Compliance and Financial Crime Risk in Banks

A Practitioners Guide

Sophia Beckett Velez Ph.D.

Compliance and Financial Crime Risk in Banks

This page intentionally left blank

Compliance and Financial Crime Risk in Banks: A Practitioners Guide

BY

SOPHIA BECKETT VELEZ, PHD

Walden University, USA

United Kingdom – North America – Japan – India – Malaysia – China

Emerald Publishing Limited
Emerald Publishing, Floor 5, Northspring, 21-23 Wellington Street, Leeds LS1 4DL

First edition 2024

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

ISBN: 978-1-83549-042-6 (Print)
ISBN: 978-1-83549-041-9 (Online)
ISBN: 978-1-83549-043-3 (Epub)

To my daughter Shikurah Velez, you are my biggest cheerleader, and I am thankful for your love and support.

To Victor Velez, thank you for believing in me.

To Peter Chidolue SJ, thank you for pushing me when I wanted to give up on my dreams.

To Marjorie Grant my mom whom I love so dearly, thank you for believing in my talents and investing in my education.

This page intentionally left blank

Contents

List of Tables

Chapter 5

Chapter 6

Chapter 7

About the Author

Sophia Beckett Velez, PhD, has worked for over 16 years as a Certified Public Accountant (CPA) with large banks providing consulting services. Her work experience has provided her with valuable background information on the banking industry in general. As a CPA, she worked for firms such as PricewaterhouseCoopers, where she performed financial audits, attestation services, and risk management analysis of large banks. Many of the regulatory compliance problems noted during her review of the large banks required her to cultivate relationships with line of business managers, and work with them to develop action plans and solutions to the issues noted. This has sparked her research interest in exploring the issues at hand in global banks.

This page intentionally left blank

Preface

The US and global banking regulators have enforced regulatory compliance laws to minimize (money laundering, terrorist funding, human trafficking, fraudulent banking activities, bad mortgage loans) that exposed banks to significant risks and losses which banks have complained that it is over regulation. This book discusses anti-money laundering standards, counter-terrorist financing measures that are aligned to AML program that cover BSA laws and control activities (prevent, detect, monitor) designed to mitigate breaches.

A qualitative e-Delphi study of 10 banking finance experts were convened to build consensus on compliance practices senior bank managers can implement that can be effective in reducing losses in banks/bank holding companies. This book offers consensus on (a) maintenance of effective and independent compliance consistent with the organizational objectives, (b) clear definition of data source for compliance analytics, (c) compliance monitoring, (d) reporting activities promptly to upper management, (e) top leadership must be a champion of code of ethics, and (f) understanding regulatory compliance activities that are effective.

This book offers an original contribution to the field of banking that undergraduates, master's, PhD students, academics, and researchers can use to gain a deeper understanding of compliance and AML risks in banks and the use of effective management practices. This book will be the first to discuss consensus on effective compliance practices in banks. Sophia Beckett Velez PhD has over 16 years of experience as a Certified Public Accountant (CPA), providing consulting services to large banks.

Sophia Velez
0000-0002-8382-3090

This page intentionally left blank

Acknowledgments

This book could not have been written without the support and encouragement of my daughter Shikurah Velez.

This page intentionally left blank

Introduction

Outline of Chapters

This book is divided into three parts. Part 1 discusses Regulatory Compliance in Domestic and Global Banks. Part 2 examines Compliance Laws and Requirements (BSA/AML). Part 3 reviews Compliance Environment and Effective Leadership Practices.

Part 1: Regulatory Compliance in Domestic and Global Banks

This part of the book discusses regulatory compliance laws that have placed stress both financially and operationally on large global banks in the United States of America (USA) and around the world. The lack of effective compliance risk management practices to control growth of fraud and money laundering spread throughout the global economy.

Chapter 1: Regulatory Compliance Requirement and Practices

In this chapter, I discuss increased in regulatory compliance laws that have placed stress both financially and operationally on global banks in the United States and around the world business practices. US and global banking regulators have enforced regulatory compliance laws to minimize bank risks (money laundering, terrorist funding, human trafficking, fraudulent banking activities, bad mortgage loans) that exposed them to significant losses which banks have complained that it is over regulation.

Chapter 2: Regulatory Compliance in Global Banks

The US and global banking regulators have enforced regulatory compliance laws to minimize bank risks (money laundering, terrorist funding, human trafficking, fraudulent banking activities, bad mortgage loans) that exposed them to significant losses which banks have complained that it is over regulation. This chapter highlights penalties and punishment issued to banks and other financial institutions for being not in compliance with SAR requirements as noted in anti-money laundering laws that have been astronomical.

Chapter 3: Compliance Requirements in BHC and International Holding Companies (IHC)

This part of the book discusses compliance costs have increased for banks, and regulators have seen an increase in their monitoring costs of these compliance regulations. An in-depth look at some of the significant increases in banks compliance costs are related to complex tracking and reporting systems to meet the enhance compliance requirements.

Chapter 4: Compliance Failures in Global Banks

Global banks have failed to implement an effective compliance program to address regulatory requirements of AML, Basel III, and Dodd Frank 2012 Bill. Banks assigned low-risk rating to high risk countries ignoring serious money laundering risk and opted to have lax AML control, which incentivized drug cartels and money launders to use the bank as their preferred financial institution.

Part 2: Compliance Laws and Requirements (BSA/AML)

This part of the book discusses risk of not meeting government compliance requirement referred to as compliance risk. An in-depth look at banks and financial institutions efforts to prevent themselves from being exposed to receiving penalties due to the business risk exposure of where they transact business (high risk countries, individuals, companies) that are susceptible to the risk of money laundering.

Chapter 5: Implications of Compliance Weakness in Banks and Regulatory Penalties

This chapter discusses banks argument that they lost their competitive edge because they have been cut back on business in some countries to meet AML regulations. Banks have failed to report accurate and complete/updated information that result in them receiving penalties.

Chapter 6: BSA AML Compliance Practices – Ineffective Practices

BSA AML requirements have intensified in recent times to counteract the significant increase in money laundering activities; such as; currency transaction reporting (CTR) thresholds, suspicious activity reporting (SAR), and responses to 9/11 'Know Your Customer (KYC) requirements. This chapter examines significant number of banks moved from manual face-to-face know your customer exercise KYC check to an automated process, which turned out to be ineffective.

Chapter 7: Capital Requirements – Ineffective Practices

This chapter discusses capital requirements were highlighted as key risk mitigation measure that banks and SIFIs need to sustain and survive in a financial crisis. OCC made changes to risk weights of the Advanced Approach system, made updates to the market risk rule to exclude credit rating-based risk assessment, introduced additional capital rules, bank capital levels increases, create a Capital Conservation Buffer, and required banks to have additional capital beyond required levels to mitigate ineffective capital practices.

Chapter 8: Training

This chapter discusses the importance of training employees and stakeholders at all levels within banks. The need for training has been highlighted after the continuous passing of new compliance laws and the severity of risk exposure stemming from lack of knowledge.

Part 3: Compliance Environment and Effective Leadership Practices

This part of the book discusses BSA AML practices when implemented within a framework that includes executive management at the governance and board levels. The use of effective leadership can garner success in the banking sector when top leadership acts as a champion of code of ethics.

Chapter 9: Sanctions

This chapter discusses banks actions to ensure they do not violate the various levels of sanctions imposed by international governments. The United States sanctions are imposed against countries, companies, and individuals that banks are prohibited from conducting business.

Chapter 10: Office of Foreign Assets Control (OFAC) Compliance Practices

Office of Foreign Assets Control (OFAC) implements and manages US economic sanctions. This chapter looks OFAC maintains a website which entails countries, companies, and individuals who act on behalf of terrorist that are placed on a blocked person list known as a Specially Designated Nationals (SDN) and Blocked Persons List. Countries that are on a blocked list are prohibited from sending funds to and from these nations.

Chapter 11: Capital Requirements – Effective Practices

This chapter discusses effective compliance requirements such as maintenance of effective and independent compliance consistent with the organizational objectives; clear definition of data source for compliance analytics; ensure compliance monitoring and reporting activities promptly to upper management; top leadership must be a champion of code of ethics; strong morals and integrity; right products for clients; understanding regulatory compliance.

Chapter 12: BSA AML Compliance Practices – Effective Practices

This chapter discusses BSA AML practices when implemented within a framework that includes executive management at the governance and board levels can garner success in the banking sector. An in-depth review of various lines of defenses involved in the monitoring of the compliance environment in the bank which includes: (i) First line of defense are business level executives/managing directors (create policies and procedures, personnel communication); (ii) Second line of defense Chief Risk Officer (monitoring of AML/CFT policies) independent of business line responsibilities; (iii) Third line of defense – internal audit (audit banks activities and report to audit committee) working collectively to create a low-risk control environment.

Part 1

Regulatory Compliance in Domestic and Global Banks

This page intentionally left blank

Chapter 1

Regulatory Compliance Requirement and Practices

Many large global banks in the United States and around the world have complained about the increase in regulatory compliance laws that have placed stress both financially and operationally on their business practices. Hogan (2021) mentioned new regulations subsequent to the Dodd–Frank Act of 2010 increased banks' average total noninterest expenses by USD 50 billion per year and caused them to reduce or discontinue many products and services such as residential mortgage lending. Many of these compliance laws became more stringent after the 2008 recession relating to capital inadequacy, increase in money laundering, terrorist funding, sanctions, mortgage lending, and redlining laws. The increased risk of bank runs caused by significant banks going out of business due to significant losses, not enough capital to absorb these idiosyncratic losses and continue business, at risk banks not making payments on their debt obligations to other banks, has contributed to a collapse in the banking sector. The US and global banking regulators have enforced regulatory compliance laws to minimize bank risks (money laundering, terrorist funding, human trafficking, fraudulent banking activities, bad mortgage loans) that exposed them to significant losses which banks have complained that it is over regulation. In the United States, the regulatory compliance laws heavily impact Bank Holding Companies (BHCs), International Holding Companies (IHCs), commercial banks struggling to meet regulatory compliance requirements that requires reporting (daily, monthly, quarterly, annual) to various government regulators who oversees these compliance laws. Money laundering, fraud, and capital inadequacy have caused strain on banks from being monitored by numerous regulators in the United States, such as the Office of the Comptroller of the Currency (OCC), the Federal Reserve System (Fed), the Federal Deposit Insurance Corporation (FDIC), and the Office of Thrift Supervision (OTS) (Hogan, 2021). Since the banking sector is interconnected globally, the US government agencies have worked with international banking government agencies to combine their efforts in mitigating global bank risks.

US law enforcement agencies works with task forces, domestic and international, to coordinate their efforts with the Financial Crimes Enforcement Network (FinCEN) and financial institutions (FIs) to fight money laundering

Compliance and Financial Crime Risk in Banks, 3–13

doi:10.1108/978-1-83549-041-920241001

(Johnson & Desmond Lim, 2002). Financial Action Task Force (FATF) established in 1989 by G7 countries (United States, Japan, Germany, France, United Kingdom, Italy, Canada) to prevent global money laundering expanded its focus to include counter terrorism after the September 11, 2001, terrorist attack and financial crimes (Meral, 2020). FATF established the international anti-money laundering (AML) standards, counterterrorist financing measures, and expanded to include 32 members (Australia, Austria, Belgium, Brazil, China, Denmark, Finland, France, Germany, Greece, Ireland, Netherlands, Spain, Sweden, Switzerland, Italy, Iceland, Japan, Canada, Luxembourg, Mexico, Norway, Portugal, Russia, Singapore, Turkey, New Zealand, the European Commission, the Gulf Cooperation Council (Meral, 2020). FATF performs periodic audits, evaluation of the global member countries systems to prevent money laundering, terrorism finance, and published in October 2016 Correspondent Banking Services document which reflected severe penalties for banks related to AML (Meral, 2020). Bank examiners received significant feedback and comments in 2017 relating to the burdens compliance requirements place on the business operations as it relates to Bank Secrecy Act/Anti-Money Laundering (BSA/AML), capital, call reports, Community Reinvestment Act (CRA) (DeMenno, 2020). Fed and other government agencies tackling the prevention of money laundering through BSA/AML laws require banks to implement an effective AML program which they continue to evaluate.

The AML program should cover the BSA laws and control activities (prevent, detect, monitor) designed to mitigate the breach of these laws. The BSA laws in the United States govern the citizens' transactions and require banks to disclose information about their customers to the federal government (Gladstein, 2021). The application of AML laws takes an all-inclusive effort where everyone is a stakeholder in the process of fighting this gruesome act. The fight against AML will require the official regulations of the financial system to include all parties involved such as banks, FIs, securities dealers, and all businesses including money services (Meral, 2020). On the global fronts, General Assembly of the United Nations at the Vienna Convention in 1988 tried to stomp out money laundering with the efforts of the G7 group of nations through the establishment of FATF that examines measures to fight money laundering and the sale of illegal drugs (Johnson & Desmond Lim, 2002). In 1990, the FATF issued 40 recommendations, comprehensive strategy action items against money laundering (Johnson & Desmond Lim, 2002). The global growth of fraud and money laundering spread through the global economy and was linked to 2%–5% of the global gross domestic product (Andrew, 2021). Global money laundering was aligned to illicit funds produced through grand corruption, laundering carried out through complex layering schemes that pass the funds off as legitimate, concealing illegal funds making them hard to detect and their origins (Andrew, 2021). Money laundering schemes range from $800 billion to $2 trillion illegal funds filtrated into the safe haven of western FIs using layering and washing schemes that are used to pass them off as legitimate transactions, causing economic instability (Andrew, 2021). Meral (2020) mentioned there are significant amount of illegal funds from criminal activities and terrorism which affects all countries' security and economic

stability. Money laundering transfers illegal criminal money through laundering activities that conceal sources(drugs, smuggling, gambling, racket, kidnapping, robbery, trafficking women and children) and pass them into the legal financial system (Meral, 2020). Many of these illegal activities thrive in an environment with laxed or weak control activities. The weak internal control and AML programs were seen as a root cause of these FIs' failure to prevent these money laundering schemes. These illegal activities are sometimes tied to terrorism funding activities which the United States is actively trying to prevent and monitor.

The United States have levied sanctions against many of the terrorism-related nations/countries and created a list of countries US institutions and citizens are prevented from doing business. These US-imposed sanctions on countries were extended to include companies and individuals that banks are prohibited from conducting business transactions. US sanctions violations are treated as liability offenses and individuals can be found guilty/liable for committing a civil violation of sanctions without their knowledge of the act or degree of fault (Eckert, 2021). In 2012, sanctions violations civil penalty up to $65,000 per violation were levied on organizations assisting people to travel to Cuba, a nation on the sanctions list (Sullivan, 2018). There is the 2014 plea deal BNP Paribas made in relation to sanctions violation, agreeing to $8.9 billion fine and legal actions against 45 employees (Rose, 2020). The knowledge of the significant fines and penalty attached to being found in violation of sanctions has jolted the degree of seriousness banks have taken these violations. This has bolstered the serious nature of the preventative controls and business decisions taken to avoid this risk of sanctions violation. This is evident where several banks have turned to de-risking their portfolio of clients they conduct business activities because of enhanced due diligence; additionally, there are significant cost incurred to monitor activities that could be in violation of AML and counterterrorist financing regulation (Rose, 2020). There are strategic locations such as doing business near South America, Cuba, and Middle East that carries a higher exposure risk of being found in violation of sanctions or terrorist funding laws due to the high risk of crime associated with these areas and their client base. Banks have seen this de-risking strategy as a preventative measure that will reduce costs associated with monitoring and onboarding, lowering sanctions and reputation risks (Rose, 2020). Many banks feared that human error or failure of detecting an act of money laundering or fraud was not a viable excuse of being found in breach of sanctions and AML laws. This was evident where many banks face significant penalties related to transactions with individuals or entities related to a sanction's regime (Eckert, 2021). Banks were fined when their controls were ineffective over the end location and use of funds, even on situations where there is no actual breach of sanctions (Eckert, 2021). The idiosyncratic growth of money laundering forced global government agents to react with more stringent requirement for banks to implement preventive, detective, monitoring, and timely reporting of monitoring results of global banks AML program.

Banks are required to implement AML control activities to prevent and deter financial and cybercrimes. As part of AML laws, bank managers are required to

complete a Suspicious Activity Report (SAR) that is used to track suspicious activities and identify customers those are involved with money laundering, fraud, and terrorist funding (Rifai & Tisnanta, 2022). Banks are expected to implement various teams that addressed cybersecurity, fraud prevention units, BSA/AML management boards, AML intelligence units, AML analysts/investigators, risk departments, and trained network administrators (Rifai & Tisnanta, 2022). Customer due diligence activities initially carried out at the onboarding of a new customer is an ongoing process throughout the business relationship with the bank; the transaction history of the customer should be reviewed looking particularly at the nature of the actual pattern of transactions against the pattern initially communicated by the customer (ElYacoubi, 2020). Senior bank managers should be actively involved in analyzing the results of customer transaction frequency assessments particularly high-risk customers, Politically Exposed Person (PEPs), and examination of triggered alerts (ElYacoubi, 2020). BSA laws in the United States established a $10,000 daily cash reporting threshold (Gladstein, 2021) which banks use in their daily surveillance and AML programs. Several international foreign governments have established similar threshold for monitoring and reporting of the AML-related transactions as well. Ecuador's Superintendency of Banks issued regulations that established the reporting of currency transactions over $10,000 or its equivalent in foreign currency (Johnson & Desmond Lim, 2002). Venezuela government efforts to fight anti-drug, AML, and unrestrained gambling houses industry enforced the Superintendency of Banking laws requiring the reporting of all transactions $10,000 or 4.5 million bolivars or more, reporting of suspicious transactions, and requiring banks to set up internal financial investigation units (Johnson & Desmond Lim, 2002). Banks have quarterly and annual reporting requirements of their effectiveness with these AML monitoring exercise established by the government and regulators. The failure of banks to block money laundering and fraudulent activities is often met by incurring penalties and fines.

Banks that fail to detect and prevent money laundering schemes and activities received significant fines from local domestic government agents and foreign government bodies. AML and compliance regulations have caused banks to become worried about the ramifications of them being found in noncompliance with these rules. Demetis and Angell (2006) posit that banks could receive heavy fines and jail sentences if bank employees inadvertently allowed a money launderer to operate on their watch. Meral (2020) noted institutions that are found to be in noncompliance with AML legal requirements receive punishments and possible sanctions. For example, several FIs had to pay large fines as they did not implement appropriate preemptive measures to prevent AML, and charges increased from $26.6 million dollars as of 2011 to $3.5 billion as of 2012 (Meral, 2020). The Hong Kong and Shanghai Banking Corporation (HSBC) is a global bank headquartered in London with subsidiaries in the United States; HSBC USA failed to implement properly designed AML program monitoring of suspicious account in areas such as Mexico and the program was poorly staffed (Rathod, 2022). The failure of the banks' AML monitoring program to prevent illegal acts in heavily exposed areas in South America has exposed them to the receipt of penalties from the Fed and other government regulators. The weakness

and ineffectiveness of HSBC AML compliance programs have made them vulnerable domestically and internationally to money laundering illegal acts occurring on their watch without detective and preventive measures stopping the occurrence of these transactions. HSBC USA monitoring program failed to prevent physical purchase of billions of US dollars, bank notes from affiliates (Rathod, 2022). This was evident where HSBC received penalties in the United States and overseas. Regulators emphasize the serious nature of banks that are deemed noncompliance with the AML laws by levying penalties on banks and confiscating assets of perpetrators who take part in AML acts. There are penalties and findings levied on banks who fail to implement timely effective compliance programs and meet the reporting guidelines established in these compliance laws. HSBC was found in violation of the BSA laws, the International Emergency Economic Powers Act (IEEPA) and Trading with Enemy Act (TWEA) (Rathod, 2022). The court documents revealed that HSBC and its subsidiaries allowed the processing of illegal transactions across banned countries like Cuba, Iran, and Libya and permitted transaction to narcotic traffickers and money launderers (Rathod, 2022). HSBC banks' AML compliance programs were ineffective and inadequate on foreign correspondent account holder, which were some of the root causes within the failure of the AML system to prevent fraud (Rathod, 2022). HSBC agreed to its employee criminal conducts and the deferred prosecution agreement by department of justice (DOJ), forfeited $1.256 billion, and paid $665 million civil penalties (Rathod, 2022). The funds from the penalties were allocated to the various government regulators where OCC received $500 million out of $665 million civil penalties and the Office of Federal Reserve received $165 million (Rathod, 2022). On the global front, HSBC faced separate actions by Financial Service Authority (FSA), UK (Rathod, 2022).

The FSA authority levied penalty on Abbey National in the amount of £2.3 million for inadequate AML procedure and inadequate practice by failing to report suspicious banking transactions in a timely manner to the National Criminal Intelligence Service (NCIS) government agency (Webb, 2004). Abbey National took over a month to report 58% of suspicious transactions to NCIS; the institution failed to carry out proper due diligence identity checks on new customers by securing and examining appropriate documents (Webb, 2004). As a result of the lack of effective onboarding due diligence, 32% of new accounts were opened without the appropriate documentation; many of these weakness at Abbey National delayed reporting per regulatory requirements, resulted in lack of awareness about AML customer identification requirements in opening new accounts (Webb, 2004). Onboarding due diligence is seen as key to banks' Risk-Based Approach (RBA). RBA should be a part of the initial customer onboarding process with consideration given to the applicable four identified risk areas(geographic risk, customer risk, product risk, delivery channels) where potential risk posed by the customer is examined (ElYacoubi, 2020). Banks should identify the high-risk types of customer accounts at the onset of onboarding (trusts, PEPs, omnibus accounts, Power of Attorney [POA] accounts, private banking, pooled accounts); many of these accounts belong to gatekeepers (accountants, lawyers, professionals) which lacks transparency of the identity of

the underlying clients/business owner and is not disclosed to the FI (ElYacoubi, 2020). There is over reliance on know your customer (KYC) and AML information relating to these gatekeeper and customer due diligence risk posed by delivery channels due to lack of face-to-face interactions (ElYacoubi, 2020). Prior to onboarding the customer, banks need to have an understanding of what purpose will the account be used for and the nature of the transactions. This will help them in making an assessment of the risk profile of this particular customer (high, medium, low) and make a determination if they want to conduct business with this type of customer. ElYacoubi (2020) posed several questions (is the customer intention to mainly perform online transactions? avail from private banking investments? is there an intention to establish offshore trust account with private bank? will this be simply a basic bank account?) where the answers to these questions will help gather pertinent information to assess customer risk prior to onboarding. Bank should address compliance risks assessment from the beginning and establish the purpose/nature of the banking relationship (ElYacoubi, 2020). High-risk customers at a minimum should be monitored and reassessed annually, medium risk every two years, and low risk every three years. ElYacoubi (2020) mentioned high-risk customers' reputation should be assessed by bank to gain an understanding of the type of institutions and jurisdictions they have business relationships with and consider if they have AML/CFT controls in place. The KYC/CDD laws require banks to establish customer identity, nature of transactions, validate funding, and assess customers' AML/CFT risks through KYC's customer process (ElYacoubi, 2020). The failure to do so results in penalties and findings on the banks.

Additionally, penalties are levied on criminals through the AML laws, but this has failed to deter or lower the numerous criminal acts by these offenders (Rifai & Tisnanta, 2022). Government prosecutors bypass the judicial process to confiscate illegal proceeds and asset used in these AML schemes. Criminals' punishment for money laundering acts is incarceration which is ineffective and insufficient in deterring money laundering acts (Rifai & Tisnanta, 2022). The global government has utilized asset recovery methods to take control of criminal assets used in money laundering fraudulent schemes without having to levy a penalty on the perpetrator referred to as Non-Conviction Based (NCB) Asset Forfeiture (Rifai & Tisnanta, 2022). The NCB Asset Forfeiture methods use assets suspected of being the proceeds of criminal actions portrayed as legal subjects, with countries represented by money laundering investigators' prosecutors against assets suspected of criminal acts proceeds and confiscate them without judicial judgment (Rifai & Tisnanta, 2022). Another area of focus for international banks compliance programs lies in prevention of mortgage fraud which was heavily underscored during the periods leading up to the 2008 recession and thereafter.

Banks' compliance programs have become more intensified after 2007 mortgage scandal to address prior regulations DeMenno (2020) referred to as mortgage lending requirements (Truth-in-Lending Act [TILA] of 1968, the Flood Disaster Protection Act of 1973, the Real Estate Settlement Procedures Act of 1973, the Home Mortgage Disclosure Act [HMDA] of 1975, CRA of 1977) and enhanced these laws. New regulations introduced during and after the Dodd–