a particular Risk Assessment Filter and to be anywhere between 0 to 100. Every filter can be divided into subsections or sub filters where the score can be calculated based on the type of violations. If the Risk Assessment Filter has n number of subsections or criteria's then the maximum score of any one of the matching filters can be considered here.

Table 2. Risk filter components

Filter Number	Risk Assessment Filters	Description	Weight	Risk Assessment Score (Max)
1	**Behavior**	Behavior views provide the behavioral aspect of data. The pattern shows if any negative behavior associated with financial data or social media profile data. (*e.g. Money transfer to illegal entities or user's social media profile linked to drug dealer profile)*	15%	100 Refer to Table 3
2	**Aggregated**	Aggregated view. a combined, weighted view on multiple risk views. Identify if an activity is suspicious faster, based on previously-recognized patterns and aggregated view of the entities. *(e.g. If a legal threshold for cash deposit in the bank account is 5000 USD and a user deposits multiple cash deposits less than 5000 for a while, then the system will create an aggregated view of customer transaction profile)*	20%	100 Refer to Table 4
3	**List Matching**	List matching. customers, accounts, and transactions can be matched against blacklists (provided by Office of the Foreign Asset Control) or defaulters lists (provided by the central or federal bank), and the results can be shown in risk views. If any of the social media profile directly or indirectly linked to any of the blacklisted people. *(e.g. If John Dave is a criminal and blacklisted by OFAC* (Office of the Foreign Asset Control) *for terrorist activities then List Matching filter will sync with OFAC list on real-time and any transaction made by John Dave will be on hold till the alert is examined)*	25%	100 Refer to Table 5
4	**Key AML noise phrases (Suspicious and Money laundering keywords)**	Text mining is the measurement of the various qualitative and quantitative attributes of textual (unstructured data) related to financial crimes. Collection of online data from social media and other online platforms in the form of unstructured text, web harvesting, and web data extraction (Batrinca & Treleaven, 2014). Text mining can be done on every word related to customer and words those are more related to money laundering can be clustered to mine meaningful insight. *(e.g. if user's social media conversation consists of appreciation to terrorist activity and the user is linked to Non-profitable Organization then the system creates risk score and creates alert)*	20%	100 Refer to Table 6

5		**Suspicious profile detection**	Any financial transaction related to blacklisted Customer, Account, Instrument, PEP (Politically Exposed Person). The profile can be identified as a suspicious profile. *(If any customer is linked to political exposed person in social media and unusual high-value transaction identified for that customer, then it creates a high score and generates alert)*(Choo, 2008).	20%	100 Refer to Table 7
		Total		**100%**	

Table 3. Risk Assessment Score. Behavior

	Behavior Subcomponents	Scenario	Assessment Score
Filter 1 . Behavior	Unusual Activity in comparison to previous data. Data are mostly derived out by comparing unusual transaction records with normal behavior norms(Gao & Ye, 2007).	Frequent transactions in comparison to previous transactions	Score out of 100
	Money transfer to the illegal entity or outside of industry entity	Money transfer to the blacklisted country	Score out of 100
	Unusual social profile network increase or decrease	Increase of irrelevant social profile count	Score out of 100
	Unusual conversation with comparison to previous data	The inclination of user conversation towards illegal social media posts	Score out of 100
	Unusual change of recency and frequency of activities	Multiple account creation from the same user	Score out of 100

Note. Please refer to Table 2(Risk filter components) and Filter number 1 for definition

Table 4. Risk Assessment Score. Aggregate View

	Aggregate View Subcomponents	Scenario	Assessment Score
Filter 2. Aggregate view	Aggregate view of cash deposit	Aggregated deposit of cash exceeds the previous record	Score out of 100
	Aggregate view of wire transfer	Aggregated wire transfer exceeds the previous record	Score out of 100
	Aggregate view of Cash Withdrawal	Aggregated cash withdrawal exceeds the previous record	Score out of 100
	Aggregate view of suspicious words on the social platform	An aggregated view of negative sentiments on the social media platform	Score out of 100
	Aggregate view of linked suspicious profiles	A complete view of linked profiles related to the customer	Score out of 100

Note. Please refer to Table 2(Risk filter components) and Filter number 2 for definition

Table 5. Risk Assessment Score. List Matching

	List Matching Subcomponents	Scenario	Assessment Score
Filter 3. List Matching	List from OFAC	OFAC issues list of blacklisted people. The business rule matches the name and based on matching it provides the score. If the name matches exactly then score comes 100 and its name matches partially then score comes 80.	Exact Matching=100 Partial Matching=80
	List from United Nations	As above	As Above

List from European Union	As above	As Above
List from World Bank	As above	As Above
Other official watch lists	As above	As Above
Country-specific sanction list	As above	As Above
Region-specific sanction list	As above	As Above

Note. Please refer to Table 2(Risk filter components) and Filter number 3 for definition

Table 6. Risk Assessment Score. Money Laundering Keywords

	Money Laundering Keywords Subcomponents	Scenario	Assessment Score
Filter 4 . Money Laundering Keywords	Terms related to the negative source of wealth	Source of money from illegal activities	Score out of 100
	Negative News	User attended a gathering which has negative news	Score out of 100
	Negative Key Words	User conversation or linked information consists of a negative keyword like “Drugs” or “Import of the illegal article”	Score out of 100
	Negative sentiments like support to terrorist activities	Sharing and support of news inclined towards illegal activities	Score out of 100
	Negative Industry	The profile is linked to industries like leather or ammunition.	Score out of 100
	Association with the bankrupt entity or illegal industry words	The profile is linked to a bankrupt company or customer.	Score out of 100

Note. Please refer to Table 2(Risk filter components) and Filter number 4 for definition

Table 7. Risk Assessment Score. Suspicious Profile

	Suspicious profile Subcomponents	Scenario	Assessment Score
Filter 5. Suspicious Profile	Geographic Patterns - Proximity relationships between apparently unrelated countries and location	Transfer from a user in the current country to another high-risk country and the user has no personal and professional relationship with risk profile countries.	Score out of 100
	Conversation Patterns - fictitious invoice numbers, fictitiously-generated transaction amounts	Profile with false information related to financial transactions.	Score out of 100
	Profile network Patterns – link to suspicious profile	Link to profile those marked as suspicious	Score out of 100
	Profile network Patterns – link to the political exposed person	The profile is linked to political parties and profile	Score out of 100
	Profile network Patterns – link to negative words e.g. Gambling and Drugs etc.	The profile is linked to the gambling profession	Score out of 100

Note. Please refer to Table 2(Risk filter components) and Filter number 5 for definition

4.3 Usage of Risk Scoring Model Framework

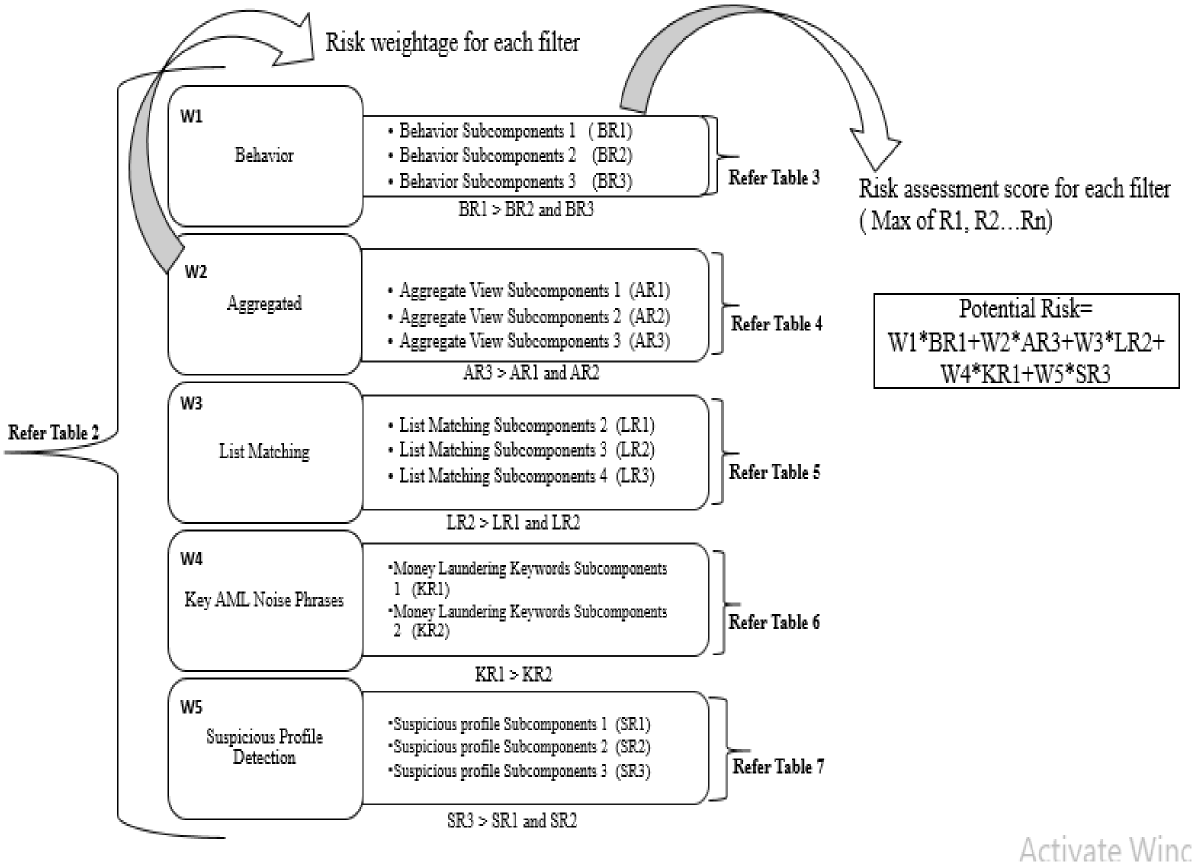
Risk weightage for each filter
W1
Behavior
• Behavior Subcomponents 1 (BR1)
• Behavior Subcomponents 2 (BR2)
• Behavior Subcomponents 3 (BR3)
BR1 > BR2 and BR3
Refer Table 3
Risk assessment score for each filter
(Max of R1, R2…Rn)
W2
Aggregated
• Aggregate View Subcomponents 1 (AR1)
• Aggregate View Subcomponents 2 (AR2)
• Aggregate View Subcomponents 3 (AR3)
AR3 > AR1 and AR2
Refer Table 4
Potential Risk=
W1*BR1+W2*AR3+W3*LR2+
W4*KR1+W5*SR3
Refer Table 2
W3
List Matching
• List Matching Subcomponents 2 (LR1)
• List Matching Subcomponents 3 (LR2)
• List Matching Subcomponents 4 (LR3)
LR2 > LR1 and LR2
Refer Table 5
W4
Key AML Noise Phrases
•Money Laundering Keywords Subcomponents 1 (KR1)
•Money Laundering Keywords Subcomponents 2 (KR2)
KR1 > KR2
Refer Table 6
W5
Suspicious Profile Detection
•Suspicious profile Subcomponents 1 (SR1)
•Suspicious profile Subcomponents 2 (SR2)
•Suspicious profile Subcomponents 3 (SR3)
SR3 > SR1 and SR2
Refer Table 7

Figure 2. Money Laundering Filter and It's Sub Components

The weight scoring formula is to calculate the potential risk of the customer. The value of the weight is used as a multiplier for the risk value. When risk values are used to compute the risk, weights are used to calculate the importance of a risk assessment score.

$$Potential\,Risk = \sum_{i=1}^{n}(W_i \times R_i)$$

Figure 3. Potential risk

Where Potential Risk = Total risk score of customer
Wi = Risk weightage for each filter i = I,..., n
Ri = Risk assessment score for each filter i = I,..., n
n = Number of risk assessment filter

Note that for each customer, the max score is taken for the Risk Assessment in the respective category. Under each risk filter component, the number of possible scores can be divided into smaller sections or areas.

Note. The parameters can be introduced or modified based on financial institutions' policies and regulations. For each filter sub-component, there will be a maximum score out of the list of parameters. If one profile matches more than 2 parameters then the Maximum score will be considered for that filter subcomponent and will be calculated for the final score.

The following table provides the risk score range to identify the risk category and it helps to promote the case to further investigation.

Table 8. Risk Category

This risk category table is a reference to the final potential score to decide whether a suspicious profile requires further investigation or not.

Minimum Risk Score	Max Risk Score	Risk Category	Further Action
0	30	Low	No
31	60	Medium	No
61	100	High	Yes

The risk category helps to filter the cases for further investigation. The cases with low risk will come to filter again with the aggregated view. It will compile all the views and comes to alter when it becomes significant. The event with the low score but frequent occurrence may accumulate to a high score for an alert.

5. Calculation of risk for Customer or Business Account with the help of Risk Assessment score and Weight

This can be better understood with the help of an example. John Smith is a Bank customer and he has an account with the Bank. The Bank needs to run the AML filter on John Smith's information to calculate the risk score based on his financial transactions and social media profile details. Below are the scenarios and risk core for John Smith to calculate the Potential risk score.

Table 9. Risk Calculation for customer profile

Risk Assessment Filters	Weight	Risk Assessment Score	Remark
Behavior	15%	55	▪ *Money transfer to an illegal entity or outside of industry entity* (John smith regularly transfers money to an account of the leather industry. But, John Smith works in Pharma Company). Based on the score matrix this event scores 55 out of 100. ▪ *Unusual social profile network increase or decrease* (John Smith added many new friends from a geo risk country and an unusual increase of profiles in the friend list.). Based on the score matrix this event scores 45 out of 100. Note. Score matrix can be repaired based on individual organization requirements. John Smith has two marked behaviors events and the max score (55, 45) is 55. So, the score of the Behavior risk assessment filter is 55. Reference form Table 3.
Aggregated	20%	45	Similar to the above. The score for *Aggregated Filter View* is 45. Reference from Table 4.
List Matching	25%	60	Similar to the above. The score for *List Matching Filter View* is 60. Reference from Table 5.
Key AML noise phrases (Suspicious and Money laundering keywords)	20%	90	Similar to the above. The score for *Key AML Noise Phrase Filter View* is 90. Reference from Table 6.
Suspicious profile detection	20%	100	Similar to the above. The score for the *Suspicious Profile Filter View* is 100. Reference from Table 7.

Refer to the expression in Equation (1)

Potential Risk Score= (.15*55) + (.2*45) + (.25*60) + (.2*90) + (.2*100)

=70.25 (The risk score is rounded off to 70.)

Risk Category. High (Reference to Table 8.)
This customer can be created as a case for further investigation and analysis by AML experts. The case management system must have a feedback system where the feedback should incorporate the changes in the scoring framework. If the score or alert is not accurate for any of the customer then the scoring framework must be updated to generate a valid score.

6. Insight

Based on the literature review of relevant research papers and personal experience in this area, this paper focuses on several key insights for the new generation AML solutions to handle money launders more effectively. This will help to mitigate financial security risks with the use of customer's social media data. Users of these insights can generate more discussion and methods to address money laundering scenarios. To determine filters or parameters for addressing different risk areas, organizations need to analyze each potential area to ensure that money laundering risks are being sufficiently considered and the organization's AML policies need to be restructured in the context of social media regulations. Although many organizations have considered social media profile check as one of the KYC (Know Your Customer) check and customer due diligence process, consideration of this data in the daily monitoring process is not widely implemented. Thus, organizations need to consider new areas in AML measurement policies to ensure that the solution is more effective to generate alerts(Reserve Bank of India - Reports, 2009). A standardized framework for all financial institutions and social media platform is required. This strategy will help to feed enough information to the monitoring system so that an accurate result can be derived from the alert generating engines of AML software.

7. Conclusion and Future Work

The money laundering policy plays an important role in banks due to its necessity. The measure on customer social media profile is rarely part of money laundering regulations. However, few banks consider social media profile checks as part of know your customer and customer due diligence process. In this paper, we provide a basic framework for identifying money laundering activity by creating a transactional profile and social media profile. We show firstly the whole process of AML activity and then the framework through which the solution can be extended considering the social profile network. We also discuss an extension of current AML solutions to have a better watch view. An important knowledge retrieved from our experience is that by selecting appropriate parameters, the solution can be customized and can be applied to detect Money Laundering cases from social networks as well. We used parameters that are widely used in the banking and financial industry. The study finds out that we have more research papers on financial transaction monitoring but there is very little research work done on suspicious social media profile identification. The monitoring solution can be more robust if we add more data from the social media platform. More data will give better insight into the customer and more parameters can be identified for the filter to have better decision points. The subcomponents are the pillars of primary filters and these subfilters can be modified based on organization policy. The business rules and boundary criteria for decisions can be enhanced based on industry and geography. Besides, the combination of subcomponents for parent filter helps to improve the accuracy in the detection of money laundering cases. The paper adds to the existing literature on improving the anti-money laundering framework and the inclusion of more parameters for each area.

References

Batrinca, B., & Treleaven, P. C. (2014). Social media analytics: a survey of techniques, tools and platforms. *AI and Society, 30*(1), 89–116. https://doi.org/10.1007/s00146-014-0549-4

Choo, K. K. R. (2008).Politically exposed persons &lpar;PEPs&rpar;&colon; risks and mitigation. *Journal of Money Laundering Control, 11*(4), 371–387. https://doi.org/10.1108/13685200810910439

Gao, Z., & Ye, M. (2007). A framework for data mining-based anti-money laundering research. *Journal of Money Laundering Control, 10*(2), 170–179. https://doi.org/10.1108/13685200710746875

Glass, N. B. (2018). *The leveraging of social media by corporate credit unions to enhance the detection and reporting of suspicious activity.*

Johnston, R. B., & Abbott, J. (2005). *Deterring Abuse of the Financial System: Elements of an Emerging International Integrity Standard* (Policy Discussion Paper No. 05/3). https://www.imf.org/en/Publications/IMF-Policy-Discussion-Papers/Issues/2016/12/31/Deterring-Abuse-of-the-Financial-System-Elements-of-an-Emerging-International-Integrity-18105

Kruisbergen, E. W., Kleemans, E. R., & Kouwenberg, R. F. (2015). Profitability, Power, or Proximity? Organized Crime Offenders Investing Their Money in Legal Economy. *European Journal on Criminal Policy and Research, 21*(2), 237–256. https://doi.org/10.1007/s10610-014-9263-5

Reserve Bank of India. (2009). *State Finances: A Study of Budgets of...* Reserve Bank of India. Retrieved June 23, 2020, from https://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=543#1R

Copyrights