MASTER OF SCIENCE (MSc) IN APPLIED RISK MANAGEMENT - INTERNAL AUDIT

MONEY LAUNDERING, ISSUES, EFFECTS OF BANK FRAUD AND CORRUPTION AND ROLE OF INTERNAL AUDIT

TUTOR: YIANNIS DRACOULIS

Dimou Vasiliki - 171006
UNIVERSITY OF ATHENS
2020

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Εθνικόν και Καποδιστριακόν
Πανεπιστήμιον Αθηνών
ΙΔΡΥΘΕΝ ΤΟ 1837

ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ ΚΑΙ ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΟΙΚΟΝΟΜΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών «ΔΙΟΙΚΗΣΗ ΟΙΚΟΝΟΜΙΚΩΝ ΜΟΝΑΔΩΝ»

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Money Laundering,
Issues, Effects of Bank Fraud and Corruption and Role of internal audit

Dimou Vasiliki

Yannis Dracoulis

ATHENS
06/2020

Περιεχόμενα

Acknowledgement

I would like to extend a distinctive thanks to my supervisor Professor Yiannis Dracoulis for the support and help during the project and the process of finalizing the thesis. Furthermore, I would like to give a special thanks to my family, they did not only raise me, but also overstretched themselves over the years for my intellectual and educational development.

Abstract

Given the interdependencies in today's markets, it is extremely likely that somewhere doing business with a company that is not effectively managing the risks of fraud, corruption, and other unethical business conduct. That is risky business. The pressure to achieve growth and develop new revenue opportunities is driving teams and individuals toward these risks and pushing them to unethical behavior themselves. On the other side, the threat posed by cybercrime to individuals, banks and other online financial service providers is real and serious. Through phishing, unsuspecting victims' Internet banking usernames and log in credentials are stolen and their accounts robbed. In addressing this issue, commercial banks and other financial institutions use a genetically similar approach in their Internet banking fraud detection systems. Internet banking fraud detection systems used by banks have several limitations that affect their efficiency in curbing fraudulent transactions in online banking.

Firstly, the banks' security systems are focused on preventing unauthorized entry and have no way of conclusively detecting an imposter using stolen credentials. Also, updating these systems is slow and their maintenance is labor-intensive and ultimately costly to the business. A major limitation of these rule-bases is brittleness; an inability to recognize the limits of their knowledge. In the main part of this thesis, we highlight the importance of looking at the "big risk picture" of the incident response process, and not just focusing on one technology at a time, we will deal with the issue of Money Laundering (ML). The abilities and skills of internal auditors suit them well for the war against money laundering. Forensic accounting skills, as well as audit expertise, are needed to help in combating this crime. The development of internal policies, procedures, and controls to prevent money laundering fits within the accountant's abilities and expertise. Money laundering can be defined as a process in which illegally obtained money (e.g. from drug trafficking, terrorist activity or other serious crimes) is given an appearance of having originated from a legitimate source. Money laundering is now taking place, only, in a high-tech global environment. Money laundering represents a derivative form of crime. This research will provide background and recent developments in efforts to combat money laundering, as well. We will try to compare the current combat between USA and European authorities, regulators, and processes. Finally, we will present two examples of Bank fraud cases/scandals which forced the American and European boards to revise, ensure and empower the audit lines, immediately.

Keywords

Money Laundering, fraud, crime, investigation, compliance, audit check, regulators

Statement of Authorship

Except where explicit reference is made in the text of the thesis, this thesis contains no material published elsewhere. No other person’s work has been relied upon or used without due acknowledgment in the main text and bibliography of the thesis.

1.Introduction

The banking sector is being reformed by globalization, innovation, customer needs and competition. Due to the development of a knowledge-built economy and the emergence of the latest information and communication technology, financial institutions particularly the banking industries have experienced thought-provoking changes during the last decade. Fraud can encompass waste and abuse, improper payments, money laundering, terrorist financing, public security, and cybersecurity. In the past, organizations had to take a fragmented approach to fraud prevention, using business rules and rudimentary analytics to look for anomalies to create alerts from separate data sets. The last ten years have seen a steady shift from traditional show-off hacking towards cybercrime with great economic consequences for society.

According to the Wisdom (2012), Information and Communication Technology, the most significant factor in the forthcoming development of the banking industry, enhances banks' ability to produce sophisticated products, to have superior market structures, to diversify their markets and to expand globally. But also, the cost of unethical behavior has never been higher, according to 'Fraud and corruption — the easy option for growth?' survey from EY (2015). Over the past decade financial scandals and large lawsuits have seized international headlines and brought increased attention to operational risk. Although banks have faced operational risks throughout the history, the attention of operational risk management has increased noticeably in recent years (Sapienza, P., & Zingales, L. 2012).

Furthermore, Darlington (1999) states that over the past three decades, customers' needs have changed significantly: customers are demanding simplicity in their daily banking services together with maximum security and safety. This trend is overseen by responsible authorities who step up their minimum requirements for risk management of financial services and, among other things, require regular risk assessment of current and emerging threats. The retail banking system, which consists of physical branches, is now being threatened by information and communication technologies characterized by automated systems of interaction with customers (mobile banking, call centers, automated teller machines (ATMs), online banking), that include relatively minimal costs and permit customers to select from the alternative delivery channels (Keivani et al., 2012).

To this point we have to mention the clear notice of the Global Banking Fraud survey, by KPMG in May 2019 that ‘In contrast, the largest proportion of respondents said that globally the total cost, average cost and volume of internal fraud stayed the same or decreased in 2017 and 2018. This however, may not present a complete picture of the internal threat to a financial institution, as in our experience many external fraud incidents originate with experienced criminal operatives working with internal sources who have a detailed working knowledge of bank systems, processes and controls (and any control gaps or weaknesses. The potential harm of insider fraud can be as great, if not greater, than external fraud, given the ability of employees to exploit weaknesses in controls to target the most valuable assets of a bank. Banks should continue to take a proactive approach to detecting insider fraud.’

Managerial and regulatory focus in the financial industry has been intensified due to a number of extremely costly and highly publicized events. In recent history several banks have reported large losses due to both internal and external fraudulent activities, where the largest loss announcements exceeded one billion US dollars (Gapper, 2011).

Many of the events that have received attention and media coverage can be categorized as internal fraud. The risks of fraud, bribery and corruption remain widespread and we continue to see businesses failing to mitigate these risks effectively.

- More than half of all respondents, and 61% of respondents in rapid-growth markets, believe that bribery and corruption is widespread in their country. And yet 42% of respondents report that their company does not have an anti-bribery policy in place or didn’t know if there was one.
- Thirty-seven percent of respondents believe that the financial performance of businesses in their markets is often overstated. And yet 20% of respondents feel their management team at head office does not understand the business environment that they face, according to the same EY survey (2015).

It is known that tip-offs are the most common way that fraud, bribery and corruption are uncovered. And yet almost a quarter of respondents imply their company does not have a whistle-blowing hotline. Another point is that training is a critical method for communicating anti-corruption policies to employees, and yet over a third of respondents have not been trained.

As a result, recent rise in bank frauds calls for a tightening of security mechanisms. A strong system of internal control is the most effective way of fraud prevention. The banks should increase their efforts to raise the level of security awareness in their organizations to combat frauds.

Who Is the Typical Fraudster?

There are several studies that seek to "identify patterns among individuals who have committed acts of fraud". Some of the big four auditing companies worldwide have investigated the identity of a fraudster. The noticed characteristic is that "typically, a fraudster is perceived as someone who is greedy and deceitful by nature," however further analysis found that "many fraudsters work within entities for several years without committing any fraud, before an influencing factor – financial worries, job dissatisfaction, aggressive targets, or simply an opportunity to commit fraud – tips the balance."

According to the KPMG (2019), the "typical fraudster" is between the ages of 36 and 45, followed next by individuals between 46 and 55 years old. In terms of gender, men are the more likely perpetrators of detected fraud. According to KPMG, "the survey's finding that men commit more fraud than women seems a reflection on the gender make-up of companies generally" and the "gender gap in fraud perpetration may reflect women's under-representation in senior management positions and, as a consequence, fewer opportunities to commit fraud."

In terms of job function, the EY (2015) report finds that people most often entrusted with a company's sensitive information are able to override controls and thus are statistically more likely to become perpetrators. The report found that "most people involved in committing fraud work in the finance function" followed by those in the "chief executive's / managing director's office," followed by those in "operations and sales."

The effect of bank fraud

Fraud is a crime and is also a civil law violation. Many fraud cases involve complicated financial transactions conducted by 'white collar criminals' such as business professionals with specialized knowledge and criminal intent. Fraud has become one of the most monumental problems in recent times. As a matter of fact, banks have become the main target of conmen for survival. It is not understatement that only well managed banks especially with respect to fraud prevention would survive in the coming years.

The effect of bank fraud is dynamic and deals with:

- bank deposits (better appreciated from the standpoint of cash depletion)
- customers' perception of feeling secure and protected
- customer loyalty and stimulate switching behavior
- loss in revenue
- inability of staying competitive in a super-fast changing market.

From the above, it is now clear that highest the turnover of frauds, theft, defalcations and forgeries is in the banking system is capable of undermining the growth, development and stability of banks which at the moment seems to be doggedly affecting the financial sector of the economy.

Fraud Management, Prevention & Operations

To combat fraud, newer technology has been developed to predict conventional tactics, uncover new schemes, and decipher increasingly sophisticated organized fraud rings. This involves more than standard analytics; it applies predictive and adaptive analytics techniques – including a form of AI known as machine learning. By combining big data sources with real-time monitoring and risk profile analysis to score on fraud risk, fraud prevention has evolved to start turning the tides of losses.

Fraud detection in today's world involves a comprehensive approach to match data points with activities to find what is abnormal. Fraudsters have developed sophisticated tactics, so it's essential to stay on top of these changing approaches of gaming the system.

To identify and stop an array of fraud attacks and crime quickly and accurately – while improving customer and citizen experiences – organizations should follow four critical steps:

1. Capture and unify all available data types from across departments or channels and incorporate them into the analytical process.
2. Continually monitor transactions, social networks, high-risk anomalies, etc., and apply behavioral analytics to enable real-time decision making.
3. Instill an enterprise wide analytics culture through data visualization at all levels, including investigative workflow optimization.
4. Employ layered security techniques.

The fraud detection and prevention technology that fraud management chooses should be able to learn from complex data patterns. It should use sophisticated decision models to better manage false positives and detect network relationships to see a holistic view of the activity of fraudsters and criminals. Combining machine learning methods – such as deep learning neural networks, extreme gradient boosting and vector machines – as well as proven methods such as logistic regression, self-organizing maps, random forests and ensembles – has proven to be far more accurate and effective than approaches based on rules.

Business and governments alike have embraced technologies like data visualization and artificial intelligence to greatly reduce and even prevent the economical and reputational repercussions of fraud. Analysts and investigators work together, breaking down silos, scoring and prioritizing alerts based on severity, then route high-priority alerts for more in-depth analysis.

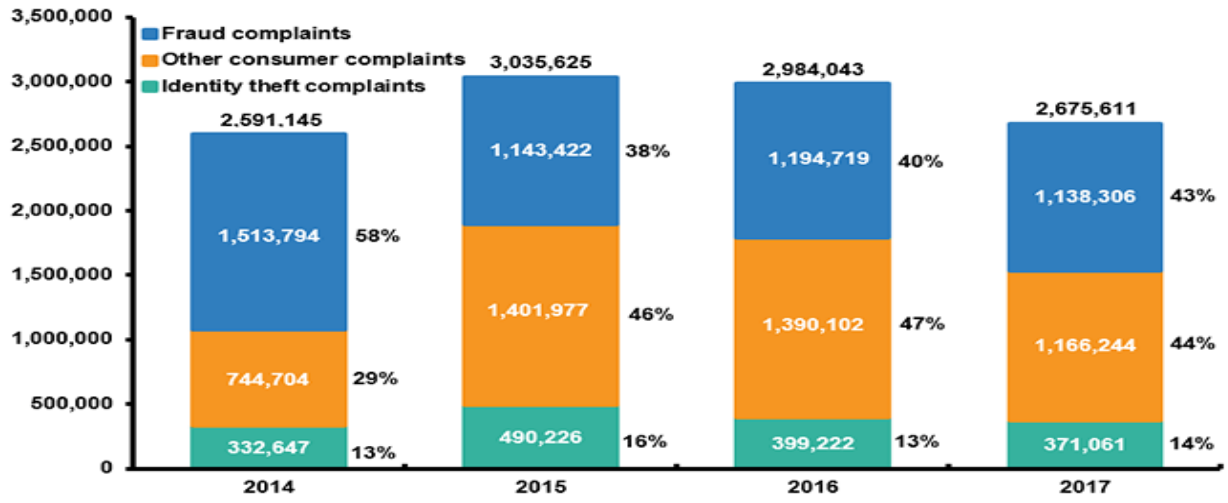
Following the new technologies, fraud management points out that the solution applies risk- and value-based scoring models to accurately score and prioritize alerts before they go to investigators. With the time saved, investigators can work more cases with greater efficiency, and focus on higher-value networks that generate a better ROI.

More accurate scoring also means fewer false positives – and that translates to less customer inconvenience and greater customer satisfaction. These techniques can also boost the efficiency of collection processes by identifying banking fraud losses that result from synthetic identities and have little to no chance of recovery.

Fraud detection on Banking

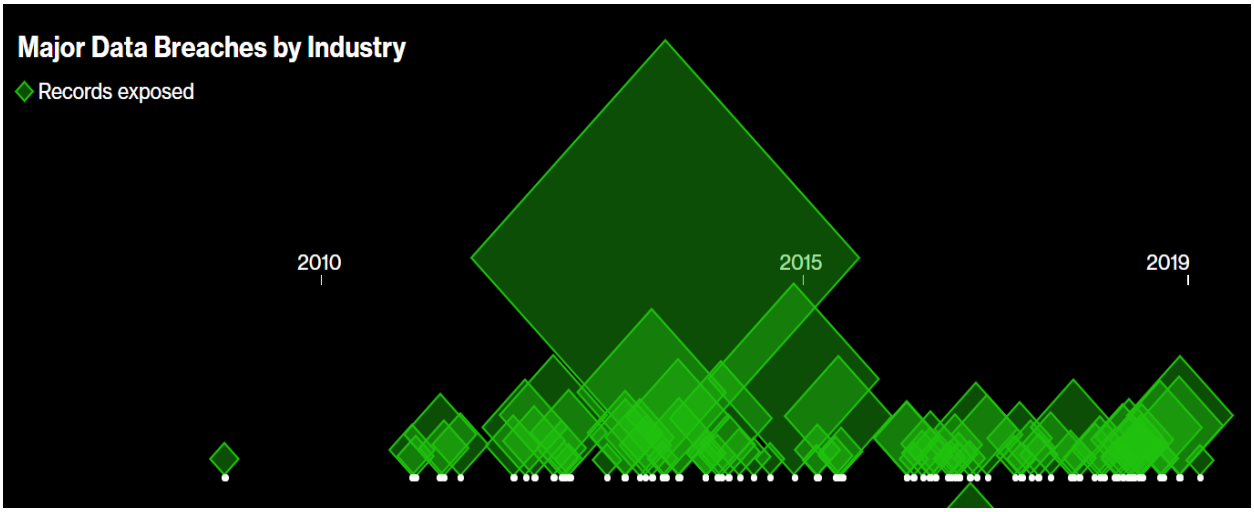
Fraud continues to be a problem for consumers and the banking industry. According to Javelin Strategy & Research in 2017, 16.7m people were victims of identity fraud and they lost an estimated $16.8bn.The Consumer Sentinel Network, maintained by the Federal Trade Commission (FTC), found that of the 2.7m identity theft and fraud reports received in 2017, 1.1m were fraud-related, costing consumers almost $905m. The median loss in these cases was $429. Imposter scams were the most reported type of fraud and accounted for $328m in losses.

The group also reported that credit card fraud was the most reported incident to the Consumer Sentinel Network, with 133,000 reports. Bank fraud accounted for 6.4% of the identity theft frauds. Primarily, most banks employ Rule-based Systems with manual evaluation for detecting fraud. Although these systems were doing a pretty decent job, in the recent years, they have become more inconsistent. That's because new fraud patterns are evolving rapidly and these systems are unable to evolve accordingly, allowing frauds to go undetected, and resulting in huge financial losses



Picture 1: Identity theft and fraud complaints, 2014-2017. Source: Federal Trade Commission, Consumer Sentinel Network.

The problem is not just the volume of incidents. Fraud schemes are constantly evolving, and organizations need to keep up with these changes. For the banking industry, this can be a challenging task. Not only are financial institutions a preferred target, they also absorb the losses in terms of revenue and consumer confidence when a fraud scheme goes undetected.



Picture 2: The worst corporate hacks of all time. Source: Bloomberg

Preventing bank fraud is deliberate activity that requires continuous update of technology, policies and procedures. On the technology side, AI-based models are no longer something just for tier 1 institutions and allow smaller organizations to enhance their existing rules-based internal controls and identify previously undetected and evolving fraud schemes.The key notice throughout these processes that technology is the only part of the solution for reducing bank fraud. Evolving policies and procedures must be in place to reduce the risk such as **Fraud Management & Intelligence** (FMI). FMI is a comprehensive, convergent and adaptive solution that enables organizations to manage frauds with a holistic approach, aligning the fraud prevention strategy with business objectives:

- **Comprehensive**: covering the strategic, tactical and operational levels (Security Governance, Risk Management, Fraud Protection), adapting fraud solutions to the organization's individual objectives in a unified way.
- **Convergent**: analyzing both internal and external insights at multiple levels (Potential Threats Confirmed Fraud), which help to increase business resilience.
- **Adaptive**: relying on both internal information (client) and related fraud patterns (sector) and collateral (profiling, clustering), identifying emerging fraud schemes not considered.

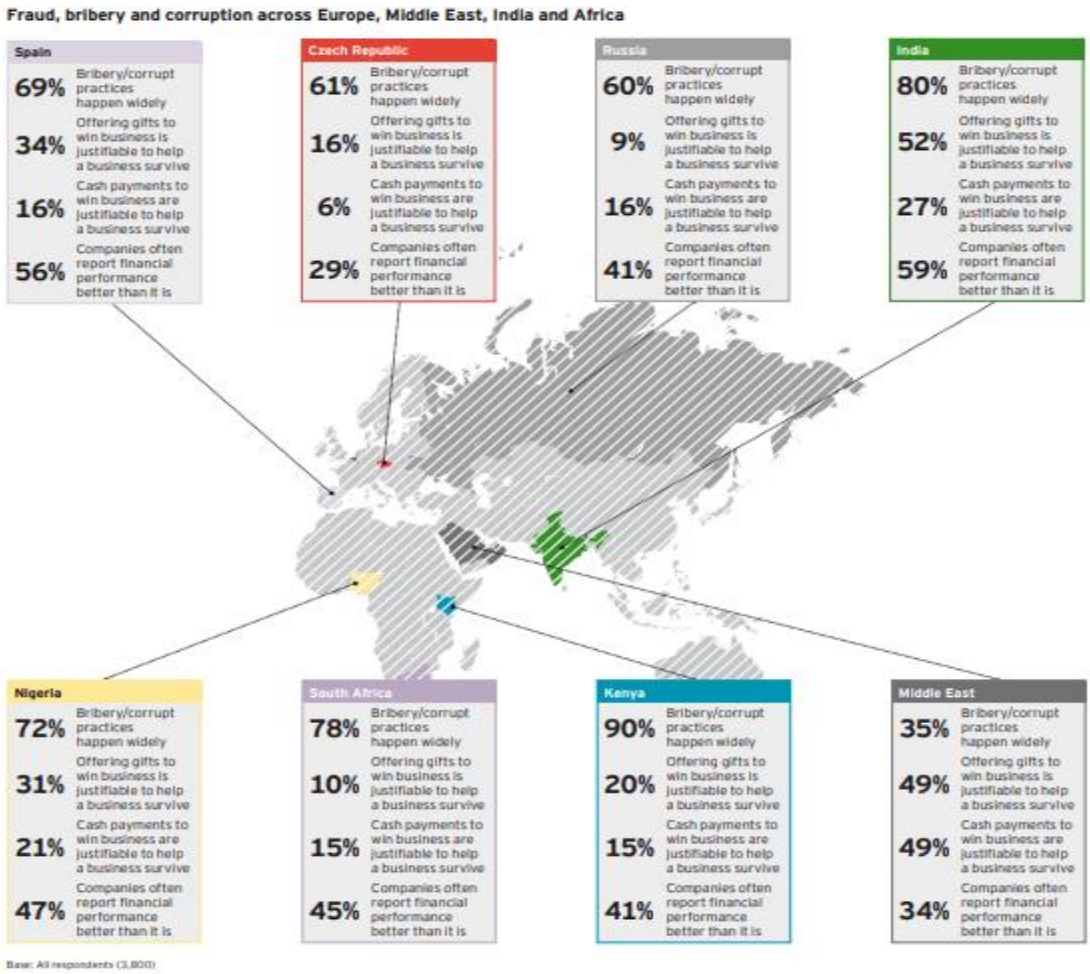
Thanks to holistic design and the risk management intelligence, FMI helps **prevent, detect, and mitigate** the impact arising from fraud affecting organizations.

2.Money Laundering

Is money laundering a crime itself?

The authorities normally define Money Laundering as the processing of the proceeds of crime to disguise their illegal origin, to avoid attracting attention to both the crime and the criminals involved. However, this is a very sloppy definition because it confuses what money laundering is, with some of the dubious reasons for doing it. In contrast to most other types of crime, money laundering is notable for the diversity of its forms, participants, and settings. It can involve the most respectable of banks unwittingly providing services to customers with apparently impeccable credentials.

So, we can come up with the note that the most serious aspect of money laundering is not the crime itself. The major problem is that it provides criminals access to the proceeds of their criminal endeavors and facilitates other criminal activities. Although money laundering, as we know it today, was nurtured in crime, it is not intrinsically criminal. Money laundering is an attempt to maintain financial privacy. It is the processing of financial transactions to disguise their provenance from prying eyes and grasping hands.



Picture 3: Global ratios

According to the United Nations Office on Drugs and Crime, the estimated amount of money laundered annually is between $800 billion - $2 trillion, which is 2-5% of global GDP. While this margin is huge, even the lower figure is serious and puts the recent global anti-money laundering efforts into perspective. We have dug into some of the biggest and most famous money laundering scandals in history and are here to give you the intriguing details and numbers.

The second act of government – the first act being to create money – is stealing it from the bearer, in the form of taxation or regulation or inflation or devaluation. Of course, fraudsters must be tracked down, but at what price? That price is not just a loss of liberty. There is a big group of experts which believe that there is a huge cost of complying with the anti-money regulations, and most of that cost will fall directly on businesses themselves.

- The USA dynamic

The International Monetary Fund (USA) estimates the global scale of money laundering as somewhere between $600 billion and $1.5 trillion annually.

Recent legislation under the USA Patriot Act (USAPA), passed in response to the events of September 11, 2001, has increased accountants' responsibilities in the fight against money laundering.

Accountants are increasingly more liable and responsible for assuring that companies have in place adequate systems of internal control. Such controls should include procedures to detect and prevent money laundering schemes. The position and role of accountants in the financial community necessitates that they take a proactive role in initiating organizational controls to expose such corruption.

- The European dynamic

The European Court of Auditors (ECA) has started an audit to examine the Union's efforts to tackle the laundering of dirty money, focusing specifically on the banking sector.

This year, 2020, the European Banking Authority (EBA) took on the tasks of leading, coordinating and monitoring the EU financial sector's fight against money laundering. It is the responsibility of the Member States to apply and enforce the EU's anti-money laundering AML rules through national legislation, and to prosecute money laundering offences. Within Europe, Europol estimates the value of suspicious transactions at around 1.3 % of EU GDP.

"Money laundering is increasingly a serious global threat, with criminals often seeking to launder money where controls are weakest, often far from the source of the funds", says Mihails Kozlovs, the member of the European Court of Auditors responsible for the audit. "Given the enormous scale of this criminal practice, including in the EU, and a number of recent high-profile scandals involving banks, we have decided to audit the effectiveness of the EU's action in the fight against money laundering in the banking sector"(Source: European Commission).

Background

Money laundering undermines the integrity of financial markets. While large sums of laundered money may arrive at institutions, they may also disappear just as quickly, causing liquidity problems.

The Board of Governors of the Federal Reserve System (2002, 7) imply that ‘The first stage in the process is placement. The placement stage involves the physical movement of currency or other funds derived from illegal activities to a place or into a form that is less suspicious to law enforcement authorities and more convenient to the criminal. The proceeds are introduced into traditional or nontraditional financial institutions or into the retail economy. The second stage is layering. The layering stage involves the separation of proceeds from their illegal source by using multiple complex financial transactions (e.g., wire transfers, monetary instruments) to obscure the audit trail and hide the proceeds. The third stage in the money laundering process is integration. During the integration stage, illegal proceeds are converted into apparently legitimate business earnings through normal financial or commercial operations.’

As a result, money laundering is usually having three sequential elements:

1. Placement,
2. Layering, and
3. Integration.

Not all money-laundering transactions involve all three distinct phases, and some may indeed involve more (van Duyne 2003). Nonetheless, the three-stage classification is a useful decomposition of what can sometimes be a complex process.

According to the European Commission ‘Money laundering is the process by which criminal proceeds are "cleaned" so that their illegal origins are hidden. It is usually associated with the types of organized crime that generate huge profits in cash, such as trafficking in drugs, weapons and human beings as well as fraud. Although it is not possible to measure money laundering in the same way as legitimate economic activity, the scale of the problem is considered to be enormous’. The keystone of the European system remains the Third Anti-Money Laundering Directive adopted in 2005, which requires financial operators and some non-financial operators – the so-called "gatekeepers" – to report any suspicious or unusual transactions or activities. The

Directive incorporates into EU law the revised Forty Recommendations of the Financial Action Task Force (FATF), which is the international standard setter in the fight against money laundering and terrorist financing.

Integrating "clean" money

Since money laundering is a complex, wide-spread and multifaceted activity, it is tackled from several different angles. The focus is, at one and the same time, on regulating financial institutions with a view to preventing money laundering and on law enforcement aspects.

Step 1: money launderers establish private corporations in other countries and route the money to these corporations. These foreign corporations can then provide loans to the money launderers back in the home country.

Step 2: phony invoices are created in import-export businesses. The import-export company gives inflated value to the export goods and when the invoices are paid, the cash is transferred, including the laundered money, from one company to the other. The invoices make the transfer of the money look legitimate.

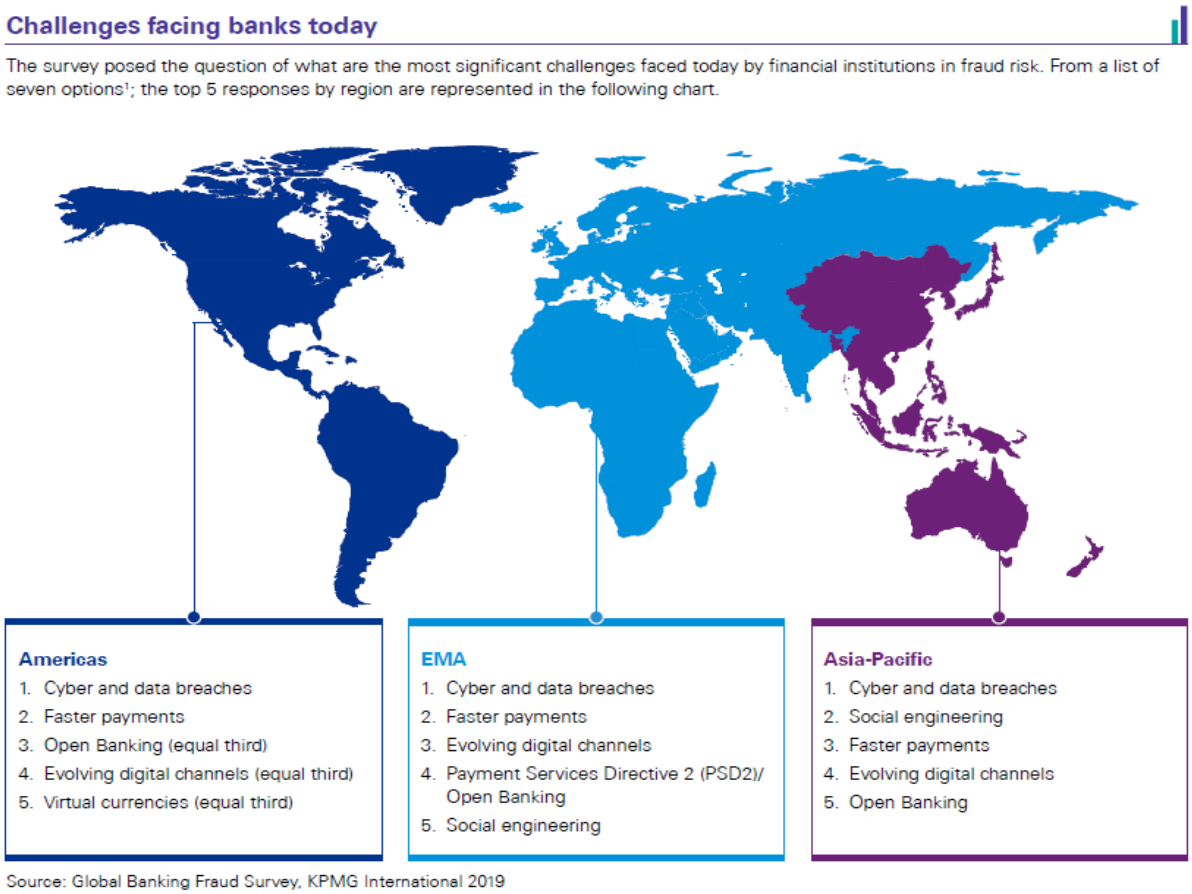
Step 3: the money launderer simply purchases an offshore bank. Illegally acquired funds are deposited in the new bank, then transferred via electronic funds transfers (EFT) to a legitimate bank.

But we have to point out here that money laundering can also involve small nonfinancial businesses knowingly providing similar services to violent criminals, as in the case of truckers smuggling large bundles of currency out of the country for drug traffickers.

Money laundering does not require international transactions; there are instances of purely domestic laundering. Nonetheless, a large number of cases do involve the movement of funds across national borders. Though governments have unique police powers at the border, those same borders can impede the flow of information.

The issue

The use of underground financial systems, such as the Colombian Black-Market Peso Exchange (BMPE), by terrorists, was examined by Alvin James, Principal at Ernst and Young, LLP. His most important notice is that while terrorists may not need to launder their money, they do need the means to move the funds covertly. The major similarity among underground financial systems, also called parallel payment systems, James notes, is their ability to facilitate anonymous international transfers of money. That ability is what makes these existing systems so attractive to terrorists: they can use them to move the dollars needed to support their activities. A reasonable conjecture is that different methods are used for laundering the proceeds from different predicate crimes. The main issue is 'Why are banks still so vulnerable to money laundering?'.



Picture 4: Banks challenges

Fortune, by Jeff John Roberts (March 2020), indicates that regulators hit banks with a near record $10 billion worth of fines in a 15-month period through 2019, and the figure is expected to increase in 2020. The 60.5% of the fines came from banks violating anti-money laundering rules, while nearly all the rest—38.7% of fines—arose because of transactions with countries under sanctions. In the latter case, it was U.S. regulators that levied almost all such fines, amounting to a total of $3.67 billion in penalties.

Financial institutions put systems in place to detect money laundering within their retail book, with other product lines left unprotected. Under increasing regulatory pressures to change this, banks hastily repurposed these systems into other areas of the business. Inevitably, these have not been suited to the product line that they are trying to protect, with systems struggling to cope with the complexity of the schemes perpetrated by organized criminals. With access to only a fraction of the available data needed, they use simplistic analysis methods, looking only at typologies dictated by the regulator.

Despite that, the only information available as to who launders money comes from criminal and civil investigations, and the data represent the interaction of enforcement tactics with the underlying reality. Enforcement may aim primarily at operations that are more professional or less professional It is obvious, we meet difficulty in precisely measuring the extent of money laundering, including the number of terrorist dollars moving through the same financial channels.

The clearest nexus between the criminal and financial realms would be persons inside the financial institutions themselves. Lawyers are thought to be among the most common laundering agents or at least facilitators, though they have been at the center of few cases not only in the United States (**Mexico's** Sinaloa cartel and Colombia's Norte del Valle cartel HSBC case) but in Europe (like Denis Jebb, Louis Glatt and Noel Horne, *Journal of Money Laundering Control*, Vol. 6 No. 1, pp. 17-26.) as well. A lawyer can use his or her own name to acquire bank accounts, credit cards, loan agreements, or other money-laundering tools on behalf of the client. Lawyers can also establish shell corporations, trusts, or partnerships.

We can realize that the genuine criminals it is difficult to be caught but there have been numerous attempts to establish the magnitude of the problem. Money laundering around the globe has been estimated at $500 billion a year.

Other professionals involved in money laundering include accountants, notaries, financial advisers, stockbrokers, insurance agents, and real estate agents. A British report on serious and organized crime noted that in 2002, “purchasing property in the UK was the most popular method identified, involving roughly one in three serious and organized crime groups where the method was known” (National Criminal Intelligence Service 2003, 53).

3. Anti Money Laundering

The Anti Money Laundering (AML) approach

Financial crime is a wide-reaching and prolific issue that banks are struggling to tackle. Laundered money is known to be funding illegal activities, including terrorism, which places banks under immense pressure to identify the source of such funds. All banks have Anti-Money Laundering (AML) systems in place, but they are crippled by a variety of different inefficiencies that are allowing criminal activity to remain undetected. In many cases, organized criminals are systemically probing the various weaknesses within these AML systems and are actively capitalizing on them in order to turn the profits of crime into ostensibly legitimate assets**.**

Methods and measures for preventing criminal acts of money laundering involve numerous actions and procedures in the domain of prevention, conducted by the competent authorities to suppress money laundering and its consequences for the society. Reports on suspicious or unusual transactions are integrated into the legal framework of the system for suppression of money laundering and represent the basis of this system for the identification of money laundering activities in diverse areas of economy.

Financial crime is a wide-reaching and prolific issue that banks are struggling to tackle. Laundered money is known to be funding illegal activities, including terrorism, which places banks under immense pressure to identify the source of such funds. All banks have Anti-Money Laundering (AML) systems in place, but they are crippled by a variety of different inefficiencies that are allowing criminal activity to remain undetected. In many cases, organized criminals are systemically probing the various weaknesses within these AML systems and are actively capitalizing on them in order to turn the profits of crime into ostensibly legitimate assets.

At first, financial institutions put systems in place to detect money laundering within their retail book, with other product lines left unprotected. Under increasing regulatory pressures to change this, banks hastily repurposed these systems into other areas of the business. Inevitably, these have not been suited to the product line that they are trying to protect, with systems struggling to cope with the complexity of the schemes perpetrated by organized criminals. With access to only a fraction of the available data needed, they use simplistic analysis methods, looking only at typologies dictated by the regulator.

Due to ineffective systems, entry level analytics and inflexible patterns of cooperation the resolution feels so far from the banking reality, from time to time. Money launderers are ultimately people and companies, not transactions and accounts. Banks have thus been able to successfully combat the problems discussed by employing entity resolution and network analysis techniques. These advanced analytical processes are able to interpret vast data sets, contextualizing seemingly isolated incidents and relationships within wider networks which ultimately helps to unearth cases of intentionally hidden money.

Connections can be extracted from internal and external data, derived from information such as names, contact information, company structures and transactional money flows. These new AML systems are proving to be far easier to rework and are therefore far more reactive to additions of new data points or typologies. This has allowed leading banks to employ AML solutions that are personalized and adaptable to their individual needs.

Keep in mind, that as political pressures mount, money launderers are becoming increasingly intelligent in how they work and the systems in place are simply not sophisticated enough to keep up with them. Banks that have taken a proactive stance to these glaring issues, embracing a more holistic and flexible approach towards anti-money laundering, are finding it is the obvious solution to a dangerous problem. Many money laundering cases appear to involve opportunistic laundering rather than professional services. Where someone apart from the offender provides the service, he may provide it only to that offender, perhaps because they are related or connected through some other activity.

- **The USA dynamic:**

Money laundering in the United States of America (USA) is a serious problem. The primary source of laundered funds comes from the accessibility of the financial system. Trade-based money laundering is another method by which criminals have laundered funds in the USA. In response to the September 11, 2001 attacks, the USA has taken advanced measures to combat money laundering and terrorist financing. The USA PATRIOT Act of 2001 amends the Bank Secrecy Act (BSA) by requiring all financial institutions to establish Anti-Money Laundering (AML) programs. The Act is intended to strengthen the USA’s measures to prevent, detect, and prosecute money laundering and the financing of terrorism.

The USA requires Suspicious Activity Reports (SARs) to be filed any time there is a large or suspicious transaction to the Financial Crimes Enforcement Network (FinCEN). FinCEN serves as the USA's Financial Intelligence Unit (FIU). The USA's financial institutions are also required to follow strict customer identification programs in order to verify the true identity of each customer and deter money laundering.

- **The European dynamic:**

Financial Intelligence Units (FIUs) play a key role in the fight against money laundering and terrorist financing. These units are responsible for receiving, requesting, analyzing and disseminating information to the competent authorities on potential money laundering or terrorist financing activities. They are usually placed within law enforcement agencies or administrative bodies reporting to Ministries of Finance in EU States, Commission ensures us.

The Commission has made significant efforts to improve coordination and cooperation between FIUs and to harmonize criminal penalties for money laundering. The operational cooperation and exchange of information among EU FIUs has been reinforced by the FIU-NET project. Funded by the Commission since its beginning, this project aims to establish a secure computer network for the exchange of financial intelligence.

Recent global and European developments call for the need to strengthen the EU's efforts to combat money laundering and the financing of terrorist activities.

In order to improve the effectiveness of the EU's Anti-Money Laundering and Counter Terrorist Financing (AML/CTF) efforts, the European Commission issued the 4th AML Directive in May 2015 and repealed the previous one. The 4th AML Directive entails the amendments that need to be adopted by all Member States by 26 June 2017.

On 5 July 2016 the European Commission presented a new proposal for a Directive amending the 4th AML Directive, which is referred to as the 5th AML Directive. The 5th AML Directive is proceeding along the European Union's legislative process.

In July 2019, the Commission adopted an Anti-Money Laundering Communication, which highlighted several measures that could be taken to remedy the weaknesses in the EU's current anti-money laundering rules.

- **The Greek Approach:**

To begin with the Bank of Greece is the authority responsible for supervising compliance with the legal and regulatory framework on the prevention and suppression of money laundering, terrorist financing (AML/CFT) and the financing of proliferation of weapons of mass destruction, by the institutions under its supervision.

The current institutional framework has been primarily established by incorporating the relevant EU legislation, which is aligned with the "Forty (40) Recommendations against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction" (adopted in February 2012 by the Financial Action Task Force (FATF)).

The Bank of Greece, in the context of its supervisory tasks, checks supervised institutions' compliance with their AML/CFT obligations and assesses the adequacy and effectiveness of their AML/CFT procedures.

It should be noted that, other than being responsible for checking compliance with the stipulated due diligence provisions when transactions are carried out by supervised institutions, including the obligation to report suspicious transactions to the Anti-Money Laundering Authority, the Bank of Greece is not vested with preliminary investigation powers nor is responsible for investigating suspicious transaction reports. The Anti-Money Laundering Authority is exclusively responsible for investigating thoroughly suspicious transactions and taking further actions.

The legal and regulatory framework is established on the basis of the Law, EU directives and regulations, the Governor's Acts, Executive Committee Acts, Credit and Insurance Committee/Banking and Credit Committee Decisions, circulars and explanatory documents.

At the same time, the last Mutual Evaluation Report relating to the implementation of anti-money laundering and counter-terrorist financing standards in Greece was undertaken in 2019. According to that Evaluation, Greece was deemed Compliant for 15 and Largely Compliant for 22

of the FATF 40 Recommendations. It was deemed Highly Effective for 0 and Substantially Effective for 5 of the Effectiveness & Technical Compliance ratings.

According to the US Department of State Money Laundering assessment (INCSR), Greece was deemed a Jurisdiction of Primary Concern by the US Department of State 2017 International Narcotics Control Strategy Report (INCSR) but has not been included since.

Key Findings from the last report are as follows:

‘Greece is considered a regional financial center for the Balkans, as well as a bridge between Europe and the Middle East. Official corruption, the presence of organized crime, and a large informal economy make the country vulnerable to money laundering and terrorist financing. Greek law enforcement proceedings show that Greece is vulnerable to narcotics trafficking, trafficking in persons, illegal migration, prostitution, smuggling of cigarettes and other contraband, serious fraud or theft, illicit gaming activities, and large-scale tax evasion.

Evidence suggests financial crimes, especially tax related, have increased in recent years. Criminal organizations, some with links to terrorist groups, are trying to use the Greek banking system to launder illicit proceeds. Criminally derived proceeds are most commonly invested in real estate, the lottery, and the stock market. Criminal organizations from southeastern Europe, the Balkans, Georgia, and Russia are responsible for a large percentage of the crime that generates illicit funds.

The imposition of capital controls in June 2015 has limited, but not halted, the widespread use of cash, which facilitates a gray economy as well as tax evasion, although the government is trying to crack down on both trends. The government is working to establish additional legal authorities to combat tax evasion. Due to the large informal economy, it is difficult to determine the value of goods smuggled into the country, including whether any of the smuggled goods are funded by narcotic or other illicit proceeds.

Greece has three free trade zones (FTZs), located in the Heraklion, Piraeus, and Thessaloniki port areas. Goods of foreign origin may be brought into the FTZs without payment of customs duties or other taxes and remain free of all duties and taxes if subsequently transshipped or re-exported. Similarly, documents pertaining to the receipt, storage, or transfer of goods within the

FTZs are free from stamp taxes. The FTZs also may be used for repacking, sorting, and re-labeling operations. Assembly and manufacture of goods are carried out on a small scale in the Thessaloniki Free Zone. These FTZs may pose vulnerabilities for trade-based and other money laundering operations.

Corruption severely affects Greece's business environment, completely distorting market competitiveness. A common form of corruption in Greece is known as 'fakelaki', translating to small envelopes and signifying bribes passed on to officials or other recipients to obtain some form of benefit. Greece's Penal Code criminalizes several forms of bribery, including passive and active bribery, abuse of office and money laundering, yet ineffective implementation of existing laws has exacerbated corruption in both the higher and lower echelons of government. The tax administration and public procurement are identified as the sectors most affected by corruption. Gifts, bribery and facilitation payments are widespread despite existing provisions that criminalize these acts.'

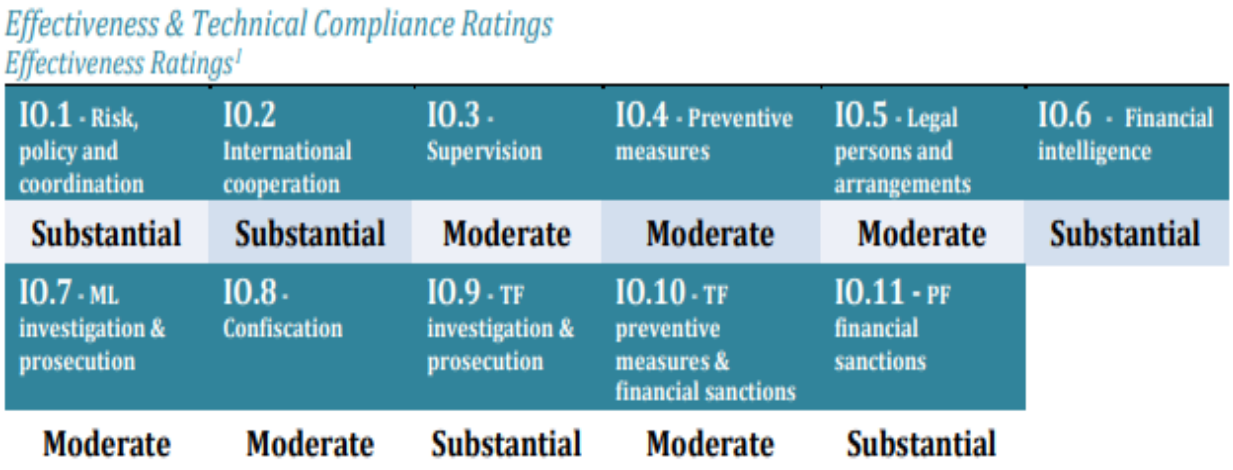
At the Executive Summary of the same report we can read that Greek authorities generally understand the ML/TF vulnerabilities and risks they face as presented in the NRA adopted in May 2018. Greece adopted a national AML/CFT Action Plan based on the findings of the NRA. Generally, the objectives of most Greek authorities are consistent with identified ML/TF risks and national AML/CFT policies. The National Strategy Committee plays a significant role in effective co-operation and coordination at the national policy making levels in Greece. However, Greece had not yet finalized its national AML/CFT Strategy at the time of the on-site visit.

It is also pointed out that Greek authorities effectively use financial intelligence and other information to develop evidence and trace proceeds in investigations for ML, TF, and associated predicate offences.

Moreover, Greek authorities make effective use of tools for seizing and freezing assets, depriving criminals of illicit proceeds and preserving assets for future confiscation. However, delays in prosecution and appellate processes prevent effective confiscation in many cases, and lack of comprehensive statistics prevents Greece from demonstrating the degree to which criminals are permanently deprived of their assets. Sanctions for false or non-declaration of cash or BNI is not proportionate or dissuasive.

They end up with the statement that ‘Generally, Greek authorities demonstrate a strong commitment to international co-operation and, on an operational level, HFIU and LEAs, particularly Customs, generally demonstrate effective co-operation with international partners. However, delays in judicial processes negatively impact Greece’s ability to consistently provide or seek timely MLA and extradition. A lack of comprehensive statistics hinders Greece’s ability to assess and improve its own effectiveness in relation to MLA, extradition and international cooperation.’

The report visualizes the ratios dealing with effectiveness and compliance for Greece’s amounts. As we can see from the following pictures many and different aspects were measured for a detailed profile.



Picture 5: Effectiveness ratings can be either a High- HE, Substantial- SE, Moderate- ME, or Low – LE, level of effectiveness.

Technical Compliance Ratings[2]

R.1 - assessing risk & applying risk-based approach	**R.2** - national cooperation and coordination	**R.3** - money laundering offence	**R.4** - confiscation & provisional measures	**R.5** - terrorist financing offence	**R.6** - targeted financial sanctions – terrorism & terrorist financing
LC	**LC**	**C**	**LC**	**LC**	**LC**
R.7- targeted financial sanctions - proliferation	**R.8** -non-profit organisations	**R.9** – financial institution secrecy laws	**R.10** – Customer due diligence	**R.11** – Record keeping	**R.12** – Politically exposed persons
LC	**PC**	**C**	**C**	**C**	**C**
R.13 – Correspondent banking	**R.14** – Money or value transfer services	**R.15** –New technologies	**R.16** –Wire transfers	**R.17** – Reliance on third parties	**R.18** – Internal controls and foreign branches and subsidiaries
PC	**C**	**LC**	**LC**	**LC**	**C**
R.19 – Higher-risk countries	**R.20** – Reporting of suspicious transactions	**R.21** – Tipping-off and confidentiality	**R.22** - DNFBPs: Customer due diligence	**R.23** – DNFBPs: Other measures	**R.24** – Transparency & BO of legal persons
LC	**C**	**C**	**LC**	**LC**	**LC**
R.25 - Transparency & BO of legal arrangements	**R.26** – Regulation and supervision of financial institutions	**R.27** – Powers of supervision	**R.28** – Regulation and supervision of DNFBPs	**R.29** – Financial intelligence units	**R.30** – Responsibilities of law enforcement and investigative authorities
LC	**LC**	**C**	**LC**	**C**	**C**
R.31 – Powers of law enforcement and investigative authorities	**R.32** – Cash couriers	**R.33** – Statistics	**R.34** – Guidance and feedback	**R.35** – Sanctions	**R.36** – International instruments
C	**PC**	**LC**	**LC**	**LC**	**LC**
R.37 – Mutual legal assistance	**R.38** – Mutual legal assistance: freezing and confiscation	**R.39** – Extradition	**R.40** – Other forms of international cooperation		
LC	**C**	**C**	**LC**		

Picture 6: Technical compliance ratings can be either a C – compliant, LC – largely compliant, PC – partially compliant or NC – noncompliant.

Coming up with a conclusion, the Mutual Report notices the prior actions Greece should take under strong consideration. First of all, the country should identify and fully understand ML/TF risks that arise independently from predicate offences, finalize and implement its National Strategy, including by taking the steps set out in its national Action Plan to address previously identified and emerging risks.

After that, should, also, examine the case management systems, prioritization of tasks and allocation of resources among prosecutors and the judiciary and make such changes as are necessary to address delays in ML and TF prosecutions, obtaining irrevocable confiscation orders and in making and executing MLA and extradition requests. To that end, Greece should also implement revised criminal procedures, including measures to address the right to adjournment and to allow for extrajudicial resolution in appropriate cases.

Additional, Greece has to raise awareness of TFS obligations, ensure appropriate resources are available to supervisory authorities, strengthen the understanding of AML/CFT risks and obligations, develop more comprehensive national statistics regarding ML/TF related issues, review the level of sanctions that are applied upon conviction for ML and TF etc..

4. Money Laundering in reality-Cases

The European Danske Bank

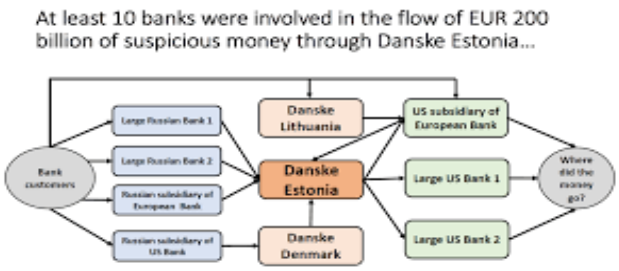
A very recent scandal, with still ongoing repercussions, the Danske Bank scandal became international news in 2018 and has now been called the largest in Europe to date.

We could say that Danske Bank ran into trouble. Its Estonian branch came about when Danske acquired Sampo Bank, a small Finnish Bank in 2007. Sampo had a non-resident portfolio in Estonia and it is this that caused the problems.

In the words of the independent report into the scandal, which preempted CEO Borgen's resignation: "Anti-money laundering procedures at the Estonian branch had been manifestly insufficient and inadequate." Danske Bank has also admitted there were "major deficiencies in controls and governance that made it possible to use Danske Bank's branch in Estonia for criminal activities such as money laundering".

Danske shut down the non-resident portfolio in 2015 after it became clear that the bank's anti-money laundering procedures at the Estonian branch weren't working. As a mere branch, Estonia should have been subject to Danske's own money laundering systems – but the branch had its own IT platform, which meant it was not covered by the same risk monitoring as the bank's Copenhagen headquarters. Finally, in 2015, Danske Bank shut down the non-resident portfolio when it became clear that the bank's anti-money laundering procedures at the Estonian branch weren't working. They even admitted there were "major deficiencies in controls and governance that made it possible to use Danske Bank's branch in Estonia for criminal activities such as money laundering".

The independent investigation found that more than half of Danske's 15,000 customers in Estonia were suspicious. The source of funds passing through the portfolio was identified as more than 58 per cent coming from Russia, Estonia and Latvia. The destinations of the funds were worldwide.



Picture 7: The fraud analysis

The difficulty in identifying the true source of the funds comes from the lack of transparency as to the real owners of the customers in the portfolio. A proportion of them are UK-based companies that are registered as limited liability partnerships – this means they are not required to publish details of their eventual owners. This is a classic case of money laundering where ownership often passes through a series of shell companies before the eventual owner can be identified.

The customers are being investigated by several national authorities including the FBI and the UK National Crime Agency. The Danish regulator is investigating Danske Bank itself. Harsh penalties for the bank could ensue – Denmark's business minister said the Danish authorities could fine Danske 4 billion Danish kroner (£475 million). But it remains to be seen what the long-term damage will be for Danske, if any.

'A wider question surrounds the failure of international anti-money laundering regimes. To date there have been no examples of significant criminal sanctions for failure to implement an effective anti-money laundering process within a business. Nor is there any rigorous external scrutiny of how guidelines are implemented. But it is high time there was – while there is still a financial system to protect.', according to News of Compliance.

As a result, a lot. EU banks paid over $16 billion in fines between 2012 and 2018 because of lax money-laundering checks, rating agency Moody's said in a report on Tuesday, with U.S. regulators levying more than 75 percent of those fines. Now the allegations have stepped up, so could the fines, according Reuters.

The American Wachovia Bank

Wachovia Bank used to be one of the largest banks in the US before it was purchased by Wells Fargo during the 2008 financial crisis, and it is also responsible for the largest money laundering case of all time.

In 2004, Wachovia was conducting business with *casa de cambios* (CDCs) in Mexico. CDCs are currency exchange houses where one can bring in cash, send it to a bank account and exchange the currency. Now, that sounds like a great and simple way to launder money—it's not surprising that even in 2004, CDCs were flagged as being risky by financial institutions. Wachovia was also aware of the risks involved, however, while other banks were slowly distancing themselves from them, concerned about the potential for money laundering, Wachovia was deepening its involvement in CDCs.

CDCs can be legitimate, provided both sides are implementing AML procedures. However, Martin Woods, a whistleblower who joined Wachovia as a money laundering reporting officer in 2005, started getting suspicious:

- after finding suspicious transactions in connection with CDCs, he filed suspicious activity reports (SARs) regarding those. He also noticed the lack of KYC information, meaning, precisely those AML procedures were missing that would make CDCs legitimate.
- From all of this, he suspected the involvement of Mexican drug cartels and money laundering.

Wachovia was not happy about his actions, and he was told to stop asking questions, which made him even more suspicious. Certain that something illegal was happening, he continued to file SARs, the Bank even told him that he had no right to access the documents the reports were based on, and he was told to stop what he was doing.

In 2007, after the US federal law enforcement started to look into Wachovia's operations, faced with pressure from the US attorney's office, the Bank stopped its activities with CDCs.

The real investigation started with a major drug bust in 2006. A DC-9 was intercepted in the Gulf of Mexico and found to be loaded with 5.7 tons of cocaine. During the course of the investigation, by the Drug Enforcement Agency (DEA), it was discovered that Mexican cartels were smuggling US dollars gained from selling illegal drugs in America across the Mexican border. These

investigations lead to Wachovia, and it was revealed that the money was given to the CDCs, who deposited it in their Mexican bank accounts.

The banks did not investigate the origin of the money, which allowed these illegal earnings to enter the legitimate sector. The funds then were wired back to Wachovia's accounts in the US, where, again, the origins of the money were not checked. Using this method, criminals were able to integrate illegal funds into the financial system.

Wachovia was bought by San Francisco-based Wells Fargo in 2008 to create the most extensive distribution system for financial services in North America. The integration of Wachovia and Wells Fargo is complete, and all Wachovia accounts have been moved to Wells Fargo.

Since the involvement of Wachovia and other U.S. banks with connections to Mexican drug cartels, Mexico has announced a plan to reward people who report suspected money laundering, which would allow the awardees to get up to one-quarter of the illicit funds or property seized. Under this new plan, people will be able to file reports in person, by telephone, or by email and the amount of their reward will be determined by a special committee. All people are eligible except public servants, law enforcement, and banking employees who would only be duplicating their efforts to monitor suspicious activity.

However, even though it's estimated that the amount of money laundered through Wachovia throughout the whole scheme was between $350-380 billion, Wachovia managed to get away with the whole thing, settling the case by paying a $160 million fine and promising to increase its AML procedures.

Conclusions

In recognition of the extent of the problem, the G7 group of major economies formed the Financial Action Task Force on Money Laundering back in 1989. The idea behind this was to produce a set of standards and guidelines and to monitor progress on anti-money laundering regimes. Many years passed by and many new regulations and standards added. Audits and investigations got stronger and more accurate.

The focus is to identify suspicious transactions and report them. For anti-money laundering efforts to be successful, it requires financial institutions to know their customers. This means that banks must be able to identify the ultimate beneficial recipient of a transaction – so the person who takes the profit – of any customer on their books.

Professional skills and expertise of internal auditors must suit them for the needs and the importance of money laundering cases. Forensic accounting skills, as well as audit expertise, are needed to help fight this crime. Development of internal policies, procedures, and controls to prevent money laundering is another key dealing with these profession's responsibilities.

Money laundering, due to today's high-tech, global environment, is worldwide and very expensive for all the parts of the acquisition. The purpose of the audit is to assess whether the bank's action in the fight against money laundering in the banking sector is effective. In particular, we must be ready to examine whether:

1. AML risks are assessed and communicated to banks and national authorities involved in fighting money laundering.
2. The available AML information for supervisory activities is shared among the stakeholders and
3. All the effective and timely action is taken in response to suspected breaches of AML.

Since we identified the issues underlying these areas of enquiry before the audit work commenced, they should not be regarded only as audit observations, conclusions or recommendations.

For the financial institutions, one of the most important features of the implementation of the money laundering suppression measures is the establishment and upgrading of the control system, to determine whether financial and other institutions implement supervision and internal control in the field of money laundering prevention. Inspection is a primary supervision method in the implementation of money laundering prevention measures. Other forms of supervision are also possible as measures of external control, such as commonly used central bank supervision or independent supervisory bodies control in case it is provided by law.

We have to remember that the increased levels of regulatory activity will not reduce in the near term, challenging economic conditions look set to remain for some time and the risks of fraud, bribery and corruption are not going away.

For the countries, their authorities, their governments, and population, they have responsibility for leading, coordinating and monitoring the financial sector's fight against money laundering and terrorist financing. This includes the drafting of regulatory instruments.

References

1. European Commission, “Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing”, C(2020) 2800 final, 7 May 2020.
2. Council of the EU, “Money laundering: Council sets strategic priorities for further reforms”, press release, 5 December 2019.
3. FATF – Egmont Group (2018), Concealment of Beneficial Ownership, FATF, Paris, France, www.fatf-gafi.org/publications/methodsandtrends/documents/concealmentbeneficial-ownership.html
4. Titcomb, J. (2014). Full investigation into the dominance of 'big four' UK banks confirmed. The Telegraph, [Online] 6 November. http://www.telegraph.co.uk/finance/newsbysector/banksandfinance/11212515/Full-investigation-into-the-dominance-of-big-four-UK-banks-confirmed.html [Retrieved: 2015-04-22]
5. Lagarde, C. (2015). Ethics and Finance - Aligning Financial Incentives with Societal Objectives, [Online] 6 May. Available at; http://www.imf.org/external/np/speeches/2015/050615.htm [Retrieved: 2015-05-10]
6. FATF (2013a), FATF Methodology for assessing compliance with the FATF Recommendations and the effectiveness of AML/CFT systems – FATF Methodology, FATF, Paris, France, www.fatf-gafi.org/publications/mutualevaluations/documents/fatfmethodology.html
7. FATF (2013b), Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals, FATF, Paris, France www.fatf-gafi.org/publications/methodsandtrends/documents/mltfvulnerabilities-legal-professionals.htm
8. Sturm, P. (2013). Operational and reputational risk in the European banking industry: The market reaction to operational risk events. Journal of Economic Behavior & Organization, 85 (1), 191–206.
9. Sapienza, P., & Zingales, L. (2012). A Trust Crisis. International Review of Finance, 12 (2), 123-131.
10. Vulliamy, Ed. “How a big U.S. bank laundered billions from Mexico’s murderous drug gangs.” The Observer. April 3, 2011.
11. Associated Press. “Mexico sets rewards for reporting money laundering.” CBS News. April 4, 2011.

12. Ruspantini, D., & Sordi, A. (2011) The reputational risk impact of internal frauds on bank customers: a case study on UniCredit Group. UniCredit & Universities Foundation Working Paper Series, 15.
13. Hasman, A. (2013). A critical review of contagion risk in banking. Journal of Economic Surveys, 27 (5), 978-995
14. B. Steel, Billy's Money Laundering Information Website. Money Laundering – A Brief History. http://www.laundryman.u-net.com/page1_hist.html, February, 2004
15. Fraud Examiner's Manual (excerpts from), The USA PATRIOT Act, signed into law after 9/11, strongly targets suspected money laundering activities and creates new requirement for financial institutions. The White Paper, July/August, 2003
16. Hull, J.C. (2012). Risk Management and Financial Institutions. 3rd Edition. Hoboken: John Wiley & Sons.
17. Bell, R.E. (2002), "The prosecution of lawyers for money laundering offences", *Journal of Money Laundering Control*, Vol. 6 No. 1, pp. 17-26. https://doi.org/10.1108/13685200310809374
18. Boskovic, M. (2001). Current problems in money laundering suppression. Security, 5., vol. 43, Belgrade, p. 565-586.
19. https://fortune.com/2020/03/11/money-laundering-record-year-bank-fines/
20. https://www.bankofgreece.gr/
21. https://egmontgroup.org/en/content/greece-anti-money-laundering-counter-terrorist-financing-and-source-funds-investigation
22. http://www.hcmc.gr/
23. http://www.fatf-gafi.org/
24. https://www.state.gov/countries-areas/
25. https://www.transparency.org/en/#
26. https://www.worldbank.org/
27. https://www.cia.gov/library/publications/the-world-factbook/