ISM 6124 – Advanced Information Systems Analysis and Design

Fall Semester 2021

Hot Topic Report

Final Report

Anti-Money Laundering (AML)
Network Analytics in AML

Shabana Ajamal Hannure

U80532141

Oct 6th, 2021

Table of Contents

Introduction **3**
Purpose 4
Scope 5
Definitions, Acronyms, Abbreviations 7
Background: Money Laundering and Anti-Money Laundering 8
Design Overview **9**
Description of Problem 9
Challenges with Traditional Monitoring Method 9
Technologies Used 10
System Architecture: 10
Network analytics in the real world **11**
Step 1: Build the Smith network 12
Step 2: Create connections 13
Step 3: Infer relationships using non-traditional data sources 14
Network-based Surveillance **15**
Application of Network Analytics **16**
Graph Network Analytics **17**
Data Exploration 17
Single Source of Truth 17
Transparency and Explainability 17
Benefits of Network Analytics **18**
Increased Coverage 18
Identify Hidden Relationships 18
RiskBased Scoring & Prioritization 18
Holistic Investigation 18
Enhanced Network Visualization 18
Conclusion **19**
Network analytics is the future of AML 19
References **20**

Introduction

In the 2017 Correspondent Banking in Emerging Markets Survey2 of over 300 banking clients in 92 countries, more than a quarter of global survey participants claimed reductions in correspondent banking relationships (CBRs). Increasingly, correspondent banks are paying greater attention to their respondents' Anti-Money Laundering / Combating the Financing of Terrorism (AML/CFT) program effectiveness, Know Your Customer and Customer Due Diligence (KYC/CDD) programs, and their jurisdiction-related obligations to comply with AML/CFT requirements. In the Survey, private sector emerging market banks identified assistance with understanding and adapting to new global standards as one solution component that would be most useful.

Rapid developments in financial information, technology, and communication have facilitated the movement of money anywhere in the world with speed and ease. This makes the task of combating money laundering more urgent than ever. Every year, US$800 billion to US$2 trillion is laundered. This is about 2−5 percent of the global GDP.3 To address this challenge, governments and regulators across the world have come up with legislation and guidelines that have evolved over the years. AML compliance for banks is no longer a standalone function but one that is increasingly complex. Its scope covers functions such as legal, risk, operations, and tax. With ignorance no longer being excused, minimum compliance with regulatory obligations is no longer enough.

Banks face increased challenges in meeting heightened expectations The focus on holding financial services firms accountable for deficiencies in their AML compliance programs has been increasing across the globe, with heavy civil and criminal penalties for failure to comply. These penalties can be more pronounced for banks with a presence across various jurisdictions requiring them to comply with regulatory expectations in these countries and their home countries. As a result, AML compliance efforts may need to go beyond responding to incidents to a proactive and integrated approach to prevent compliance failure. In the survey responses, banks have identified increased regulatory expectations and enforcement of current regulations and regulatory directives/ compliance with multi-jurisdictional requirements as key challenges. AML compliance management is also turning out be a battle for the best talent; often the first line of defense against money laundering is staff with specialized skills that can monitor transactions. The absence of such talent can pose challenges in AML compliance. This is also reflected in the concerns expressed by the respondents. Historically, AML programs have been incident driven with lean teams managing response to events or changes in regulatory developments. Taking an enterprise-wide approach enables organizations to increase the effectiveness of their prevention initiatives and streamline their financial crime-related activities. Breaking down silos and taking a cross-enterprise view of customers and transactions also make it harder for criminals to exploit gaps amongst business systems, databases, and countries.

Purpose

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

Scope

Money laundering is a serious problem for the global economy, with the sums involved variously estimated at between 2 and 5 percent of global GDP.1 Financial institutions are required by regulators to help combat money laundering and have invested billions of dollars to comply. Nevertheless, the penalties these institutions incur for compliance failure continue to rise: in 2017, fines were widely reported as having totaled $321 billion since 2008 and $42 billion in 2016 alone.2 This suggests that regulators are determined to crack down but also that criminals are becoming increasingly sophisticated.

Customer risk-rating models are one of three primary tools used by financial institutions to detect money laundering. The models deployed by most institutions today are based on an assessment of risk factors such as the customer's occupation, salary, and the banking products used. The information is collected when an account is opened, but it is infrequently updated. These inputs, along with the weighting each is given, are used to calculate a risk-rating score. But the scores are notoriously inaccurate, not only failing to detect some high-risk customers, but often misclassifying thousands of low-risk customers as high risk. This forces institutions to review vast numbers of cases unnecessarily, which in turn drives up their costs, annoys many low-risk customers because of the extra scrutiny, and dilutes the effectiveness of anti-money laundering (AML) efforts as resources are concentrated in the wrong place.

In the past, financial institutions have hesitated to do things differently, uncertain how regulators might respond. Yet regulators around the world are now encouraging innovative approaches to combat money laundering and leading banks are responding by testing prototype versions of new processes and practices.3 Some of those leaders have adopted the approach to customer risk rating described in this article, which integrates aspects of two other important AML tools: transaction monitoring and customer screening. The approach identifies high-risk customers far more effectively than the method used by most financial institutions today, in some cases reducing the number of incorrectly labeled high-risk customers by between 25 and 50 percent. It also uses AML resources far more efficiently.

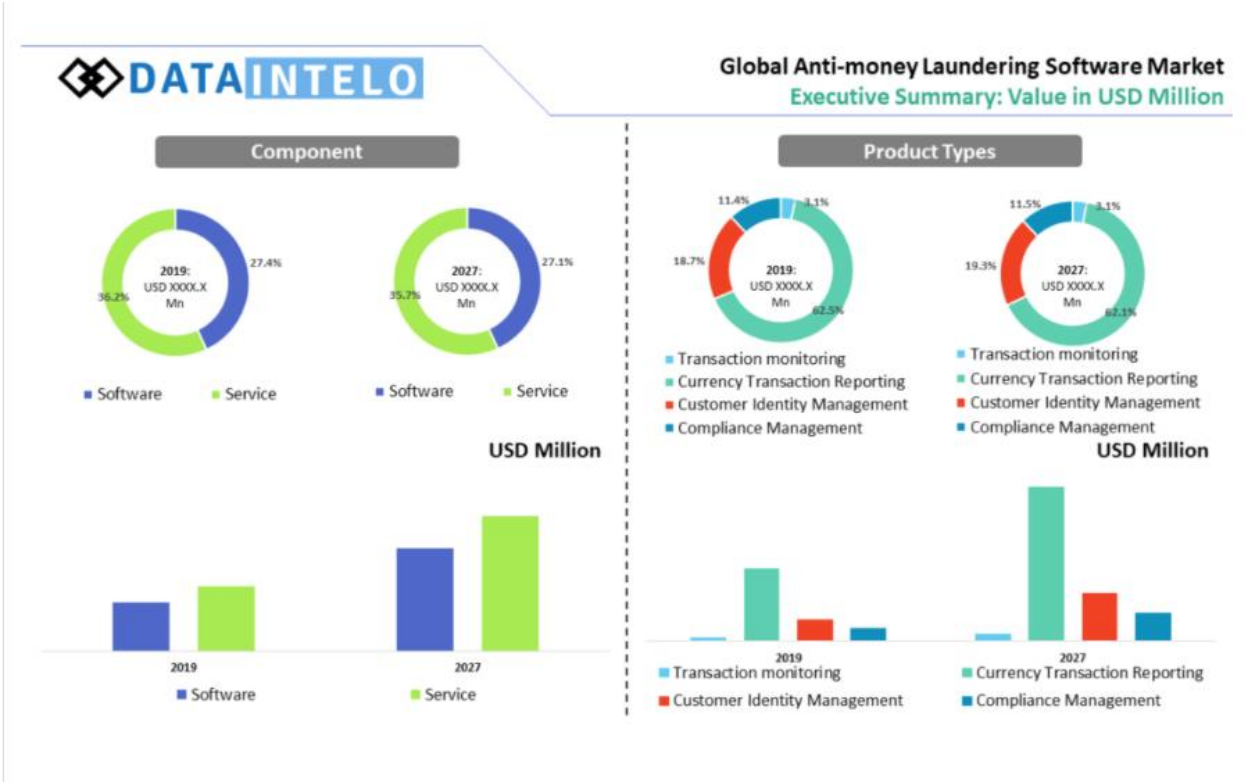


Image Source: https://dataintelo.com/report/anti-money-laundering-software-market/

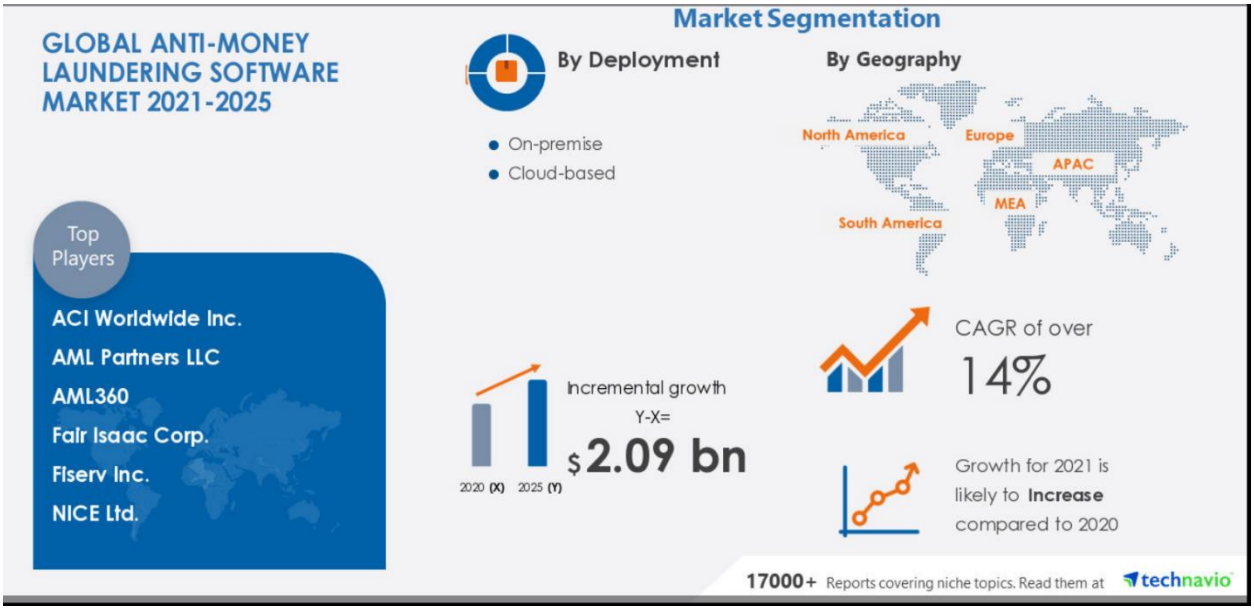


Image Source: https://www.prnewswire.com/news-releases/anti-money-laundering-software-market-to-grow-by-usd-2-09-billiontechnavio-301347408.html

Definitions, Acronyms, Abbreviations

AML Anti-money laundering

BCBS Basel Committee on Banking Supervision

BIS Bank for International Settlements

CBR Correspondent banking relationship

CDD Customer due diligence

COSO The Committee of Sponsoring Organizations of the Treadway Commission

CPMI The Committee on Payment and Market Infrastructures

CFT Combating the financing of terrorism

EDD Enhanced due diligence

FATF Financial Action Task Force

FIU Financial intelligence unit

FSB Financial Stability Board

FT Financing of terrorism

GPN Good Practice Note

IFC International Finance Corporation

IMF International Monetary Fund

KRI Key risk indicators

KYC Know your customer

KYCC Know your customer's customer

ML Money laundering

MTO Money transfer operators

PEP Politically exposed person

STR Suspicious-transaction report

WBG World Bank Group

Background: Money Laundering and Anti-Money Laundering

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

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

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

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

Design Overview

Description of Problem

Money laundering has potentially devastating economic, security, and social consequences. It provides the fuel for drug dealers, terrorists, illegal arms dealers, corrupt public officials, and others to operate and expand their criminal enterprises. Criminal elements in today's technology-driven society are using every means available at their disposal to launder the proceeds from their illegal activities. While many anti-money laundering (AML) solutions have been in place for some time within the financial community, they face the challenge to adapt to the ever-changing risk and methods in relation to money laundering (ML).

Challenges with Traditional Monitoring Method

The traditional way of surveillance not only generates a massive number of cases, but also has several fundamental issues, such as:

 Lacks Holistic Surveillance: A specific behavior can be an indicator of suspicious activity and should be assessed in conjunction with other indicators, not in a silo. When cases are created for the entity, as soon as there is a suspicious rule hit, the surveillance process is not factoring the behaviors that occurred before and after the specific activity. This means the surveillance process is lacking a holistic view, which makes the detection process ineffective to some degree.

 Siloed Investigation: For flagged transactions, AML staff investigate the specific circumstances surrounding the transaction. High-risk products, areas of operation, business lines, and basic customer information can influence the amount of transaction testing. During the investigation process, users do their best to include any related cases found manually, which is primarily based on customer and account. Although this helps investigators include previous cases for that customer, this does not factor other related, loosely related, or hidden suspicious behaviors. These manually linked cases may provide some additional information about investigated entity; however, it may not quantify overall risk.

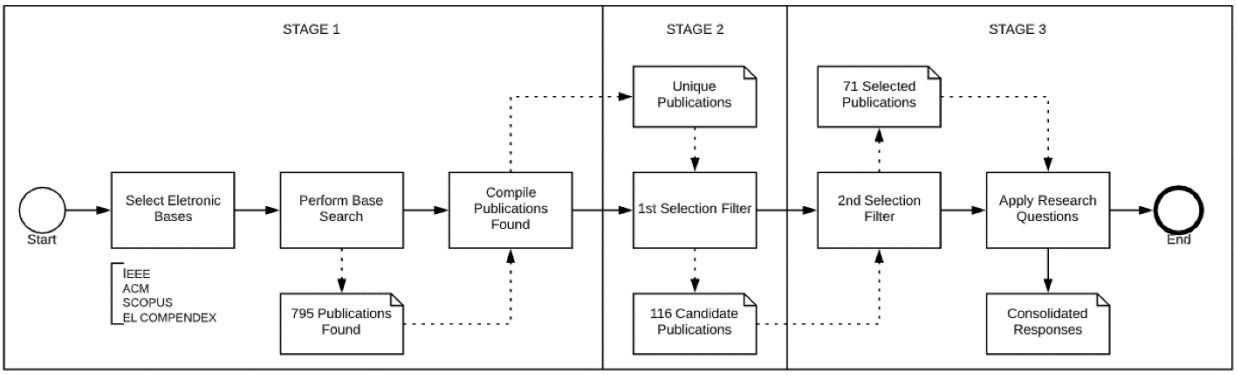
 Too Much Information: Data is collected during the transaction testing process and during follow up investigations. Manual linkage of related cases adds a significant amount of data, which investigators will have to study as part of their investigation. This may be very hard to make sense of in absence of a proper network view of all the involved parties.

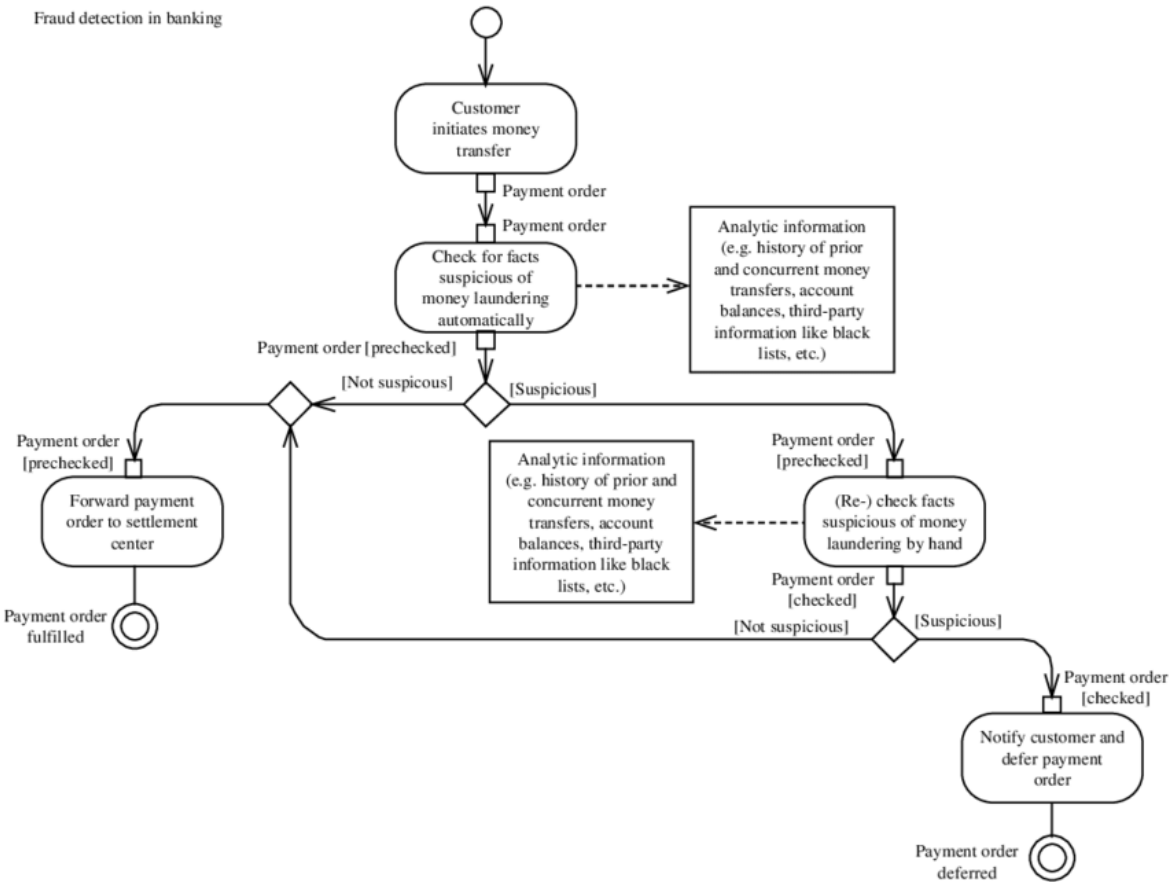
In summary, the traditional way of pattern detection leads to an enormous number of cases, which then require analysis of several other systems for a comprehensive investigation. Overall, this leads to longer investigation periods and makes the entire process highly inefficient.

Technologies Used

Network analytics has the potential to significantly improve the effectiveness of AML programs. Banks need the right external data sources and network science capabilities, and deep subject matter expertise, to get the benefits.

System Architecture:





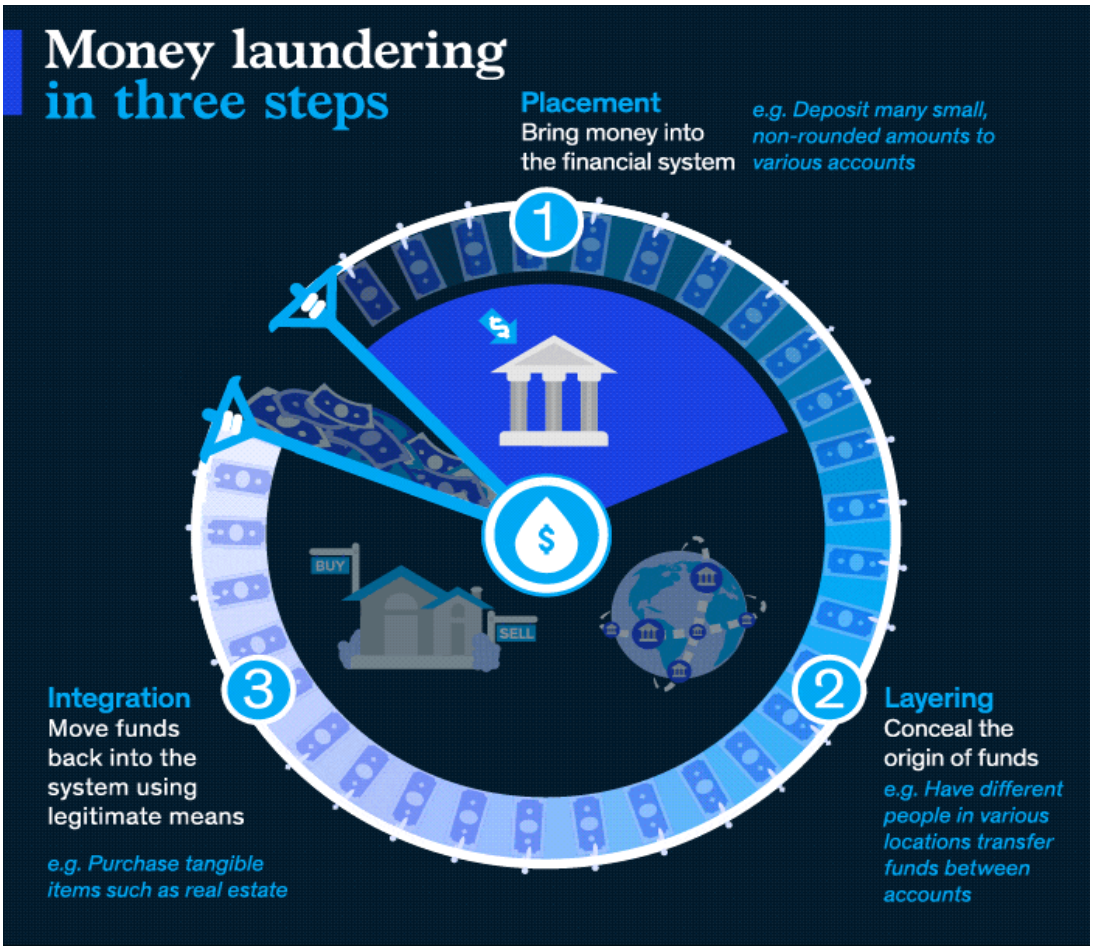
Activity Diagram for Fraud Detection

Network analytics in the real world

Network analytics examines the connections between related entities to better illuminate relationships. Instead of analyzing an individual, subcomponents of the network are reviewed for similarity to known methods of money laundering and atypical customer behavior.

Networks are formed by links between customers and related activity. These (sometimes inferred) links can be internal data, such as account transfers or joint ownership, or external data, such as a shared address or common use of the same ATM.

Network analytics compliments existing machine learning and fuzzy logic-based approaches that many banks use for AML monitoring. Network statistics (for example, connectivity) for each customer can be used as an input to improve the accuracy of customer risk rating or transaction monitoring models. Fuzzy logic-based approaches that resolve customer identities can also be improved by looking at how closely accounts are connected. In addition to improving the effectiveness of existing techniques, network analytics provides investigators with new capabilities. For example, community detection algorithms can identify the presence of customer groups that could be indicative of criminal behavior.

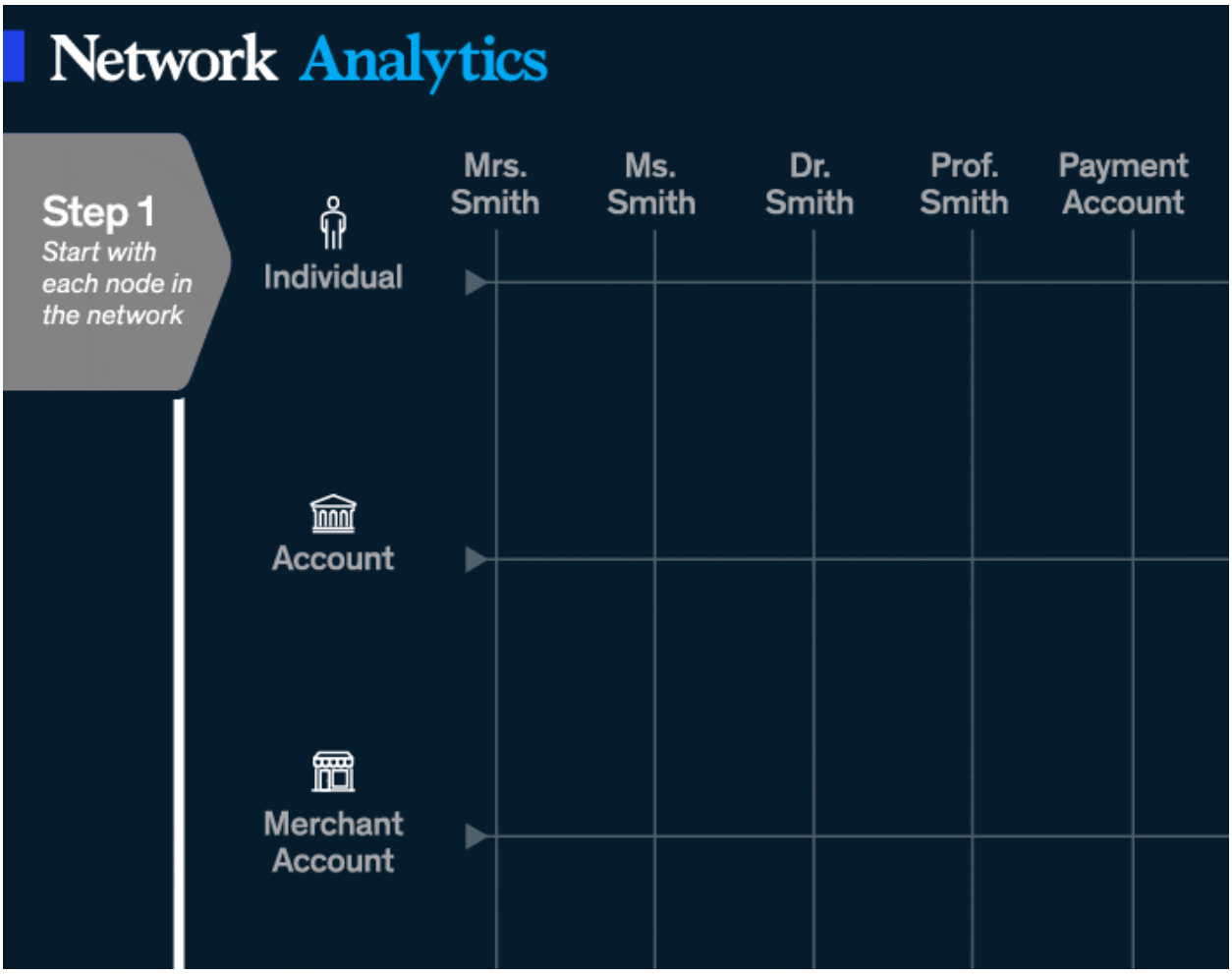


For example: The Smith family is laundering money by dividing large transactions into small deposits, filtered through online bill payments into temporary accounts. The payments are then used to purchase a boat which is quickly resold for cash—creating a paper trail to clean the money.

Network analytics can help identify the Smith family's illegal activities. Here's how it works:

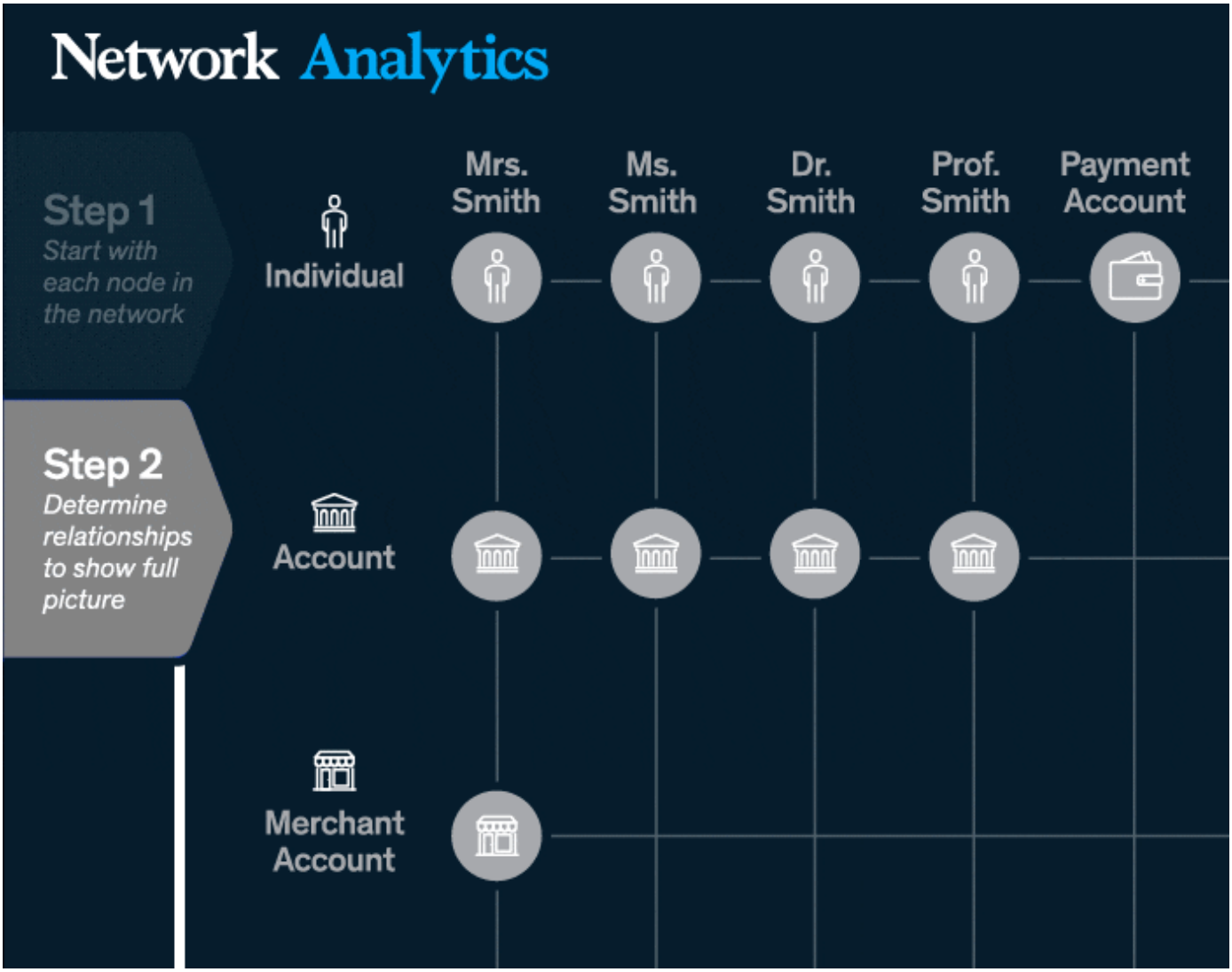
Step 1: Build the Smith network

Begin with Mrs. Smith and identify all other entities, including accounts and people, that she is connected to.



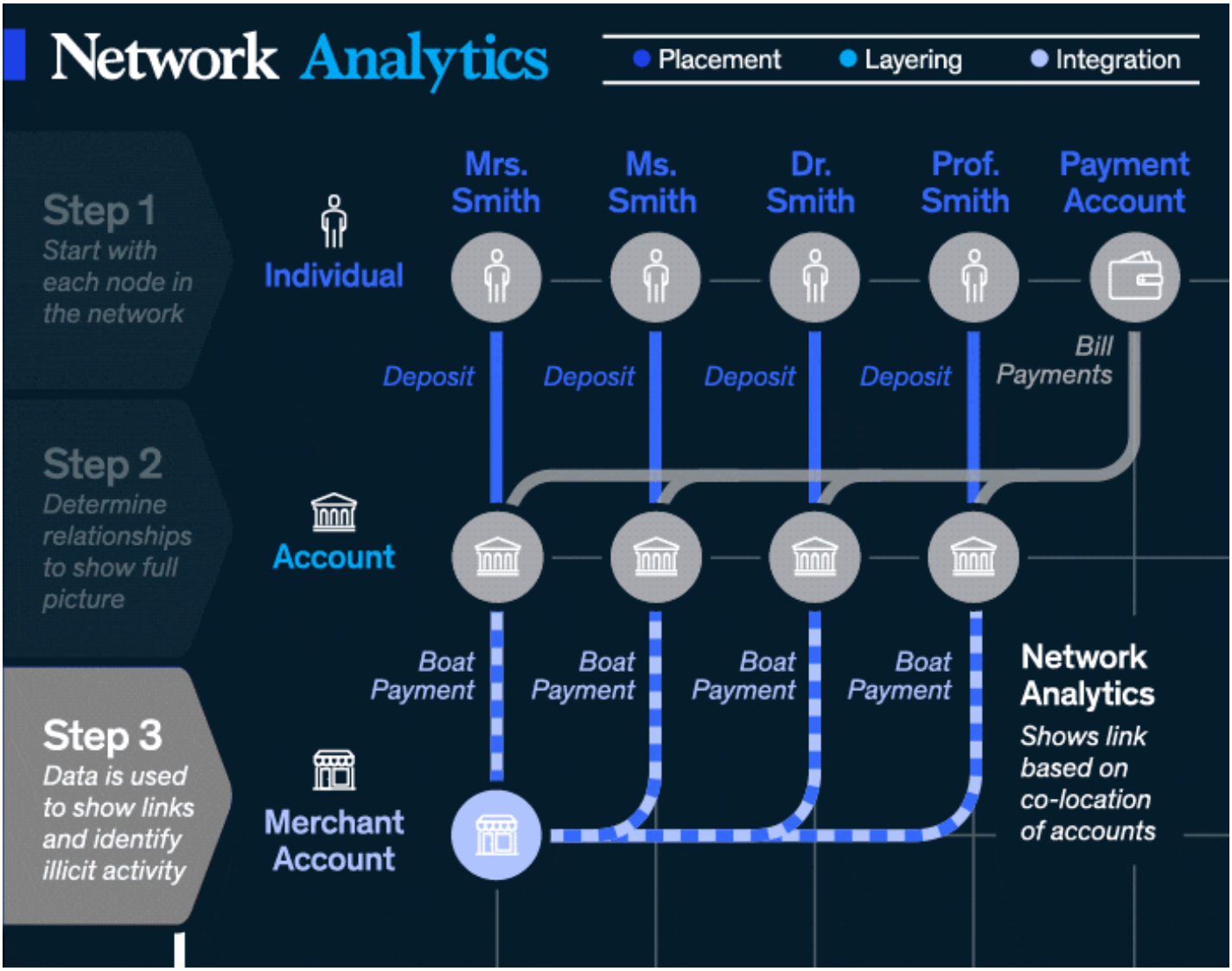
Step 2: Create connections

Next, add the relationships between the individuals, their respective accounts, and any related activity showing payments made within the system to show the flow of funds.



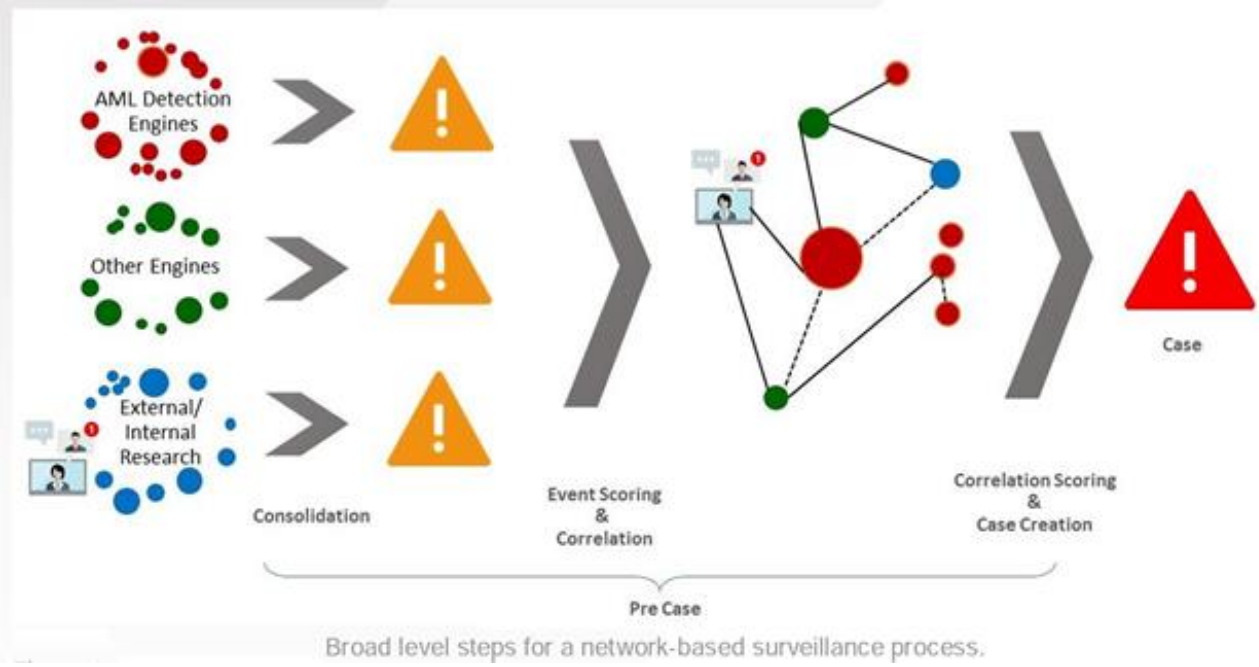
Step 3: Infer relationships using non-traditional data sources

Use enriched data about individuals and their related accounts in order to uncover inferred connections that show suspicious or anomalous activity that might suggest money laundering.

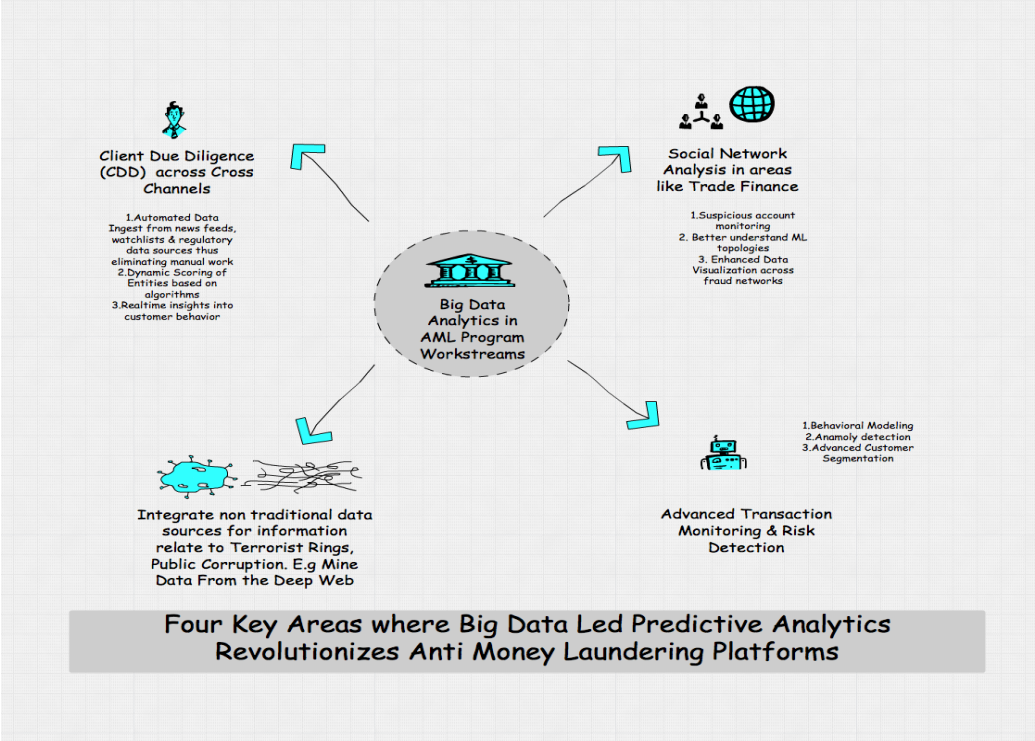


Network-based Surveillance

The purpose of network-based surveillance is to leverage an optimization layer for all the risk indicators (events) to apply a risk-based assessment. This will further allow a comprehensive entity focused case to be created for investigation



Broad level steps for a network-based surveillance process.



Application of Network Analytics

The different machine learning and A.I. techniques work with varied efficacy on a range of fraud detection problems. For example, neural network based face recognition systems work well for identity verification as part of a KYC onboarding routine and can help cut identity fraud. Network analytics lends itself well to identify suspicious relationships and transaction behaviour. We list 4 kinds of frauds which network analytics have proved effective for.

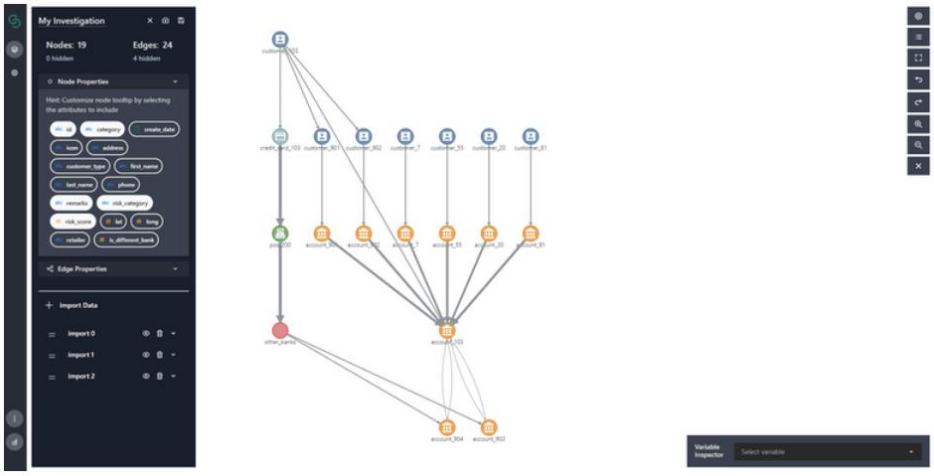
Fraud Rings: Fraud rings can consist of ten to thousands of criminals devoted to committing a specific type of fraud. This can include identity theft, mail or tax fraud, or forgery. These organised syndicates engage in a wide range of illicit behaviours including cheque and signature fraud, claiming false loan applications or using stolen credit cards.

Synthetic Identities: Synthetic Identity fraud happens when criminals combine real and fake information to create a new identity. This new identity is then used to open new accounts or make fraudulent purchases. The identities are also used to pump up the credit score of fake IDs to extend their credit. Accounts are often used as mule accounts to facilitate other illegal activities while hiding under the radar of the risk and compliance teams.

Account Takeover: In this type of fraud, a criminal takes control of an account that belongs to a bank customer. They then use the customers' information to make unauthorized transactions, possibly siphoning the funds over time to an overseas account which makes it hard for remedial actions to be taken.

Insurance Fraud: Insurance fraud includes false quotes and claims, inflated claims, or disaster fraud. These can be committed by organized groups to steal sums through fraudulent business activities

Graph Network Analytics



Besides having access to a wide range of network science algorithms, there are multiple benefits of adopting a network approach in fraud investigation and as part of a data exploratory process.

Data Exploration

Visualizing connections as a graph often helps in decision-making and provides better clarity and context than information in tabular form. This increases the efficiency of incident response teams and makes complex relationship structures more easily understood.

Single Source of Truth

Traditional methods of manual screening involve a long and tedious process since data is often stored in multiple different silos. Graph database solutions allow multiple different types of data to be stored in a single source of truth. Information on a particular customer's behaviors and fraudulent activities can be easily queried and retrieved.

Transparency and Explainability

Obtain better transparency and explainability with clear graphical evidence. As regulations and requirements on machine learning explainability and fairness grow, network science offers a good middle ground between accuracy and explainability.

Pattern matching is a relatively simple idea to grasp and many graph techniques are grounded on strong mathematical and statistical theory

Benefits of Network Analytics

Increased Coverage: Instead of investigating each risk indicator (event), network-based pattern detection allows for prioritization of risk events, thus increasing the monitoring coverage.

Identify Hidden Relationships: Party relationships can be defined based on tightly or loosely related links. This helps identify hidden relationships at the surveillance layer itself, which may have been missed during investigation.

RiskBased Scoring & Prioritization: Networkbased multiple layer correlation risk scoring, not at case level, but at individual event and entity level too.

Holistic Investigation: process allows for Since correlated entities and events are linked and present case information, this allows for investigation from any entity perspective

Enhanced Network Visualization: Now that relationships are identified and enriched leveraging both internal and external data, much more advance network visualization can be used to determine bad entities.

While this new way of monitoring means a much more efficient AntiMoney Laundering and Anti-Terrorist Financing program, organizations should be careful about the level of network link to be used for correlation. If not thought through, this can lead to a much more complex case and might 'over help' investigators. Appropriate training, future need for delinking ,and information sharing between analytics and Financial Investigation Units should be considered when getting into this new program. Lastly, the subsequent phase would be to apply machine learning to identify new hidden relationships, statistical techniques for scoring and determine case promotion threshold based on historical information.

Conclusion

Network analytics is the future of AML

Network analytics has the potential to significantly improve the effectiveness of AML programs. In practice, statistics from a network (for example, how closely it resembles a known money-laundering typology) would be incorporated into existing customer-risk rating and transaction monitoring models as inputs to improve model accuracy. New capabilities such as community detection would help accelerate investigations and identify hidden risks.

Network analytics takes time to get right and can require an enormous amount of computational power to sift through all current and past customer relationships. Historically, uniquely identifying a customer across systems to build links was also quite difficult. But this has changed over the past three to five years as banks have invested heavily in data infrastructure and built unique customer identifiers that are shared across systems. Scalable infrastructure (for example, Hadoop, AWS) has also provided institutions with more storage and computational power—enabling new use cases including network analytics.

Start by building a network of existing customer links by using account transfers, shared account ownership, and payments to build linkages both internally and to external institutions using the destination account number. Then create inferred links between customers by looking at shared addresses, employer, or social media data. Although often the target state, an enterprise grade graph database is usually not required—data can be stored in a standard relational database to get started. Even without advanced analytics, creating this database of links will accelerate investigations and provide data scientists with a rich asset that can be used for AML, in addition to a wide variety of other use cases (for example, marketing).

To take full advantage, most institutions will need to build capabilities in network science as the tools may be unfamiliar to even experienced data scientists. This will unlock a significant opportunity to improve both customer risk rating and transaction monitoring. The secrets to success are having the right external data sources and network science capabilities, and using deep subject matter expertise to inform model development.

References

1. Use Cases: Anti-Money Laundering

2. A Reference Model for Anti-Money Laundering in the Financial Sector, F. Timm, A. Zasada, Felix Thiede, Published in LWDA 2016, Computer Science, Business

3. Anti-money laundering software : Wikipedia

4. Building a Reference Model for Anti-Money Laundering in the Financial Sector Felix Timm1, Andrea Zasada1, Felix Thiede1 1University of Rostock, Institute of Computer Science, Rostock, Germany

5. Anti-money laundering technology must operate in a collaborative ecosystem : Link

6. What is Machine Learning? by IBM Cloud Education, July 2020

7. Derisking machine learning and artificial intelligence, February 2019

8. Institute of the Future by Dell Technology, August 2019

9. https://www.mufg.jp/dam/ir/presentation/2018/pdf/slides190219_en.pdf

10. https://www.ibm.com/downloads/cas/WKLQKD3W

11. https://www.federalreserve.gov/newsevents/speech/brainard20210112a.htm

12. https://www.federalreserve.gov/newsevents/pressreleases/bcreg20210329a.htm

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

    https://www.researchgate.net/

14. Risk Transforming approaches to AML and financial crime, September 2009, McKinsey & Company