International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2020): 7.803

Digital Identity: The Influence of Digitalization and New Technologies on the Challenge of Balancing the Anti-Financial Crimes Program and Customer Satisfaction in Banking Institutions

Loubna IDRISSI[1], Fatima IDRISSI[2]

[1]PhD Candidate in Management Sciences , Mohammed V University of Rabat, Faculty of Legal, Economic and Social Sciences Agdal, Laboratory of Studies and Research in Management Sciences (LSRMS)
loobna.idrissy[at]gmail.com

[2]Doctor in Management Sciences, Mohammed V University of Rabat, Faculty of Legal, Economic and Social Sciences Agdal, Laboratory of Studies and Research in Management Sciences (LSRMS)

Abstract: ***This paper provides a partial overview of the concept related to digital identity and a summary of its adoption in banking institutions as well as its impact on the challenge balancing the antifinancial crimes program and customer satisfaction. Indeed, many criminal networks make advantage of the global banking system to recycle the products with a criminal source, whether it be human trafficking, drug or arms trafficking, or even money laundering that has been used to finance criminal or terrorist activities, crime monitoring represents a huge global challenge. Since convictions are extremely rare, it is essential to find evidence leading to successful prosecutions. The challenge is huge : limiting financial crimes and fraud, strengthening security and customer-related checks while onboarding them as they should be (optimal experience). The KYC process must obviously be safe and compliant with regulations, the customer welcomed in the best possible way and in compliance with the Morrocan Law n ° 09-08 relating to the protection of personal data. In fact, onboarding customers aims to be efficient, but not hasty : by speeding up procedures or bypassing controls to win a customer, you expose the banking company to a massive sanctions risk and fines in case of non-compliance. The KYC process must also be precise and compliant, but not invasive to customers. Following customer identity verification protocols to the letter without worrying about the target can prove fatal. At each stage, the customer can prefer to stop everything and ultimately join a competitor who can perform these operations more quickly and in a less restrictive manner. Finding new ways to improve the customer experience is therefore vital for financial and banking institutions, and in the current context of digital transformation, digital technology is helping us with innovative solutions.***

Keywords: Banking and financial system, Anti Money Laundering and Terrorist Financing, AML-CFT impacts linked to the COVID-19 crisis, Customer satisfaction, Digitalization and new technologies

1. Introduction

Since the adoption of the Patriot Act in the United States, in the aftermath of the terrorist attacks of September 2011, the banking system has had to cope with the growing regulatory requirements forcing banks to collect more information on their customers and to find out the source of funds of illegal origin of which they are the custodians through KYC (Know Your Customer) procedures.

Those who are unable to meet these requirements face severe sanctions. Since 2008, banks around the world have had to pay billions of dollars in fines due to breaking financial crime regulations.

The bank must therefore strike a balance between compliance requirements and customer satisfaction. The onboarding of a new customer provides an invaluable opportunity for any bank or financial institution to demonstrate their efficiency and commitment to the customer, but very often, entering into a relationship presents challenges that create a bad first impression.

According to a study by PwC[1], an American audit firm, 73% of consumers say that the customer experience is an important factor in their purchasing decision. Also, over 90% of customers believe the companies they buy from "could do better" when it comes to onboarding new users. Finally, almost a third of customers would stop doing business with a brand they liked after just one bad experience.

As regulatory demands are ever more numerous and complex, the pressure on the customer should however be as low as possible. Assess the risks, yes. Losing a prospect or a customer, no. If we took the image of a physical store, letting a (potential) customer enter an airlock, a security guard searching him, questioning him before finally letting him enter the store, we can imagine that the experience could be very unpleasant for the customer. A tricky manner to welcome him.D'autre part, ce procédé est consommateur de temps et de ressources (matérielle et humaine, donc financière) pour la boutique.

[1] PricewaterhouseCoopers, Future of Customer Experience Survey 2017/18.

The subject of this paper revolves around the impact of digitization and new technologies on the Anti-Money Laundering and Counter-Terrorist Financing program in the banking system. As digitalization and new technologies are omnipresent in our daily lives, there is no longer any question for the bank to ask itself if they constitute an opportunity or a threat but rather to measure their impact, it's useful for that to " analyze the nature of the interactions that may take place between digitization and its impact on the financial crime management system within the banking establishment.

This paper devotes the first part to the study of the concept of the banking and financial system by presenting some definitions. A second point is dedicated to the presentation of the AML/CFT (Anti-Money Laundering and Counter-Terrorist Financing) program and the strengthening of KYC (Know Your Customer) laws by the banking regulator. A third highlighting a new typology of AML risks resulting from the COVID-19 crisis. Finally, the last part is devoted to the analysis of the dimension "Digitalization and new technologies" and their impact on the balancing challenge "anti-financial crimes & customer satisfaction" and summarizes the main conclusions.

2. Banking and Financial System

According to Peyrard (2001)[2], the financial system is broadly defined as : "all the institutions, markets, rules and practices of the international monetary and financial system that governments, businesses and individuals follow in their economic and financial activities ". Even if this definition, is offering a broad vision of the concept under review, it does not fully reflect the perception of the financial system adopted within the framework of this study. Thus, our vision of the financial system is in line with the definition proposed by Stiglitz (1997)[3], when he affirms that: "the financial system is a part of the economy which includes all the institutions participating in the transfer of money. Savings from savers (households and companies) to borrowers, as well as in the transfer, sharing and insurance of risks " Or again as defined by Jean-Paul POLLIN (2021)[4] : "A financial system is defined by all the rules, practices and institutions (stock exchanges, banks, etc.) which make it possible to mobilize capital to put it in place available to agents with financing needs. These needs essentially correspond to investment projects of companies, administrations or individuals ". In other words, the financial system can be seen as being the set of public or private banking or financial structures that participate in the collection and / or allocation of monetary or financial resources between economic agents with excess capital (savers) and those with capital deficit (borrowers).

Michel Dietsch and Philippe Wahl (2012)[5] also agree with the two previous opinions in their article by specifying that "the role of the financial system is to allocate capital by transferring savings to financing needs. However, the properties that savers want to give to their assets are different from those that borrowers are looking for. The financial system must therefore transform the characteristics of funds, ie manage time and risk. This transformation takes place directly by agreement of the contracting parties in financial markets or indirectly within financial institutions. To achieve this transformation, it must develop specific techniques for processing information - to assess and monitor risks - but also for "liquefying" financial assets. It is ultimately these two types of information and liquidity services that economic agents expect from the financial system ".

In summary, the bank is an integral part of the financial system by having an activity almost exclusively financial and because its main function is to offer services of a financial nature, such as collecting savings, receiving money deposits, granting of loans and management of means of payment. The banking system is a set of organizations providing independent financial intermediation and which are characterized by the power of monetary creation. It is made up of the Central Bank and second-tier banks also called commercial banks. It operates with the help of the regulatory, supervisory and representative bodies of the profession. The banking system operates directly or indirectly in the process of creation or circulation of money and savings or simply in the circulation of money and savings.

2.1 Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT)

The bursting of the internet bubble in the 2000s and the financial crisis in 2008 led to further regulation of banking and financial activities as complex products. Prudential rules have since their origin tended to ensure financial stability. First, relating to the liquidity and solvency of banking and financial institutions, now their strengthening appears in connection with the AntiMoney Laundering and Counter-Terrorist Financing.

Indeed, the professional secrecy accompanying the treatment of the various services offered by the bank (deposits, loans, investments and foreign exchange transactions) serves as a screen against financial delinquency and an alibi for many criminal networks. These criminals exploit the global banking system to recycle criminally sourced proceeds and force it to track money and implement an Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT) compliance program meeting international standards in order to obtain evidences that can lead to successful prosecutions.

[2] PEYRARD Josette et PEYRARD Max, Finance dictionary, Vuibert, 2nd edition, 2001.

[3] STIGLITZ Joseph, Principles of modern economics, Bruxelles, Paris, de Boeck University, 1st edition, 1997.

[4] Jean-Paul POLLIN, « macroéconomie - Systèmes financiers », *Encyclopædia Universalis* [on line].

[5] Michel Dietsch & Philippe Wahl, « Revue d'économie financière - Système financier et création de valeur », Financial Economics Association[on line].

An AML/CFT program has three main components : the fight against terrorist financing, money laundering and compliance with embargoes.

The fight against the financing of terrorism may consist in preventing the financing of all actions carried out by groups of individuals who aim to commit acts of destruction against people or property. The terrorism that we have witnessed in recent years is essentially the result of organizations using terrorism as a means of conveying their beliefs, their separatist ideas, or any other form of claim, whatever its nature.

While money laundering is an operation or a series of operations used to conceal the origin of a sum of money or the identity of its originator and / or beneficiary. In other words, it is the transformation of illicit funds into licit money, which can therefore be reinvested in legal sectors or used for personal ends. Terrorist financing, on the contrary, uses techniques to try to hide the destination of funds. Note that the funds used to finance terrorism can be of quite legitimate origin.

Embargoes generally result in measures banning some types of operations, such as, the ban on trading in nuclear or military material, or the ban on exporting oil resources to a country under embargo. The application and implementation of these measures by credit institutions during their various transactions avoids going against the restrictions on the embargoes in force.

However, the central bank Bank Al Maghrib[6] has forced credit institutions to comply with international standards enacted by the Financial Action Task Force on Money Laundering (FATF), created in Paris in 1989, at the G-7 summit. , in response to the growing concern over money laundering and terrorist financing. The mission of the FATF is to examine the techniques and trends of money laundering and terrorist financing, to examine the actions which have been taken at the national or international level and to develop the measures which remain to be taken to fight against money laundering and terrorist financing. In April 1990, less than a year after its creation, the FATF published a first report containing a series of forty recommendations which provide a comprehensive AML/CFT action plan.

The implementation of recommendations in credit institutions is reflected in an in-depth process of knowing and monitoring customers as well as transaction controls.

KYC (Know Your Customer) due diligence is designed to always ensure that banks verify identities, assess risks appropriately, and do not provide funding to people on sanctioned person lists. In addition, KYC laws help in the fight against fraud, money laundering and terrorist financing. It is therefore essential to find the right balance so that innocent customers do not have to bear the brunt of the demands.

The KYC customer verification process is mandatory and banks cannot escape it. These laws were originally incorporated in 2001 as part of the Patriot Act (Katherine Manning, 2021)[7], passed to help prevent and monitor terrorist activity. Today, any financial product or transaction must pass KYC controls.

The customer identification program includes the request for specific documents relating to identification information depending on whether it is a natural or legal person. The next aspect of KYC goes through the due diligence rules based on the information collected on the customer, the bank must be able to predict the types of financial transactions that a customer could carry out in order to be able to spot suspicious activities, monitor according to the score assigned after assessment of the customer risk profile and identify very high risk clients with whom the bank should not onboard.

When it's justified, banks could ask potential customers for additional information, such as occupation, description of activities, source of funding, purpose of account, etc. This is essential when the bank comes to file suspicious activity reports (Katherine Manning, 2021).

Monitoring when entering into a relationship with a customer is also reinforced by filtering tools through which a credit institution may check the presence of its customer on one or more sanction lists. The official authorities (national or supranational such as the UN or the European Union) have established lists of persons under sanction which include all natural and legal persons who are subject to a national or international measure and with whom any transaction is prohibited. Originally the lists were made up of personalities linked to drug trafficking. Over time, depending on their activity, individuals or groups have been hit with a nominative embargo measure : political figures from countries under embargo, soldiers prosecuted for war crimes, arms traffickers, etc. (Patrice Bedikian[7]).

The most common screening tool used by financial institutions to meet KYC due diligence and compliance needs is World Check, which is a database of Politically Exposed Persons (PEPs), high risk individuals and organizations. World Check is used worldwide to help identify and manage financial, regulatory and reputational risks, it's creation came from the legislation aiming to reduce the incidence of financial crimes. World-Check information was first used by banks and financial institutions as a comprehensive solution to assess, manage and correct risk. However, as legislation has become increasingly complex and global, the demand for such informations has grown beyond the financial sector to include organizations from all sectors.

When a bank has been sufficiently vigilant, it can report wire transfers, international transactions, suspicious offshore transactions as well as report a "high risk" customer and provide a higher level of oversight.

---

[6] BAM Circular N ° 5 / W / 2017 relating to the due diligence obligation incumbent on credit institutions. [7] Katherine Manning, Know Your Customer (KYC) Process Guide for Banking Services, 2021.

[7] Patrice Bedikian, co-founder of AP SOLUTIONS IO, « La sécurité financière » article of APSCAN, INTERFACE and API for Screening.

So we notice that KYC and AML protocols are almost similar and connected. KYC brings transparency to the fight against money laundering and terrorist financing by using its verification, monitoring and reporting activities to highlight suspicious activity.

The strengthening of the risk-based approach expected by the banking regulator makes it possible to concentrate KYC due diligence on the most critical / high / high risk areas, to size the system accordingly and to reduce the footprint of compliance on the relationship with the greatest number of customers: reduction of compliance costs, satisfied regulators and controlled AML-CFT risks (Alexandre Fenet-Garde, Théodore Kovalkov and Dylan Bergounhe, 2019[8]).

2.2 Sophistication of AML/CFT risks resulting from the COVID-19 crisis

Governments have mostly adopted almost similar policies, in the same sequence, and at around the same time in front of the COVID-19 pandemic, they have taken measures ranging from social assistance to restricting travel in through tax cuts and mandatory containment measures. These measures to contain the pandemic, however, may have had the unintended consequence of opening up new opportunities for criminals and terrorists to generate and launder the proceeds of illicit activities (FATF, 2020[9]).

Fears over the virus have presented a great opportunity for criminals to carry out financial frauds and scams, including :

1) Violations related to the trade in fictitious or non-compliant sanitary equipment: these scams can generally be initiated by fictitious companies or those whose activity has no connection with the sanitary field and thus producing equipment that does not meet the standards health in force ;
2) Violations related to scams and donation scams :
   - Fraudsters create domain names or email addresses pretending to be NGOs or public administrations ;
   - In some cases, a pivot person receives international transfers on the grounds that they are donations to be redistributed to individuals ;
   - The unusual increase in client wealth during the pandemic context ;
   - Another variant of this type of scam is to increase fundraising appeals on social networks ;
   - An unexplained increase in the volume of transactions carried out by professionals operating in sectors heavily affected by the pandemic ;
   - Fraud by sending an email under the name of a senior manager of the company asking for example (most generally) to transfer a certain amount of money outside the company or to disclose personal information ;
   - Recurring transfers to various individuals issued by bogus tourism professionals which are justified by the reimbursement of reservations canceled due to a pandemic ;
   - The upsurge in self-proclaimed health and wellness professionals offering a range of fictitious services ;
   - Forgery and use of forgeries when opening accounts that would be funded by remittances of falsified international checks, or recipients of fraudulent international transfers.

Also, malicious or fraudulent cybercrime, fundraising for fake charities and various medical scams targeting innocent victims have multiplied as criminals have tried to take advantage of the pandemic by disseminating false information about COVID- 19 and exploiting people in need of emergency care and the goodwill of the public.

AML-specific trends and typologies have emerged from the COVID-19 crisis relying on the misuse of virtual assets for the laundering of illicit proceeds and on the misuse of the official banking system. No specific typology of FT linked to COVID-19 has been identified by members of the FATF. However, the FATF has cautioned financial institutions against potential risks such as circumventing customer due diligence measures by taking advantage of temporary difficulties resulting from remote working to launder money, increased use of online financial services, the exploitation of economic stimulus and insolvency regimes, the withdrawal of money from the banking system due to instability and the increased reliance on the unregulated financial sector (FATF, 2020).

2.3 Digitalization and new technologies : a solution for mitigating AML-FT risks and customer loyalty in the banking community

As the world's population was forced into lockdowns or strict social distancing during a pandemic, accessing banking services became difficult and placed customers at unnecessary risk of infection. Thus, the use of new technologies and the digitalization of banking services has been of great importance for the continuity of activities, especially by offering its online services, its applications for smartphones, innovative services (temporary lifting of the credit card) or even the electronic signature of contracts, the bank has perfectly assimilated the fact that today, growth depends on digital innovation.

Digitalization could be defined as the dematerialization of the entire value creation chain, which aims to transform the company and reinvent its entire strategy, positioning, organization and customer experience in order to improve its performance. Some innovative technologies have the potential to revolutionize many sectors: Virtual reality used in learning or even today used by some psychologists for specific therapies, augmented reality capable of revolutionizing tourism and guided tours.

By doing a little retrospective work, we see that the world has quickly become "hyperconnected" and that over a very short period of history. In 1984, for example, there were 1000 computers connected to the Internet in the world, 1 million in 1992, 370 million in 2000. Today, the number of connected objects is estimated at 8 billion, and we are

[8] Article co-written with Alexandre Fenet-Garde, Associé Risk Advisory, Théodore Kovalkov et Dylan Bergounhe, consultants Risk Advisory, 2019.
[9] FATF (2020), COVID-19, Money Laundering and Terrorist Financing, Policy Risks and Responses, FATF, Paris, France.

Paper ID: SR21620234335 DOI: 10.21275/SR21620234335

talking about potentially 20 billion in 2020 Today 3.4 billion people have access to the internet, nearly half of humanity (Le cercle Turgot, 2018) [10]. This shows how digital is developing exponentially and integrating our daily lives.

The question today is no longer whether digitization is an opportunity or a threat, but rather to measure its impact because digitization is already here. Technologies are mature, customer behavior and expectations have already been modified by this digital disruption which is now well established. The businesses as well as the whole society must adapt and we already have enough hindsight to see the many opportunities that digitalization has created for businesses and customers.For example, it has enabled the banking sector to rethink customer relations by offering more service, autonomy, flexibility, availability and immediacy. At the end of the 20th century, a few years before the arrival of digital in homes, banks and business advisers were very important to customers.

Previously, it was important for clients to go to a bank branch to see their advisor, who could even be considered a “member of the family”. Today, digitalization is revolutionizing our entire society and this revolution is materialized by many changes in customer habits, behaviors and expectations, as well as the emergence of new players (Pure players and FinTech). The batch of novelties intended to benefit the greatest number does not come without also coming with new risks.

All these developments must change the way the bank sees its business. The arrival of digitalization is above all an opportunity for the banking sector in terms of the posture of the advisor to its clients.

Ho & Mallick (2010)[11] theorize that "despite investments in IT infrastructure, there is no clear evidence of increased productivity of bank workers". For Tournois (2017)[12], "new technologies weaken this form of relationship since many online services have now replaced the adviser". The contribution of the advice is above all the creation of value by the advisor.

The link with digital creates new directions. Already for Strauss in 2013 [13], banking professions were undergoing intrinsic changes : “the advisory profession is undergoing major changes, in particular through the digitalization of banking activity or the appearance of new activities, such as crowdfunding or still brokerage agency ”. In his research, the opening up of the digital world to banking represents a real multiplication of banking players with new objectives put in place.

In a context where bank profitability is disrupted, non-value-generating services are provided by the customer, and the others are repatriated to the agency because they generate bank profitability (Garets et al, 2009)[14]. Although poorly perceived, this digital transition for banks is the subject of a potential creation of digital value for banks according to Julien & Marot (2012) and Tchibozo (2017)[15].

However, the directives relating to the anti money laundering and counter-terrorist financing suggest that the AML/FT risk is higher when the client is not physically present in order to better allow his identification and that the democratization of remote onboarding customers as well as operations carried out remotely complicate document checks, respect the KYC by establishments but also their way of working. Moreover, the Moroccan central bank (Bank Al Maghrib) highlights it in its circular n ° 5 / W / 17 relating to the obligation of vigilance incumbent on credit institutions (2017, p.11)[16] citing : “Are subject to same requirements referred to in Articles 12 and 15 above, requests to open accounts remotely (by electronic means for example).

When opening accounts from abroad, institutions must observe the following additional cumulative conditions :

- Obtain additional supporting documents to confirm the identity of the client (residence permit, passport) ;
- Require that the first transaction credited to the new account be carried out from an account already opened by the applicant on the books of a banking establishment located in a country complying with the standards of the Financial Action Task Force (FATF) ;
- Apply enhanced due diligence measures on the account as long as the client has not presented himself to the agency concerned. [...] "

Even though this increasing digitization would have reinforced certain already existing risks and would have favored the emergence of new ones, as mentioned in the previous part. New technologies such as "Regtech", a sub-segment of FinTech, nevertheless seem to operate in the spectrum of technological regulations by offering traditional banking players services facilitating adaptation to various regulatory technological constraints (KYC, ALM management which is a practice aiming to optimize the return on equity while maintaining an acceptable level of risk….). In fact, even the FATF encourages the use of technology, including Fintech, Regtech and Suptech, wherever possible.

The FATF recently published the Digital Identity Guidelines, which highlight the benefits of a trusted digital identity for maximizing security, privacy and ease of identification of individuals remotely, at the both for the onboarding of a new client and for the completion of

[10] Le cercle Turgot, Banks facing their near future, 2018, p101.
[11] Ho, S. J., & Mallick, S. K., 2010. The impact of information technology on the banking industry, Journal of the Operational Research Society, Vol. 61, No. 2, pp. 211–221.
[12] Tournois N. (2017), Banking Marketing in front of new technologies, Elsevier Masson, Practical Business Management, Paris.
[13] Strauss J.-L. (2013), « Qu’est-ce que l’innovation dans la banque ? », Bank Review, Vol. 762.
[14] Des Garets, Pacquerot M & Sueur I. (2009) The relational approach in banks, myth or reality ? French Management Review, n°191, p.123-138.
[15] Banking and insurance marketing / Anne Julien, André Marot, Edited by Dunod. Paris, 2012.
[16] BAM Circular N ° 5 / W / 2017 relating to the due diligence obligation incumbent on credit institutions.

transactions, while mitigating the risks of AML/FT. The FATF recommends that all countries consider using digital identity, as appropriate, to facilitate financial transactions while managing AML/FT risks during the crisis. He also notes that digital identity systems "have the potential to improve the reliability, security, privacy, convenience and efficiency of identifying individuals in the provision of financial services." Since the AML/FT risks identified by financial institutions or other companies are low, the FATF standards allow them to adopt simplified due diligence measures, which could facilitate their adaptation, in particular to the pandemic context.

In order to meet the regulatory requirements of knowing its customers, in particular with regard to the categorization of customers, the verification of their profile, their risk appetite and also in the context of the fight against money laundering and the financing of terrorism, the automation and optimization of KYC due diligence is also required. Indeed, there are many tools on the market that allow you to quickly probe multiple databases to achieve a more complete, faster and therefore more effective AML-CFT initial risk assessment. Artificial intelligence will also be able, as mentioned above, to accelerate KYC analyzes or analyzes relating to suspicious transactions in order to channel human efforts where it is most relevant.

According to Katherine Manning (2021), digital processes can revolutionize KYC and remove the need for physical interactions while reducing processing time and extracting the full picture of every customer. Optimizing the KYC process with the right steps and the right tools should have the following capabilities :

- Checks the authenticity of identification documents ;
- Captures biometric data ;
- Validate of the customer's identity by cross-checking biometric data with identity documents ;
- Scalable for banks with a global presence or desire to grow ;
- Improve the positive customer experience during boarding.

However, transaction control is more efficient and data quality is improved. Some of these innovations include real-time identity verification to provide fraud protection and security while responding quickly to customer needs. This allows banks to mitigate risk while improving the onboarding experience. Customers can upload the required documents directly to an online portal. The system automatically extracts relevant customer data and flags high-risk requests for processing.

Traditionally, as mentioned by Michael Eisner (2020)[17], for example to perform a credit analysis, it was necessary for a bank employee to manually collect and enter customer information on system. Through automation, lenders can automatically extract and tabulate relevant financial data from documents such as tax returns and balance sheets. Lenders can also screen and rate borrowers, as well as make immediate credit decisions.

Eliminating manual processes gives analysts more time to perform risk assessments and reduces the frequency of errors. Especially since in 2021, a bank can no longer afford to keep its customers waiting, let alone provide them with a bumpy and laborious user experience. A fortiori, when its direct competitors offer a perfectly optimized alternative.

It is possible to take a smarter approach to KYC by leveraging decentralized digital technology, also known as Blockchain, which today can not only meet AML-CFT requirements but also protect individuals personal data and security. Indeed, it guarantees :

- Processing speed without deteriorating the quality of the verification process, even better, its reliability is significantly enhanced : it is no longer a question of simply checking the conformity of a document (on the basis of a cross-checking of partial information), but to go directly back to the source to verify the authenticity of the document in question ;
- Confidentiality and security : thanks to its cryptographic processes, the Blockchain makes it possible to effectively protect the identity of its users and the confidentiality of information stored within the framework of KYC procedures. Therefore, rather than resorting to centralized storage on a server (and exposing themselves to particularly compromising data leaks), companies today have every interest in relying on the Blockchain in order to preserve their customer's data and to comply with their various legal obligations in this area. Blockchain technology indeed provides more resilience (especially in the event of a failure thanks to its distributed ledger), but also an additional layer of trust and traceability making it almost impossible for a cyber attack to occur. From a technical point of view, because they encrypt information transfers between two systems in the form of fingerprints or signatures, the hash functions used guarantee the security and reliability of the information of each actor, at the same time preventing any modification attempt subsequent to the initial entry.

3. Conclusion

In the end, only the customer counts. For a long-term vision, entering into a relationship is of major importance. The goal is to avoid friction and to build customer loyalty. Let it go quickly and be done without a hitch. While compliance with KYC standards can increase costs and lead times when implemented through existing systems and manual labor, it is important to note that KYC innovations such as automation and blockchain can help increase accuracy, efficiency, cycle times, auditability, transparency, centralization, overall compliance and customer satisfaction. KYC is an essential process to reduce fraud, money laundering, financial irregularities, etc. However, now is the time to simplify the KYC process with future-proof technologies.

However, a change in mindset will also be required on the part of regulators, who should review their conception of the

[17]Michael Eisner, Automation of customer reception in commercial banks, 2020.

compliance process, especially their perception of KYC protocols and their AML/ CFT methods and data sharing. The financial crime detection framework must be transformed into a cost-effective technological model, focused on aligning the efforts of all stakeholders, and allowing information to flow easily between the public and private sectors.

Applying an intelligence and data-based approach to combating the financial activities of organized crime can only be truly effective if this approach is based on collaboration, not only between organizations. banks, but also between them and governments, regulators, auditors and security agencies.

It is in everyone's best interests that banks move away from their compliance-driven approach to financial crime and adopt a proactive prevention and control approach.

References

[1] PwC Future of Customer Experience Survey 2017/18.

[2] PEYRARD Josette et PEYRARD Max, Finance dictionary, Vuibert, 2nd edition, 2001.

[3] STIGLITZ Joseph, Principles of modern economics, Bruxelles, Paris, de Boeck University, 1st edition, 1997.

[4] Jean-Paul POLLIN, « macroéconomie - Systèmes financiers », *Encyclopædia Universalis* [on line]. URL :https://www.universalis.fr/encyclopedie/macroeconomie-systemes-financiers/

[5] Michel Dietsch & Philippe Wahl, « Revue d'économie financière - Système financier et création de valeur », Financial Economics Association[on line]. URL : https://www.aef.asso.fr/publications/revue-d-economie-financiere/106-systeme-financieret-creation-de-valeur

[6] Law No. 03-03 on terrorism (2003) supplementing the Criminal Code.

[7] Law No. 43-05 relating to AML as amended by Law No. 13-10 supplementing and amending the Criminal Code.

[8] BAM Circular N ° 5 / W / 2017 relating to the due diligence obligation incumbent on credit institutions.

[9] BAM Directive No. 3 / W / 2019 relating to the implementation of the risk-based approach in terms of due diligence incumbent on credit institutions and similar organizations.

[10] Katherine Manning, Know Your Customer (KYC) Process Guide for Banking Services, 2021.

[11] Patrice Bedikian, co-founder of AP SOLUTIONS IO, « La sécurité financière » article of APSCAN, INTERFACE and API for Screening.

[12] World Check by Refinitiv URL : https://www.refinitiv.com/en/products/world-check-kyc-screening/about-world-check

[13] Article co-written with Alexandre Fenet-Garde, Associé Risk Advisory, Théodore Kovalkov et Dylan Bergounhe, consultants Risk Advisory, 2019.

[14] FATF, COVID-19, Money Laundering and Terrorist Financing, Policy Risks and Responses, FATF, Paris, France, 2020.

[15] Marie-Agnes NICOLET, New compliance challenges : Scope of the non-compliance risk mapping function, 2015.

[16] Ho, S. J., & Mallick, S. K., The impact of information technology on the banking industry, Journal of the Operational Research Society, Vol. 61, No. 2, pp. 211–221, 2010.

[17] Tournois N., Banking Marketing in front of new technologies, Elsevier Masson, Practical Business Management, Paris, 2017.

[18] Strauss J.-L., « Qu'est-ce que l'innovation dans la banque ? », Bank Review, Vol. 762, 2013.

[19] Des Garets, Pacquerot M & Sueur I., The relational approach in banks, myth or reality? French Management Review, n°191, p.123-138, 2009.

[20] Banking and insurance marketing / Anne Julien, André Marot, Edited by Dunod. Paris, 2012.

[21] Le cercle Turgot, Banks facing their near future, p101, 2018.

[22] Michael Eisner, Automation of customer reception in commercial banks, 2020.

[23] « Les enjeux de la connaissance client à l'ère numérique », ARCHIMAG Magazine, 2021.