Banking in Ghana and the Outlook on Customer Due Diligence (CDD) Measures Amid Covid-19
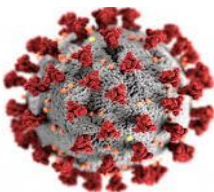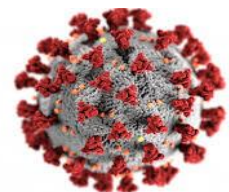
February 22, 2021 - Nana Oparebea Mante - Lead Consultant

34 Chaffinch Avenue, London, CR0 7SE
Tel.: +44 79503 77849; Email: info@opselcompliance.com
www.opselcompliance.com

Introduction

The COVID-19 pandemic has led to unprecedented global challenges and disruptions to businesses in all sectors, including the banking sector. Banks have had to adopt new ways of conducting business given the prevailing measures and protocols such as lockdowns and social distancing aimed at preventing and reducing the spread of the COVID-19 virus. In some regions in the West, the banking industry is operating almost entirely remotely. Going by how the COVID-19 pandemic has accelerated the trend towards digitalization, the adoption of new technologies will continue to drive change in the financial sector post-COVID-19.

This article looks at how banks in Ghana are adapting compliance procedures, specifically Customer Due Diligence (CDD) procedures amid the COVID-19 pandemic to ensure banks meet their regulatory obligations at all times. The article also analyses some key issues related to CDD that should be prioritized by the regulator, management, and compliance professionals in the Ghanaian banking industry.

Although some of the issues discussed do not apply equally to all the banks in Ghana and while many of the issues are relevant outside the borders of Ghana, the analyses in this article are focused primarily on issues related to the Ghanaian banking industry.

Why Money Laundering (ML) and other Financial Crime issues must be a priority in Ghana.

Before the pandemic, one of the most pressing financial crime challenges facing financial crime experts was increase in cybercrime and the growing sophistication of cybercrimes. Unfortunately, the ongoing global pandemic has exacerbated cybercrime. Whiles governments around the globe are taking various measures to contain the spread of the disease with some governments rolling out mass vaccinations programmes, opportunistic criminals are also looking for ways to exploit lapses in Anti-Money Laundering (AML) controls to perpetuate crimes. Given that CDD is one of the primary tools used to detect money laundering and other financial crimes, banks in Ghana must tighten CDD and other compliance procedures. More so because Ghana is grey listed by the Financial Action Task Force (FATF) and the European Commission (EC) for having deficiencies in its AML frameworks. As such, it would be prudent for the Ghanaian banking sector to increase efforts towards attaining the FATF global Anti-Money Laundering and Counter Terrorism Financing AML/CTF and other Anti-Financial Crime standards to redeem the country's reputation on the global stage and avert its implications on the economy.

Bank's customer due diligence requirements?

The requirement to carry out CDD measures is derived from the FATF Recommendation 10 ([1]) on customer due diligence (CDD) applicable to all regulated businesses in member states. The Bank of Ghana and Financial Intelligence Centre Anti-Money Laundering/Combating the Financing of Terrorism & the Proliferation of Weapons of Mass Destruction (BoG & FIC - AML/CFT& P) Guideline ([2]) for Banks and Non-Bank Financial Institutions in Ghana July, 2018, sections 1.4 &1.5 on CDD and CDD Procedures stipulates CDD requirements for banks in the country to carry out various CDD measures to identify, manage and mitigate their overall ML and other FC risk an ongoing basis. Principally, CDD covers both Know Your Customer (KYC) and Ongoing Due Diligence procedures. Banks are to conduct CDD procedures using the risk-based approach to ensure that more resources are allocated to high-risk areas. To summarise, banks must carry out:

Identity Verification: Verify clients identity and be reasonably satisfied that the client is who they say they are and live where they say they live when opening new account or when undertaking occasional transactions. Banks can conduct ID verifications manually, by corroborating various paper-based documents to verify the identities of customers to meet differing levels of KYC/CDD requirements or can do so entirely digitally, using digital ID Verification Systems.

AML Screening: Screen clients and clients' related parties for Political Exposed Person (PEP), Sanctions, and Adverse Media status at onboarding and retrospectively as dictated by client's risk rating to understand the inherent risk associated with the client to enable banks to take proportionate measures to counter risks identified. Where electronic payments are concerned, adherence to the FATF Recommendation 16 ([3]) on Payment Transparency is required.

KYC Review: Regularly review the KYC and other customer due diligence information held on clients and keep them up to date with client's transactions or activities to ensure ML and other FC controls in place remain effective continuously.

Transaction Monitoring (TM): Monitor clients transactions/activities to report suspicious transactions/activities. Post-event TM involves matching clients transactions against already documented expected transactions or activities based on onboarding or periodic CDD information collated to highlight any deviations. The flexibilities of the risk-based approach allow banks to adopt TM approach suitable for their business type and volume of business activity generated. Hence, a bank's design and implementation of TM programme must be based on individual bank's specific risks, contexts and needs. To that end, a bank can use a manual process, or an automated process aided by TM solution or system to conduct TM. Whichever process a bank uses must be commensurate with identified risks. Where a bank generates large numbers of transactions, it is appropriate to have an automated TM system in place to be able to safeguard the effectiveness, consistency, and processing time of the transaction monitoring.

COVID-19 responses and impact of lockdown on CDD Measures on Banks in Ghana.

Since 2017, Ghana has embarked on the financial sector clean up by consolidating banks to reduce the numbers and promote best practices in the sector. Currently, there are 23 banks ([4]), consisting of 14 international banks and 9 indigenous banks with 1,225 branches spread across the 16 regions of the country. In addition to the 23 universal banks, there is one mini-central bank, Association of Rural Banks (ARB) Apex Bank responsible for supervising the 145 rural and community banks (RCBs) in the country. RCBs are also regulated by Ghana's central bank and regulator, the BoG, and thereby form part of the country's regulated financial sector. ARB Apex Bank provides only specialized services essential to improving the quality and scope of products offered by RCBs and important supervisory functions delegated by the BoG. RCBs are the largest providers of formal financial services in rural areas and represent about half of the total banking outlets in Ghana.

Responding to the needs of the COVID-19 business environment, FATF issued a Digital Identification ([5]) guide in March 2020 to assist governments, regulated entities and other relevant stakeholders in determining how digital ID systems can be used to conduct certain elements of customer due diligence (CDD) under FATF Recommendation 10. Key to the implementation of this guidance is for governments to provide assurance checks on the reliability and independence of a digital ID system whether the digital ID Verification System

is provided by a government body or by a private organisation. This is to ensure that whatever digital ID system is being used in a country is officially recognised as appropriate for CDD. In other words, a state authority must provide the assurance that the ID system is derived based on technology, sufficient governance, processes, and procedures that provides the levels of confidence that the system produces accurate results.

The BoG embracing the digital transformation happening in the banking industry, established the BoG Fintech and Innovations Office, in May 2020 to license and develop polices to promote Fintech, innovation, and interoperability in the country. GVIVE is an online ID Verification System licensed by BoG that integrates with existing ID database systems for real time ID Verification. The GVIVE online ID Verification System is linked to the Electoral Commission, the Passport Office, the Social Security and National Insurance Trust (SSNIT) and Drivers and Vehicle Licensing Authority (DVLA) database. A large number of the banks relied on GVIVE to verify clients identities remotely, except for the aforementioned IDs issued in 2020 since the national database linked to the system has not been updated with the IDs issued in 2020. Ghana also launched GhanaPostGPS in 2017 to pushed forward digital addressing systems. It is worth the mention, that before the pandemic, electronic commerce on the internet used for online payment and online banking was prevalent among banks in Ghana. Most banks in Ghana use a combination of manual and digital ID systems to verify and authenticate client's identity.

Part of the Ghana government's initial COVID-19 measures was a partial lockdown of the worst affected cities in the country, namely Accra, Tema and Kumasi for three weeks in April 2020 and mobility restrictions to and from the worst affected areas. All the other cities in the country were allowed to go about their usual daily activities but were required to observed other COVID-19 safety measures.

As a result, the majority of banks in the affected cities did not close down entirely but operated reduced services by keeping a number of branches opened and a small number of staff working remotely. This enabled the banks to offer both remote and in-person account opening services using a combination of manual and automated procedures to verify prospective clients identities whiles maintaining COVID-19 safety protocols. Many banks in Ghana, both small and big banks, rely primarily on AML technological solutions to conduct their TM procedures, as such, these banks were able to generate system alerts to investigate for potential suspicious transactions whether working onsite or remotely during the partial lockdown. According to the BoG reports, (⁶) over 85% of universal banks in Ghana have automated AML tools that allow real-time monitoring of unusual transactions for the identification and reporting of suspicious transactions. The problem that can arise here is that, for banks in Ghana who do not store their customer reference data electronically, the unavailability of customer reference data or information online for the investigative team to verify findings when working remotely can impede the timelines and quality of alerts clearance and documentation. Bearing in mind that effective transaction monitoring is heavily reliant on customer's KYC/CDD data and information. The banks need to consider how to store customer reference data electronically to support remote working.

Whereas the precise responses to the COVID-19 crises in each bank in the country may vary depending on the bank's nature of business, IT infrastructure and peculiar response to COVID19 crises, the general indication is that the initial partial lockdown in April 2020 did not cause any significant disruptions to the banks' CDD procedures. By and large, the banks were able to ensure continuous compliance with the regulations because a number of staff worked on site. However, with the recent upsurge of COVID-19 infections in the country, can the banks continue to carry out CDD procedures when working entirely remotely if Ghana

goes into full lockdown and how are banks in Ghana preparing for the post-COVID-19 banking industry?

Observations, considerations & the way forward

Critical to banks' business continuity during national lockdowns in Ghana and staying compliant with respect to CDD obligations will be determined by (i) how the banks in Ghana can shift from traditional KYC processes to eKYC processes (ii) how banks can migrate customer data/information to digital information with speed and scale up to meet the new ways of working and (iii) how banks can design and implement effective TM procedures aided by the right TM technological tools. It is essential to have the right processes in place from onboarding to transaction monitoring, but more importantly, the technology supporting these processes also needs to be fully compliant with the regulations and approved by the relevant authorities.

ID Verifications

eKYC is a pivotal approach that enables banks to conduct KYC remotely. The COVID-19 crises have brought to the fore the importance and urgency of adopting eKYC for business continuity during crises and its survival in the post-COVID-19 digital banking industry. Studies have shown that digital ID systems rely on more robust methods for identifying and verifying clients than the manual collating of paper documents which can be falsified and misplaced relatively easily. Furthermore, Digital ID verification can improve the accessibility, efficiency, and transparency of service delivery, and serve as a foundation for the digital economy. Once government recognises a digital ID system as an independent and reliable digital ID system to verify a customer's identity it can be used in a wide variety of settings, and its widespread adoption can pave way for financial inclusion. Hopefully, the authorities working on updating the national database linked to GVIVE will increase efforts to ensure that the database is updated in good time so that the banks can rely on GVIVE for remote ID verifications and authentication of the aforementioned national official IDs including those issued in 2020.

Data Management & Privacy Protections

The evolving digital business environment and remote working increasingly mandate a rethink of strategic approach to CDD procedures related to access, processing, and storage of CDD and regulatory issues around customer privacy protection. Banks in Ghana must therefore reconcile the need to build privacy protections into their technology, data management, business strategies and operational processes to prevent breaches. Building solid data management and governance foundations now is what will help the banks in Ghana to become a data driven organisation in this evolving digital and information age. Banks ought to centralise data and information throughout the organisation as opposed to being stored in silos in different departments, that way, proper checks can be put in place to ensure that data captured is complete and correct, categorised, and validated to support compliance needs. Additionally, data and technology are the enablers of evolving digital trends, the functions of AML and AFC make compliance one of the most data rich parts of the banking business. Therefore, it is good to see the value that the right data management can bring to a business in terms of analysing data with analytics to derive insight to inform business decisions or to provide better customer experience.

Transaction Monitoring (TM)

The global upsurge and increasing sophistication in cybercrime associated with the COVID-19 pandemic necessitates a corresponding increase in transaction monitoring efforts by banks everywhere. According to the Ghana National Risk Assessment 2018 [7], over 95% of suspicious transactions reports (STR) received by Financial intelligence Centre (FIC) from 2010 to 2018, were reports on fraud. Cybercrime in the form of romance fraud, advanced fee fraud and gold scams are the most commonly committed offences in Ghana. In a recent survey by the author, responses from 10 of the banks in Ghana that took part in the survey revealed the trend has not changed. Cyber fraud continues to top all predicate offences in Ghana. Hence, banks need to ensure their TM systems and controls are effective for mitigating the types and levels of fraud and other FC risks banks are exposed to.

Considerations for effective TM programs

Accurate identification & assessment of business-wide risks: Accurate risk assessment and the use of relevant typologies and scenarios supports effective transaction monitoring. Given the growth in both online financial transactions and increase in cybercrime, there is the need for banks to revisit their risk assessment and adapt their set of business rules to reflect the current nature of fraud activities linked to COVID-19, such as phishing, business email compromise, tax frauds, advance fees frauds, fake medicines, and fund raising for non-existing non-profit organisations carried out by the so called 'Yahoo Boys' and 'Next-Level Cybercriminals' operating in the sub-region, to ensure continued effectiveness in the execution of TM controls.

Continuous evaluation of rules/scenarios: Among other things, to obtain and maintain an effective and efficient TM program, a continuous evaluation is required. The effectiveness and efficiency of scenarios must be assessed continually. Continuous tuning and control documentation is key for banks to reduce false alerts and be able to document rationale for tuning for audit purposes. There is also the need for business intelligence from the frontline staff, alert investigations teams, and BoG's FIC on relevant fraud and AML typologies within the region to shape and improve the effectiveness of existing TM program.

TM Maturity Model: One of the workable ways to improve and maintain effective and efficient TM procedures and processes in the banks is the use of TM Maturity Model for the continuous evaluation of post-event TM processes in banks as practiced by De Nederlandsche Bank NV (DNB), the central bank of the Netherlands. Central to the DNB Post-Event TM Maturity Model[8] is the conducting of Systemic Integrity Risk Analysis (SIRA) at the operational level and translating the outcomes from SIRA into policies, and procedures and risk-based TM approach where business rules set to flag detection can be traced to the outcomes of the residual risk resulting from the SIRA. Experience from the Netherlands TM Guidance demonstrates how the Dutch regulator used the model to set out expectations regarding envisaged behaviour in supervision practice, an appropriate application of the legal framework relating to the requirements of transaction monitoring. The BoG should consider adopting a similar approach by providing a TM Maturity Model guidance for the banking sector in Ghana. The proponents of AML maturity models argue that as opposed to compliance audits that focuses on reviewing the adherence to compliance processes, maturity assessments tend to be more collaborative and therefore more effective in facilitating the embedding of cultural change and developing compliance capability. (Owori et al, 2015, Page 7)[9]. Using the Maturity Model and the Systemic Integrity Risk Analysis (SIRA) methodology, the banks can strengthen TM controls and/or redesign continuous controls monitoring programs.

Trends in TM technologies: Technological innovations in TM solutions that use Artificial Intelligence (AI) and Machine Learning (ML), are empowering tools that can give business decision-making processes a massive upgrade. Compared to the TM solutions with basic analytics capabilities that flag alerts by screening customer activity against a set of rules/scenarios to search for deviations. TM solutions with AI and Data Analytics are better at highlighting links and trends within bank's data and therefore better for detecting fraud and other suspicious activities. The DNB guidance encourages the use of advanced technological tools for TM, accentuating the use of data analysis and AI in TM such as the use of big data and data modelling techniques to increase possibilities of detection of unusual patterns of transaction and deviations of transaction behaviour.

Quest for AML technological tools

Arguably, the latest wave of technological breakthroughs in mobile money and the use of drones to deliver medical care and equipment to non-urban areas in the sub-region have triggered renewed interest in innovative technologies to enhance work processes. Currently, a large number of the indigenous banks rely on TM solutions driven by technologies with basic analytics, with few more relying on TM solutions with enhanced analytic capabilities such as robotics process automation (RPA) and machine learning (ML). The need for innovation and adaptability is at an all-time high among banks in the SSA sub-region, including Ghana. Especially the need to follow trends in shifting from rule-based solutions to monitoring solutions with advance analytics ideal for todays' complexities of online risk and real-time continuous monitoring, but due to the absence of technological infrastructures and lack of financial resource, most will be constrained. The profit margins of banks are likely to plunge as a result of the COVID-19 pandemic, this may aggravate an already bad financial situation; but for a few multinational banks and indigenous big commercial banks in the country with deep pockets who will have the financial resources to invest in new technologies, most of the medium and small banks in the country will be disadvantaged as they may not be able to afford these digital technologies and will continue to rely on traditional customer due diligence procedures, thereby creating a slower process in adapting to the new ways of working.

Human capital

We cannot rely on complete automated CDD process to achieve effective CDD outcomes. At best AML or compliance technology can help detect unusual activity and not suspicion. It is important, therefore, to recognise that the human element is a very critical element of an effective compliance procedure and CDD for that matter. Banks require human analysts to determine whether an unusual activity flagged by a TM solution is a suspicious activity. Regardless of the pace at which the Ghanaian banking industry transcends from traditional CDD processes to digital processes, at some point, some restructuring in the banking sector will be needed. New functions will emerge which will require different kinds of skill sets, demanding upskilling and reskilling in data analytics, cloud computing and cybersecurity to build the required human capital. Frontline functions that are more exposed to information processing will be more affected by digital disruption. Now is the time for the banks to encourage reskilling and upskilling of talent to meet the needs of the digital banking industry. The banks must take advantage of Ghana's youthful technology-savvy population who have a good understanding of mobile applications, social media, and data analytics and prepare them to take up the new digital functions. Technology-savvy youth can be used in frontline customer services as they can easily engage with customers using digital communication channels to facilitate the high customer experience standards in this digital banking age of convenience.

Conclusion

In the pre-pandemic banking industry in developing countries, it was Fintech start-ups that were rapidly transforming the banking industry. Ghana in particular is often cited as one of the countries that has witness a positive and dramatic impact of mobile technology on financial inclusion in sub-Saharan Africa. COVID-19 has also crystallized and accelerated the technological disruption of the banking industry globally. Given the importance of digitalization to business continuity and maintaining continuous compliance with regulations. A critical step would be for government to invest in digital capital to create an enabling environment for banks to accelerate digitalization to reduce the technology gap in an attempt to catch up.

How can Opsel help?

Opsel can work with you to determine the gaps in your AML and Financial Crime Compliance programs in regard to complying with KYC/CDD, Fraud, Bribery & Corruption, Sanctions, Data Protection & Privacy requirements.

- **Transaction Monitoring Programs**
  we can work with you to assess the effectiveness of TM programs, identify any gaps in current TM program, design and implement an effective TM program using the DNB SIRA methodology tailored to cover all relevant integrity risks specific to your bank and industry.

- **AML & Financial Crime Audit Reviews**
  We can review your current AML and Financial Crime programs in relation to the applicable regulatory requirements and make recommendations by comparing against best practices, and industry standards.

- **AML & Financial Crime Training**
  We can work with you to design a comprehensive training and assessment program that equips individuals and specialist teams to ensure a thorough understanding of the financial crime risks and controls within your organisation.

  We offer high quality and relevant training in all areas of financial crime and compliance. To learn more about Opsel and our training programs go to: www.opselcompliance.com. Contact: info@opselcompliance.com or via our contact page.

Reference

[1]. The FATF Recommendations; International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, Oct. 2020; Page 64

[2]. Bank of Ghana and Financial Intelligence Centre Anti-Money Laundering/Combating the Financing of Terrorism &the Proliferation of Weapons of Mass Destruction (AML/CFT & P) Guideline for Banks and Non-Bank Financial Institutions IN Ghana; July 2018, Part A,

Section 1.4 & 1.5 Page 5

[3]. The FATF Recommendations; International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, Oct. 2020; Page 78

[4]. Bank of Ghana Banking Sector Report; July 2019, Page 4

[5]. The FATF Guidance on Digital Identity; Page 5

[6]. National Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Risk Assessment of Ghana 2018, Page 34

[7]. National Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Risk Assessment of Ghana 2018, Page 46

[8]. www.dnb.nl/en/sector-information

[9]. Owori T et al (2015); 'The Financial Industry Maturity Model for Anti-Money Laundering' *International Journal of Business Excellence* (January 2015), 8(4):492, Page 7,

DOI: 10.1504/IJBEX.2015.070317.