Walden University
ScholarWorks

Walden Dissertations and Doctoral Studies

Walden Dissertations and Doctoral Studies Collection

2023

Money Laundering and Terrorist Financing Typologies That Reduce Financial Crime Risks

Sina Vinod Patel
Walden University

Follow this and additional works at: https://scholarworks.waldenu.edu/dissertations

This Dissertation is brought to you for free and open access by the Walden Dissertations and Doctoral Studies Collection at ScholarWorks. It has been accepted for inclusion in Walden Dissertations and Doctoral Studies by an authorized administrator of ScholarWorks. For more information, please contact ScholarWorks@waldenu.edu.

Walden University

College of Management and Human Potential

This is to certify that the doctoral dissertation by

Sina Vinod Patel

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Maja Zelihic, Committee Chairperson, Management Faculty
Dr. Holly Rick, Committee Member, Management Faculty
Dr. Karina Kasztelnik, University Reviewer, Management Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2023

Abstract

Money Laundering and Terrorist Financing Typologies That Reduce Financial Crime Risks

by

Sina Vinod Patel

MPhil, Walden University, 2021

MSA, Walden University, 2018

MSF, Walden University, 2017

BS, The Pennsylvania State University, 2014

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Management

Walden University

May 2023

Abstract

The Covid-19 pandemic has increased concerns over money laundering and terrorist financing and their impacts on societies and the world's finance and economic systems. Some financial institutions are failing to detect and track new emerging financial crime threats. The purpose of this qualitative descriptive case study was to identify predicate offense typologies that U.S. banking and financial services company compliance managers use to reduce the risks of money laundering and terrorist financing. To understand the concepts of predicate offense and financial crime risks, Gary Becker's economic theory of criminal behavior was the conceptual framework that grounded this study. The population was comprised of 15 compliance managers and anti-money laundering investigators. Data sources included semistructured interviews, semistructured observations, and document reviews from business and finance academic journals. Coding, thematic analysis, and content analysis revealed eight main themes as predicate offense typologies: structuring, fraud, cybercrime, human trafficking, illicit arms trafficking, illicit drug trafficking, real estate money laundering, and trade-based money laundering. Four subthemes were identified: red flags, key indicators, typology-specific common signs, and 95% or above. The insights drawn from this study may contribute to efforts by compliance managers to increase transparency and close gaps in the anti-money laundering and counter terrorist financing compliance framework, which could enhance business practice. Implications for positive social change include a reduced risk of bank failures, increased employment opportunities, and promotion of public awareness about financial crimes.

Money Laundering and Terrorist Financing Typologies That Reduce Financial Crime Risks

by

Sina Vinod Patel

MPhil, Walden University, 2021

MSA, Walden University, 2018

MSF, Walden University, 2017

BS, The Pennsylvania State University, 2014

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Management

Walden University

May 2023

Dedication

I dedicate this study to my late great grandfather, Ramji Dada, and my late great grandmother, Maragha Ba. My great grandparents believed that material things can be destroyed and taken; however, knowledge that a human being has about the world in which they live in cannot be taken or destroyed. A person living in a certain city can relocate and establish a new life in another place with the power of education.

Acknowledgments

First and foremost, I want to thank God for all His blessings. Without God by my side every step of the way, I could not begin or complete this wonderful journey. With God, all things are possible. My deepest gratitude to my mother, Surekha; father, Vinod; and brother, Dr. Saran, who envisioned this dream and encouraged me to push the bar higher. My family is my pillar of strength and courage. Thank you for your guidance, understanding, patience, and prayers. Your relentless faith in me motivated me to succeed and become the first in the family to attain a Doctor of Philosophy (PhD) degree. I am deeply and forever grateful for everything.

A special note to my mentor, Kamal uncle, for your constant support, words of encouragement, and help throughout my doctoral journey. Thank you so much for sharing your experiences, expertise, and knowledge. You played an integral role in helping me accomplish my goal. Words are not enough to express my gratitude towards you. I would also like to express my appreciation to all the research participants. Thank you for your invaluable time and contribution to this research study.

My sincerest thank you to Dr. Maja Zelihic, my committee chair, who challenged me to think outside the box, always supported me in times of need, and guided me each step of the way. Also, thank you to Dr. Holly Rick, my second committee member, who challenged me to think about each aspect of my study and dedicated her time and efforts to ensuring a high-quality study. Finally, a sincere thank you from the bottom of my heart to the Walden University faculty and community who shape students into scholars and invest in the success of their doctoral journeys.

Table of Contents

List of Tables

List of Figures

Chapter 1: Introduction to the Study

There are rising concerns about money laundering and terrorist financing in the midst of the Covid-19 pandemic and the impact on societies and the world's finance and economic systems (Jamil et al., 2021). The Financial Action Task Force (2020a) reported that the Covid-19 pandemic has had a profound effect on our banking and financial institutions. Rising unemployment, financial distress, the bankruptcy of organizations, the increased circulation of cash in economies, and accelerated implementation of stimulus programs represent vulnerabilities that criminals have exploited during the pandemic (Financial Action Task Force, 2020a). These factors have influenced and shaped organized crime and illicit markets. The changes in consumer, organizational, and governmental behavior have presented criminals with new opportunities to commit financial crimes and launder the proceeds (Basit, 2020). The rise in Covid-19-related crimes such as fraud, cybercrime, misuse and corruption of government assistance funds, money laundering, and terrorist financing has introduced new sources of proceeds for criminal actors.

The primary focus of this research was on how U.S. banking and financial service company compliance managers identify predicate offense typologies to reduce the risks of money laundering and terrorist financing activities. The compliance managers who participated in this study are experts with anti-money laundering experience in the banking and finance field. The results of this study may help compliance managers to build a new set of indicators or red flags to look out for when conducting their compliance obligations. Furthermore, the findings of this study may lead to positive

social change in terms of preparing the banking and financial industries to adapt to new emerging threats and changing environments such as the Covid-19 pandemic.

In Chapter 1, I provide an overview of the study. After introducing the study, I will present the background of the study, problem statement, purpose of the study, and the research questions (RQs). Next, I will introduce and explain the key concepts that support the conceptual framework. Then, I will provide operational definitions of key concepts and terms, explain the assumptions, describe the scope and delimitations, and define the limitations of the study. Finally, I will transition to Chapter 2 by emphasizing the significance of the study and summarizing the pivotal points of Chapter 1.

Background of the Study

Money laundering is an auxiliary offense in nature and derives from the necessity of a predicate offense from which the illegal proceeds initiate. The predicate offense involves an acquisitive crime that is necessary for the subsequent money laundering process to take place (Keesoony, 2016). Hence, the crime of money laundering is subjective to, but objective of, that predicate offense (Boister, 2012). Specifically, money laundering is the act of hiding the money derived from illegal activities. It is a type of criminal activity that involves concealing illicit funds as lawful income (Nobanee & Ellili, 2018). The process of money laundering includes three stages: placement, layering, and integration. The first stage of money laundering is placement, which is the process of inserting the illegal proceeds into the financial system (Al-Suwaidi & Nobanee, 2020). The second stage of money laundering, layering, consists of converting the illegal proceeds into another asset or fund and creating complex financial transaction layers to

cover up the audit trail and source of funds (Al-Suwaidi & Nobanee, 2020). The third and last stage of money laundering is integration or extraction of the illegal yet seemingly legitimate funds for criminal use, goods, and assets (Al-Suwaidi & Nobanee, 2020). In brief, money laundering is the process of crafting a mask of lawful cleanliness. Criminals manage to perpetrate a predicate offense and launder the illegal money to make it challenging to trail the proceeds.

Alternatively, terrorist financing is a preparatory offense in nature and involves legal or illegal proceeds gathered to execute a future crime of terrorism. Terrorist financing involves the process of moving transactions that may be used by actors to organize terrorism (Al-Suwaidi & Nobanee, 2020). The means to finance terrorist funds differs from lawful to unlawful. Terrorists are inclined to work through ambiguous, undisclosed systems and obscure businesses. Furthermore, terrorists always pursue methods to allow them to launder their acquired assets through apparent business and the substitute transmittal system or clandestine financial networks (Al-Suwaidi & Nobanee, 2020). The illicit funds are necessary to buy arms and cover operational expenses, recruitment, training, and salaries and compensation. Comprehensive anti-money laundering programs and effective compliance strategies can prevent terrorist that finance terrorism from succeeding.

In the post-9/11 world, the banking industry and financial services sector has faced heightened financial crime risks. Globally, trillions of U.S. dollars are money laundered each year (Yeoh, 2020). Lawmakers and regulators have taken steps to hold banks and financial services companies responsible for such crimes. To fight against

financial crimes, the United States government became stringent and amended The USA PATRIOT Act of 2001. The USA PATRIOT Act of 2001 was an extension of the Bank Secrecy Act. The Bank Secrecy Act, legislated in 1970, requires businesses to keep records and file reports indicative of acts related to criminal, tax, and regulatory matters (Mackenna, 2017). In addition, the Bank Secrecy Act requirements rely heavily on law enforcement agencies to identify, detect, and prevent criminal businesses, terrorism, tax evasion, and other unlawful activity. Lawmakers amended the act in the USA PATRIOT Act of 2001. The USA PATRIOT Act of 2001 included requirements that force bank leaders to establish a customer identification program as part of the Bank Secrecy Act compliance program (Mackenna, 2017). Banks and financial institutions were fined for the lack of compliance regulations conducted on financial transactions.

Banks and financial institutions are responsible for creating an anti-money laundering division within their compliance departments. The purpose of anti-money laundering and counter financing of terrorism requirements is to regulate transactions; record and file reports of cash purchases more than $10,000 (daily aggregate amount); identify suspicious behavior or patterns related to financial crimes such as money laundering, terrorist financing, tax evasion, and other criminal activities; and conduct customer due diligence to maintain regulatory compliance (Khan et al., 2021; Mugarura, 2014). Based on certain financial crime risk categories such as amount of transactions, number of transactions, and rule types, an alert triggers in the banking system to indicate the compliance department of unusual activity. Compliance managers of banking and financial institutions are required to mitigate financial crime risks according to the risk-

based approach. The risk-based approach groups customers into high-, standard-, or low-risk categories based on predicate offense typologies, customer profile, type of activity, and pattern of activity (Mugarura, 2014). If the transactional activity cannot be mitigated, a customer is obligated to report the activity and file proper documents. Banking and financial institutions attempt to manage financial crime risks by implementing compliance strategies.

Researchers have conducted recent studies on financial crime risk management from different perspectives. They have empirically assessed the success rate of money laundering controls and inherent flaws and weaknesses in effective compliance regulations (e.g., Cash, 2020; Pol, 2020; Yeoh, 2020). Others have explored how technological innovations affect the evolution of money laundering and modern anti-money laundering and counter terrorist financing methods (e.g., Carayannis et al., 2021; Han et al., 2020; Kurum, 2020; Li, 2019). Although these studies have addressed a wide range of issues, there is a lack of research on comprehensive predicate offense typologies in money laundering (Al-Suwaidi & Nobanee, 2020). A predicate offense is an element of a larger crime that generates monetary proceeds (Rusanov & Pudovochkin, 2021). For example, generating illegal proceeds is the primary offense, and money laundering is the predicate offense. Predicate offenses are crimes underlying money laundering or terrorist financing activity and serve as powerful indicators of such financial crimes. The current state of academic research reveals that there is a gap in the literature and absence of information about predicate offense typologies in money laundering and terrorist financing.

Problem Statement

The issue that prompted this study is the severity of financial crime risks during the Covid-19 pandemic crisis and a need for financial institutions to revise their financial crime risk management strategies with new emerging threats (Crisanto & Preno, 2020). Banking and financial services institutions have undertaken specialized investigations due to increased money laundering and terrorist financing activities. However, the institutions are unable to feasibly detect and track the increased money laundering and terrorist financing activities due to the scale of the offenses, the lack of appropriate tools to counter the offenses, and continual changes to anti-money laundering policies and procedures during the global pandemic (Naheem, 2019). Money laundering and terrorist financing activities expose banking and financial institutions to increased reputational, operational, legal, and concentration risks, which can result in compliance costs, financial penalties, and banking failures (Lawlor-Forsyth & Gallant, 2018; Pol, 2020).

The current state of anti-money laundering and counter terrorist financing regulations utilized by firms exhibit some drawbacks (Chen, 2020). Yeoh (2020) indicated that money laundering risks have become heightened, given the enormity of the estimated total of $500 billion to $1 trillion money laundered globally. Additionally, Pol (2020) indicated that modern anti-money laundering programs are ineffectual because of policy failure and inadequate effective assessments of policy standards and procedures. The general problem is that large U.S. banking and financial services institutions lack modern compliance strategies to mitigate the risks of financial crime (Pol, 2020). The specific problem is that some U.S. banking and financial services company compliance

managers fail to identify predicate offense typologies to reduce the risks of money laundering and terrorist financing activities. There is a gap in the literature on predicate offense typologies in money laundering and terrorist financing.

Purpose of the Study

The purpose of this qualitative descriptive case study was to identify predicate offense typologies that U.S. banking and financial services company compliance managers use to reduce the risks of money laundering and terrorist financing activities. Although researchers have investigated this issue, they have not explored the topic of financial crime risk management in this way. In previous empirical studies, researchers have assessed the success rate of money laundering controls and inherent flaws and weaknesses in effective compliance regulations (e.g., Cash, 2020; Pol, 2020; Yeoh, 2020). Others have explored how technological innovations affect the evolution of money laundering and modern anti-money laundering and counter terrorist financing methods (e.g., Carayannis et al., 2021; Han et al., 2020; Kurum, 2020; Li, 2019). Although these studies have addressed a wide range of issues, there is a lack of research on comprehensive predicate offense typologies in money laundering (Al-Suwaidi & Nobanee, 2020). A predicate offense is a crime that is an element of a larger crime that generates monetary proceeds (Rusanov & Pudovochkin, 2021). For example, generating illegal proceeds is the primary offense, and money laundering is the predicate offense. Predicate offenses underlie money laundering or terrorist financing activity and serve as powerful indicators of financial crimes. The current state of academic research reveals that there is a gap in the literature. Much remains to be done at both the empirical and the

theoretical level, especially in relation to the identification of compliance typologies and indicators of predicate offenses to decrease the risks of financial crime.

Research Questions

The overarching RQ was, What are the predicate offense typologies that U.S. banking and financial services company compliance managers identify to reduce the risks of money laundering and terrorist financing activities? To gain a deeper understanding of the phenomenon under study, I also sought to answer the following subquestions (SQs):

SQ1: How do anti-money laundering investigators identify predicate offense typologies?

SQ2: How successful are the investigators in identifying predicate offense typologies?

SQ3: What characteristics classify money laundering and terrorist financing as predicate offense typologies?

SQ4: How does identifying predicate offense typologies reduce money laundering and terrorist financing?

Conceptual Framework

The concept of predicate offense has become a part of the lexicon of the banking and financial industry. It is germane from a socioeconomic perspective in today's financialized practice of capitalism. The key concepts of this research were predicate offense and financial crime risks. In the late 1980s, predicate offense began to take shape in the form of the Money Laundering Control Act of 1986 (Kemsley et al., 2021). Under this act, to convict a criminal of financial crimes, the legal commission requires two

conditions. First, the offense must be a staid illicit activity; second, the offense must be a premeditated act intended to secrete or hide the funds from the predicate activity (Kemsley et al., 2021). A criminal activity that meets both necessary conditions is sufficient for conviction.

Additionally, under the subsection 18 USC 1956(c) (7) of the Act, a list of crimes is stipulated and classified as specified unlawful activities (Bell, 2002). Most of these activities are correlated with organized crime, and the U.S. Congress frequently adds new offenses to the list. For years, the Financial Action Task Force abides by these two provisions when prosecuting predicate offenses. These two conditions divide the crimes to incur two independent penalties: a penalty for the predicate offense, and a penalty for the distinct financial crime (Kemsley et al., 2021). An articulate conceptual framework for predicate offense and financial crime risks requires a comprehensive understanding of the liaison between the two concepts.

Financial crime risks are derived from the works of criminal syndicates and have significant implications for corporate operations (Reurink, 2016). The three primary components of financial crime risks presented to financial services companies are criminal acts, compliance and monitoring, and intangible impacts. First, criminal acts include concrete financial crimes and clearly illegal acts, such as money laundering, terrorist financing, fraud, electronic crime, bribery and corruption, tax evasion, insider trading, market abuse, and information security (Hasham et al., 2019). Most banking and financial institutions and customers can recognize these types of activities and their domino effect.

Second, compliance and monitoring activities include trading and sanctions compliance, suspicious activity monitoring, and "know your customer" requirements (Hasham et al., 2019). Compliance and monitoring activities are a business expense and are regulated by laws. In recent times, banking and financial services organizations have come to understand how processes and procedures affect anti-money laundering investigators, compliance officers, and consumers. Continual investment in training and revising compliance strategies is regularly compulsory to reduce regulatory fines, sanctions violations, and other financial crime risks (Hasham et al., 2019). Through this effort, banking and financial services organizations can gain value from compliance programs such as anti-money laundering programs.

Last, intangible impacts are the subtler impacts including secondary effect of hindrance, obligations of internal processes, negative effect of consumer disturbance, and reputational damage (Hasham et al., 2019). Other types of less tangible impact are additional resources to support apt regulatory filings or investigations, the audit and supervisory procedure expenses related to ongoing training, opportunity costs, and technology cost to store data. Frequently, these opportunity costs are not computed in the total cost incurred to an organization despite their implication.

The new emerging threats involving financial crime risks necessitate a shift in institutional mindset and a comprehensive understanding of what are the indicators and red flags, why do financial crimes transpire, and how can banking and financial services institutions reduce and limit the effects of this type of risk. Compliance managers need to have an awareness of financial crime risk by understanding how several types of risk

manifest past operational or divisional breakdown. In addition, having an insight about financial crime risk requires an understanding into three main categories: prevention risk, detection risk, and investigation risk. The preliminary stage of the financial crime risk framework involves future predictive threats of a banking or financial services organization. Prevention risk involves activities to stop any suspicious or unlawful activities before they develop into a problem (Spencer Pickett & Pickett, 2002). An initiative-taking approach to address financial crime risks warrants teamwork and expertise across the organization. This approach can benefit an organization by reducing the risk of financial crime and consequential costs (Spencer Pickett & Pickett, 2002).

Consequently, the second stage of the financial crime risk framework consists of detection risk—in other words, the ability of compliance managers to recognize and counter operative or occurring threats. To manage this risk type, accuracy and speed are required to halt a criminal act or the consequences of a financial or data damage, compliance breach, or consumer disorder (Spencer Pickett & Pickett, 2002). By recognizing certain patterns and understanding the nature of threats, banking and financial services institutions can identify high-risk, criminal activities (Hasham et al., 2019). The final stage of the financial crime risk management framework is investigation risk. The investigation step involves comprehending how financial crime risks are controlled and addressed after they have been discovered by well-trained investigators. The benefit of investigating financial crime risk is the possibility of protecting the organization from substantial functional expenses and reducing unlawful hindrances for

customers (Hasham et al., 2019). Effective financial crime risk management strategies can allow firms to leverage corporate-wide risk coverage.

Several theoretical frameworks have been used to explore new financial crime risk management such as risk-based approach. For this research, I used the seminal work of Gary Becker (1968) on the economic theory of criminal behavior to explain the rationale behind financial crimes. In conducting this qualitative study, I sought to identify predicate offense classification related to the goal of economic theory of criminal behavior.

Economic Theory of Criminal Behavior

The economic theory of criminal behavior provides a deeper understanding of the driving forces behind criminal behavior. Early seminal authors including Cesare Beccaria in 1767 and Jeremy Bentham in 1789 developed several concepts later known as the economic theory of criminal behavior. The economic theory of criminal behavior implies that profit impels an individual to commit crime and the cost of the punishment prevents an individual from committing crime (Rottenberg, 1973). McCarthy (2002) suggested that people use the same principles of cost-benefit analysis to rationalize their illegal activities (see also Becker, 1968; Ehrlich, 1974; Eide, 1994; Schmidt & Witte, 1984). The neoclassical approach taken here follows McCarthy's analysis of financial crimes motivated by people’s choices, opinions towards risk, and comparisons between an illicit and legal opportunity’s availability, benefits, and costs. Early theorists of economic crime assumed that maximized self-interest is the rational factor behind a person's commission of a crime. Thus, the key ideology of the neoclassical approach is that financial crime risk

management strategies include lowering the economic benefits to financial crime or amplifying the gravity or likelihood of punishment. Incorporating the neoclassical approach in the conceptual framework supported this study's overall purpose of identifying predicate offense typologies that U.S. banking and financial services company compliance managers could use to reduce the risks of money laundering and terrorist financing activities.

Nature of the Study

A qualitative case study methodology enables researchers to gain an in-depth understanding of a specific phenomenon through participants' experiences, actions, behaviors, and perspectives (Ravitch & Carl, 2016). The focus of my RQs was on obtaining a deeper understanding of what the predicate offense typologies are to help managers reduce the risks of financial crime. The questions were helpful in exploring the identification process used by managers to reduce money laundering and terrorist financing activities. The methodology of this study was qualitative in nature; I used a descriptive case study approach to explore the identification process of predicate offense typologies that increase the risks of financial crime. O'Boyle et al. (2012) marked significant differences in the features of qualitative and quantitative research. Quantitative researchers validate theories based on statistical measures, whereas qualitative ones relate directly with the participants' experiences (Ravitch & Carl, 2016). There are five major types of qualitative research designs, namely narrative, grounded theory, phenomenology, ethnography, and case study (Burkholder et al., 2016). A case study design was appropriate for this research because I explored a modern phenomenon

within its real-life context. The other qualitative research designs were inappropriate for various reasons. The aim of phenomenology is to understand the lived experiences and perspectives of participants (Manen, 2016). Ethnography entails the study of an entire cultural group (Burkholder et al., 2016). Cresswell (2013) explained that grounded theory involves compound levels of data collection related only to participants' views, without contemplating their opinions whereas narrative research identifies the role of participants in a given situation.

For this study, a descriptive case study design was appropriate to understand and expand knowledge of opinions and reasonings related to predicate offense typologies. This perspective presumes that knowledge requires reflection, which in turn yields meaning to an individual (Manen, 2016). The source of the knowledge stems from observations made from an event, situation, or individual. A researcher who uses the descriptive design attempts to identify patterns in a shared phenomenon that transcends individual experience (Burkholder et al., 2016). In this study, I interviewed 15 compliance managers and anti-money laundering investigators who have extensive knowledge of the principles of money laundering and terrorist financing and anti-money laundering and counter terrorist financing policies and procedures. I also conducted observation and reviewed organizational documents. A case study was appropriate for this study because it allowed me to draw conclusions based on direct observations and interactions and to describe the experience of the subjects.

To identify the participants from a targeted population, I used a purposeful sampling strategy. Yin (2018) cautioned that the ability to achieve data saturation is more

important than the size of the sample. Because the sample size depends on several factors, including the RQs and the purpose of the study, Wahyuni (2012) argued that there must be at least 15 participants to have sufficient data saturation in a qualitative research study. I took samples from U.S. banking and financial services organizations to conduct semistructured interviews and observations, to collect organizational documents, and to gather information from business and finance academic journals for triangulation. Friedrich-Baasner et al. (2018) suggested that researchers can use semistructured interviews, observations, and document analysis to attain quality data that corresponds to the coding scheme and evaluates any undetermined effects. To answer the RQs and to ensure triangulation, I analyzed the data from multiple sources (interview scripts, the notes from the semistructured observations, and organizational documents); furthermore, I used multiple schemes, such as coding, thematic analysis, and content analysis, for data analysis (see Yin, 2018). For this study, I followed the steps recommended by Yin (2018), which are (a) begin by reading through all the data; (b) sort and organize the data for analysis; (c) start a comprehensive analysis, using a coding scheme, by labeling the compiled data into manageable units; (d) summarize and categorize the data into a sequence of patterns and themes; (e) interpret patterns and themes' and (f) develop a meaningful data set.

Definitions

The following common terms and operational definitions are used in this study:

Anti-money laundering: A set of laws, policies, and procedures intended to prevent financial criminals from disguising illegally generated funds as lawful income (Yeandle et al., 2005).

Counterterrorist financing: A set of policies and procedures corporations must abide by to ensure financial funds are not utilized to finance terrorist activities (Azinge, 2019).

Financial crimes: Any activity that entails illegal or fraudulent behavior for the intent of financial profit, though it could involve the unlawful transfer of property ownership (Gottschalk, 2010; Saddiq & Abu Bakar, 2019). Financial crime involves the following activities: money laundering, terrorist financing, fraud, tax evasion, embezzlement, forgery, counterfeiting, and identity theft (Gottschalk, 2010; Saddiq & Abu Bakar, 2019).

Money laundering: The illegal act of hiding the large amounts of money generated by criminal activity by concealing and disguising them as lawful and legal earnings (Nobanee & Ellili, 2018).

Predicate offense: A crime that is an element of a larger crime that generates monetary proceeds (Rusanov & Pudovochkin, 2021).

Risk management: The process of predicting and assessing business risks while identifying procedures to minimize the impact in decision-making (Hubbard, 2020).

Terrorist financing: The means that terrorists use legal or illegal funds to execute the crime of terrorism through terrorist acts in the future (Al-Suwaidi & Nobanee, 2020).

Typology: A means, tactic, strategy, process, approach, or tool criminals utilize to disguise, launder, or move illegal proceeds (Plaksiy et al., 2018).

Assumptions

Assumptions represent understandings by the researcher that certain elements of the study are true or at least plausible (Yin, 2018). Researchers will get as close as possible to the participants without crossing boundaries and allowing their personal biases to influence the outcome of the research (Golafshani, 2003; Stewart & Hitchcock, 2016). Such information can cause a flawed groundwork in a qualitative study and can affect the confirmability of the study (Shufutinsky, 2020). In this study, the first assumption was that the 15 participants would provide truthful and transparent answers to the interview questions. The second assumption was that the selected participants were adequate to generate meaningful results and that the participants were knowledgeable about predicate offense typologies for reducing the risks of money laundering and terrorist financing activities and could provide sufficient information. The third assumption was that I would be able to collect relevant data from the participants' responses; semistructured observations of anti-money laundering investigators; and applicable organizational documents such as compliance policies, procedures, and organizational reports.

Scope and Delimitations

A delimitation concerns the boundary and scope of the study. Yazan (2015) explained that a delimitation is a boundary that the researcher defines to investigate the phenomenon of interest. The scope of this study included compliance managers and anti-

money laundering investigators of U.S. banking and financial services organizations. In this study, I used a screening measure to ensure that the research participants met this delimiting characteristic. The three delimitations of this qualitative study included a strict focus on (a) U.S. banking and financial services companies, (b) compliance managers, and (c) factors that are the cause of money laundering and terrorist financing activities. For this study, I did not include compliance managers from other banking and financial institutions such as insurance companies, central banks, and credit unions. I omitted participants who were compliance officers not directly involved with anti-money laundering processes. In addition, I omitted international banking and financial services institutions. A disconnect exists between what is considered a predicate offense by the United States versus the international community (Kemsley et al., 2021; Teichmann, 2020). In the United States, companies set higher compliance standards whereas other countries are much more lenient or permissive. The comparison of money laundering in different countries is subject to various limitations (Teichmann, 2020). So, the scope of this research was limited to organizations that operate as U.S. banking and financial services organizations. Given these delimitations, my findings can potentially be used by future compliance managers to identify predicate offense typologies and can be generalized for future studies on money laundering and terrorist financing.

Limitations

Limitations are defined as matters in a study that researchers cannot control. They are weaknesses concerning the trustworthiness of the results and transferability of the conclusions (Larrinaga, 2017). In a qualitative study, transferability cannot be guaranteed

(Merriam & Tisdell, 2016). The three limitations of this study are (a) the use of qualitative data analysis, (b) potential researcher bias, and (c) limited transferability. The first limitation is the qualitative data collection method. I needed to obtain voluntary informed consent from U.S. banking and financial services institutions. The second limitation is researcher bias, which is a possibility with all research (Stewart & Hitchcock, 2017). I have investigation experience with money laundering and terrorist financing activities; however, I did not discuss my experience with any of the study participants. It is imperative for a researcher to maintain a level of objectivity and prevent personal experiences from influencing the data. In Chapter 3, I discussed other means of mitigating potential bias. The third limitation is the transferability of the findings because of the focus on a particular population. I addressed all the limitations to avoid their intrusion with the research study. Future researchers could use the study findings to expand on financial crime issues that affect modern compliance strategies.

Significance of the Study

This study is significant in that it could benefit large U.S. banking and financial services institution compliance leaders. Large U.S. banking and financial services institution compliance leaders could augment their compliance programs to build a new set of indicators or red flags to look out for when conducting their compliance obligations. As the capabilities of criminals and money laundering and terrorist financing activities evolve, compliance officers may look to update and learn more typologies by focusing on the most relevant to their products or services. Rocha-Salazar et al. (2021) indicated that anti-money laundering and counter terrorist financing typologies are risk

indicators and useful control to trigger enhanced due diligence and further monitoring. Effective mitigation approaches could diminish the societal risks related to financial crime. There is a lack of research on modern compliance strategies (Al-Suwaidi & Nobanee, 2020). In recent times, it is perilously important for banking and financial services institutions to fully comprehend the financial crime threats and take the opportunity to undergo a latest, comprehensive health-check (Crisanto & Preno, 2020). Banks and financial services institutions are encountering several critical anti-money laundering compliance challenges that impute flawed mitigation approaches (Cash, 2020). Organizations that neglect to preclude money laundering and terrorist financing activities tend to face decreasing profits, consumer discontent, huge monetary fines, loss of reputation, and decline in stock prices (Balani, 2019). The findings of this study may continue to emphasize anti-money laundering and counter terrorist financing activities for banking and financial services organizations, although practices can change to be more pragmatic to current situations.

Significance to Practice

The results of the study may indicate the benefits of modifying money laundering and terrorist financing risk mitigation approaches and develop new mitigating controls. By this means, the results of the study may transform and implement sound risk-based anti-money laundering and counter terrorist financing compliance programs and standards to minimize and regulate U.S. banking and financial services institutions' money laundering and terrorist financing exposure through practical approaches that deter money launderers and terrorists from endeavoring to infiltrate their corporations.

The results of the study may suggest enhancements in increasing transparency and closing gaps in the anti-money laundering and counter terrorist financing compliance framework (Zagaris, 2020). Corporate benefits such as improving operational efficiency and effectiveness of anti-money laundering and counter terrorist financing regulations may lower compliance costs and increase revenue for financial institutions can ensue from the study (Cash, 2020). Additionally, the study findings may increase insight for compliance managers to implement strategic changes that will stimulate long-term sustainable growth and economic value. New processes of technological advancements could sustain digital due diligence solutions to meet present and future operational risk management needs (Ekberg, 2020; Han et al., 2020). Compliance managers may understand new risks and modify operational measures to mitigate financial crime risks.

Significance to Theory

The results of this study may identify effective compliance practices that address a knowledge gap towards managing financial crime risks and contribute fundamental qualitative data to the study's conceptual framework. Notwithstanding the growing literature on the significance of money laundering and terrorist financing (Tiwari et al., 2020), there has been a failure to identify predicate offense typologies that improve and develop effective compliance regulations and requirements thus reducing financial crime risks and risky criminal behavior (Sisira Dharmasri Jayasekara, 2021). Although economic theory of criminal behavior discusses the relationship between financial crimes and benefit-cost analysis, a descriptive case study approach may meet the purpose of the study and offer distinct contributions to the theory. The descriptive case study approach

may provide findings from a consensual process that uses semistructured interviews to collect subject matter expert opinions to enlighten theoretical change and extend the results of prior studies. Applying economic theory of criminal behavior to U.S. banking and financial services institutions may provide a theoretical understanding of the problem relevant to the recent increase in financial crime risks and a lack of adequate compliance strategies and regulations (Gowhor, 2021). This may be a significant addition to the seminal works of Gary Becker (1968) neoclassical approach in playing a role in the motivation behind financial crimes.

Significance to Social Change

American society could benefit from the results of the study. The banking and financial industries ought to be prepared for the future and continue to adapt to new emerging threats, varying consumer classification, and changing environment. Banking and financial services institutions play a substantial role in the community. By changing and developing new policies and procedures, these organizations can work towards effective money laundering and terrorist financing prevention plans. Additionally, banks and financial services institutions may clarify and strengthen customer due diligence requirements to protect their organizations and reduce financial crime risks. The implications for positive social change may include the possibilities to develop new compliance strategies and strengthen existing regulatory mechanisms to help compliance managers, reduce the risk of bank failures, increase employment opportunities, and promote public awareness by educating consumer about financial crimes.

Summary and Transition

In Chapter 1, I discussed the reasoning behind this study about how the Covid-19 pandemic has led to greater risks of financial crime in the current economic environment. The challenging Covid-19 economic environment provided new opportunities for criminals to engage in money laundering, terrorist financing, and other criminal activity by the advent of government stimulus packages, escalated online banking and financial services activities, and remote working measures. The banking and financial institutions need to reassess their risk management frameworks to prevent financial crime activities. A best practice to provide a sound framework to manage financial crime risks is for U.S. banking and financial service company compliance managers to identify predicate offense typologies. Although the current literature to the date signified that there has been intensive research on the topic of financial crime risk management, there is a gap in literature that I addressed by identifying predicate offense typologies that U.S. banking and financial services company compliance managers can use to reduce the risks of money laundering and terrorist financing. To provide a deeper understanding of how compliance managers can identify predicate offense typologies and indicators to reduce the risks of money laundering and terrorist financing, I proposed a qualitative descriptive case study on U.S. banking and financial services companies that uses a holistic methodology, based on predicate offense and financial crime risks conceptual frameworks.

In Chapter 2, I will present a detailed literature review of predicate offense typologies, money laundering, and terrorist financing, starting with literature search

strategies and an integrated theoretical and conceptual framework. In financial crime research, several theories are used to explore the influential factors that drive individual decisions to commit financial crimes. In Chapter 2, I will present Becker's (1968) economic theory of criminal behavior framework. Then, I will summarize several types of literature in predicate offense typologies, money laundering, and terrorist financing.

Chapter 2: Literature Review

Introduction

The Covid-19 pandemic has infected over 235 million people globally and killed over 4.81 million people as of early October 2021 (World Health Organization, 2021). Most governments imposed public health measures that interfered with socioeconomic activities; these measures included restrictions on large gatherings, in-office work environments, and unnecessary traveling (Jamil et al., 2021). The Covid-19 pandemic has had an unprecedented impact on peoples' lives, societies, different industries, and businesses including financial crimes and regulatory compliance (Ilahi & Widowaty, 2021). Covid-19 has caused a significant global economic crisis and given rise to financial crimes, which continue to pose a threat to economic growth (Wronka, 2022). Globally, banks and financial institutions encountered a $1.15 trillion loss with a projected range of $800 billion to $2 trillion money laundered. (Kesler, 2021). The risks associated with financial crimes increased during the global pandemic as criminals and terrorists exploited the volatile economic situation.

Criminals continue to exploit the opportunities created by the pandemic across the world, with growing cases of the contractual fraud of medical supplies, investment fraud, cyber-crime scams, and corruption involving the financial stimulus measures enacted by governments (Financial Action Task Force, 2020a). The Financial Action Task Force has been monitoring these changes in criminal activity, their impact on current compliance strategies, and the actions that governments have executed to respond to diverse types of challenges presented. The Financial Action Task Force continues to gather and evaluate

information on financial crimes. This evaluation validates that the risks remain pertinent to the changes in predicate offenses and money laundering and terrorist financing activities. Since the beginning of the Covid-19 pandemic, financial crime activity has evolved. Lockdowns have caused an increase in different types of financial crime opportunities. Although it is difficult to ascertain whether financial crime activity has increased across the world because of the pandemic, the Financial Action Task Force has reported a remarkable increase in the numbers of certain types of cases. These surges seem to correlate to certain types of predicate offences because of the pandemic.

An issue is that many compliance managers of U.S. banking and financial services organizations lack awareness of predicate offense typologies and financial crime risk management strategies (Crisanto & Preno, 2020). Some scholars have theorized that there exists a level of economic theory of criminal behavior when compliance managers fail to detect financial crime foreseeability and investigate the foreseeability of financial crime acts due to ineffective compliance regulations (Arnold & Bonython, 2016). Financial institutions are unable to manage the scale and feasibility of detecting and tracking increased money laundering and terrorist financing activities (Naheem, 2019). The social problem is that large U.S. banking and financial services institutions lack modern compliance strategies to mitigate the risks of financial crime (Pol, 2020). The specific research problem is that that some U.S. banking and financial services company compliance managers fail to identify predicate offense typologies to reduce the risks of money laundering and terrorist financing activities.

The purpose of this qualitative descriptive case study was to identify predicate offense typologies that U.S. banking and financial services company compliance managers use to reduce the risks of money laundering and terrorist financing activities. Compliance managers seeking to understand predicate offense and financial crime risk concepts are challenged by financial crime motives and incentives and criminal behavior (Levi & Soudijn, 2020). In Chapter 2, I will first discuss the literature search strategy and the conceptual framework that grounded the study. These overviews will be followed by a synthesis of previous literature, an explanation of a gap in the literature, and a transition to Chapter 3.

Literature Search Strategy

A literature review is an overview of current knowledge that allows a researcher to identify relevant theories, methods, and gaps in the existing research. In the literature review for this chapter, I present an overview of topics relevant to compliance managers' effective practice towards predicate offenses and financial crime risks in U.S. banking and financial services institutions that is aligned with the RQ. To conduct a comprehensive literature search, I used multiple databases and search engines including Emerald Management; SAGE Journals Online; ProQuest Central; ProQuest Dissertations & Theses; Google Scholar; EBSCOhost; Accounting, Tax, and Banking Collection; and Taylor & Francis, as well as Walden University's Thoreau Multi-Database search tool.

I started with a broad search featuring keywords and combinations relevant to the topic of this study and added additional keywords that emerged from the searches. These keywords included *money laundering*, *terrorist financing*, *predicate offense*, *typologies*,

financial crime, financial risk, financial compliance, financial regulation, banking, bank failure, company failure, risk management, enterprise risk management, risk governance, risk assessment, anti-money laundering (AML), AML practices, AML regulation, counter terrorist financing (CTF), AML/CTF compliance programs, AML/CTF monitoring tools, Bank Secrecy Act, USA Patriot Act, mitigation, compliance, ethics, due diligence, and *compliance strategies.* Additional words and phrases included *knowledge management, change management,* and *strategic management*. To locate current literature, I searched for peer-reviewed scholarly articles published between 2017 and 2022. The keywords were searched to ensure saturation of scholarly information to ground this study.

In the literature review, I will provide more information on predicate offense, financial crime risks such as money laundering and terrorist financing, and criminal behaviors stemming from economic theory of criminal behavior. I will discuss the need for financial crime risk management practices that, if not identified and implemented, can lead to increased risks and adverse consequences for banks and financial services. The review also includes discussion of the effects of economic theory of criminal behavior and cost-benefit analysis that could incentivize financial crime behavior amongst individuals.

Conceptual Framework

The objective of this qualitative descriptive case study was to identify predicate offense typologies that U.S. banking and financial services company compliance managers use to reduce the risks of money laundering and terrorist financing activities. The concepts in the RQs, design, and method shaped the research study. To frame this

study, I used the key concepts of predicate offense and financial crime risks. The concept of predicate offense is relevant to this study, and it has broad applicability in the literature on financial crime. To fight against money laundering and terrorist financing activities, it is necessary to understand the root cause or predicate offense. Any serious offenses derived from a criminal activity constitutes a predicate offense (Kemsley et al., 2021). Any underlying criminal activity that generates illegal proceeds is a financial crime. Several underlying threats to the financial services industry are categorized as financial crime risks. The common types of financial crime risks are money laundering and terrorist financing.

Money launderers and terrorist launder illicit their proceeds to retain the benefits from criminal conduct and to support terrorism (Bhogal & Trivedi, 2019) whereas financial crime risks are driven by the role of incentives (Hashim et al., 2020). Ali (2021) addressed the commonalities among criminals of financial crimes which is derived from an afflicted personality or psychological disorder. Li (2021) explained criminals' motives and behaviors to conduct financial crimes and the parameters of crime prevention. The purpose of this qualitative descriptive case study was to identify predicate offense typologies that U.S. banking and financial services company compliance managers use to reduce the risks of money laundering and terrorist financing activities. Gary Becker's neoclassical approach paved the way for contemporary scholarship on economic theory of criminal behavior (Brandariz & González-Sánchez, 2018). The findings of this study may distinguish predicate offense typologies that U.S. banking and financial service

company compliance managers can use to reduce the risks of money laundering and terrorist financing activities.

Predicate Offenses

Recently, law enforcement agencies are focusing their efforts to close regulatory gaps by placing a particular emphasis on predicate offenses. The Financial Action Task Force, which is acknowledged as the global requirement setter for anti-money laundering efforts, has a harmonizing definition and an exhaustive list of predicate offenses. A predicate offense is described as a serious crime which is a constituent of a larger crime (Financial Action Task Force, 2020a). In a financial context, a predicate offense is a crime that generates illicit proceeds. The Financial Action Task Force continues to increase its list of predicate offenses to better exhibit the modern financial risk landscape.

During the Covid-19 pandemic, the most common types of predicate offenses to increase global financial crime risks are money laundering and terrorist financing (Financial Action Task Force, 2020c). A money laundering predicate offense is the fundamental criminal activity that engenders profits. As soon as criminals launder the profit, it ensues in the offense of money laundering. Crimes that qualify as money laundering predicate offenses are added to an ongoing list which continues to expand. Currently, the list of criminal acts systematizes 22 predicate offenses for money laundering which includes: human trafficking, migrant smuggling, sexual exploitation, narcotics trafficking, illegal arms trafficking, stole goods trafficking, corruption, murder, fraud, counterfeiting currency, counterfeit of products, environmental crime, kidnapping and taking hostage, robbery and theft, smuggling, tax crime, extortion, forgery, piracy,

cybercrime, terrorism, insider trading, market manipulation, organized crime, and racketeering (Financial Action Task Force, 2020a). The money laundering offenses continue to evolve and expand this list as the United States legislations require the application of the widest range of predicate offenses.

The description of the predicate offenses depends on two factors. First, each category of offenses must include a range of offenses (Schott, 2006). For instance, under the "robbery and theft" category, the proceeds of a vehicle theft including goods will be classified as a money laundering predicate offense. Second, according to the nature of the crime, countries have the discretion to define the offenses (Schott, 2006). Generally, it is important that the legislations criminalize the earnings from the type of conduct manifested in the above expanding list.

Financial Crime Risk

Since the last global financial crisis in modern history, it is evident that, in the financial sector, there are known financial crime risks. Although, the Covid-19 pandemic demonstrated that the financial crime risk profile of banks and financial services institutions has increased drastically. Financial crime risk is defined as a governing, reputational, or economic act or effort against financial services institutions by inner or outer mediators to embezzle, con, employ, or evade established regulations (Schott, 2006). The main types of financial crime risks are money laundering, terrorist financing, fraud, corruption, insider trading, tax evasion, counterfeiting, identity theft, and electronic crime. These crimes are executed by internal and external perpetrators including top leaders of businesses, employees, individual criminals, or organized crime groups. The

risk of financial crime can range on a spectrum of low to high. The types of behavior that fall under the low financial crime risk umbrella include personal purchases, payroll schemes, forgery, and many others. On the other hand, the highest financial crime risks include organized crime. These new and emerging risks of financial crime are impacting financial institutions in altered ways. Most institutions are exposed to greater and more imminent risks.

Globally, criminals are exploiting the Covid-19 pandemic crisis to execute their goals and operations (Hodgkinson & Andresen, 2020). Among the main types of financial crime risks, financial fraud is the greatest challenge. The predominant situation has caused an increase in fraud presenting a financial struggle for people. Thus, the prevailing conditions are motivating people to explore alternative means of earning money (Beaunoyer et al., 2020). People are adopting fraudulent behavior, including scamming, as an alternative means. Criminals found these prevailing conditions advantageous to conceal money and other financial resources (Albanese, 2021). Therefore, financial crime risk has been on the rise during the pandemic. To combat the emergence of new patterns of financial crime risks, the government needs to reassess legal regulations.

Literature Review

In this literature review, I reviewed the laws and legal regulations that mandate banks and financial services organizations to implement anti-money laundering programs which are responsible to detect and mitigate the risks of money laundering and terrorist financing. I examined the topics of money laundering and terrorist financing in greater

depth to understand the risk factors related to each financial crime. Understanding the aspects of each financial crime is necessary to comprehend predicate offense typologies. I continued with a review and synthesis of the literature on money laundering and terrorist financing typologies. I concluded the review with an analysis of Gary Becker's economic theory of criminal behavior and the neoclassical approach to criminal behavior.

Legal Regulations

The Bank Secrecy Act

The Bank Secrecy Act also known as the BSA is the law policing anti-money laundering compliance requirements. In 1970, the United States government passed the Currency and Foreign Transaction Reporting Act better known as the Bank Secrecy Act today (Sykes, 2018). Banks and financial services institutions use the terms Bank Secrecy Act and anti-money laundering collectively and reassess their compliance frameworks according to regulatory changes to adapt to newly emerging threats and fight financial crimes. The Bank Secrecy Act classifies certain individuals and corporations as high-risk through the Office of Foreign Assets Control and Specially Designated Nationals lists (Wong, 2020). The basis of the Bank Secrecy Act is to provide reporting standards for banks and financial services institutions to report suspicious activity to the Financial Crime Enforcement Network (FinCEN), central financial intelligence unit within the United States.

The suspicious activity that is documented and reporting according to the Bank Secrecy Act guidelines are accessible to law enforcement nationally and internationally (Sykes, 2018). The Bank Secrecy Act is responsible for regulating banks and financial

services institutions including loan providers, automobile lenders, and money services businesses. Sykes (2018) indicated that the aim of the Bank Secrecy Act was to locate the origin and movement of money derived from crime such as drugs during the era of the War on Drugs. Since 1970, other acts including the Money Laundering Control Act of 1986, which warranted all banking institutions in the United States establish anti-money laundering programs, and the Money Laundering Suppression Act, which specified the power of the U.S. Treasury, were passed which reinforced the Bank Secrecy Act.

Furthermore, in 1996, the Bank Secrecy Act instituted explicit policies and procedures including the responsibility to file Suspicious Activity Reports (SARs) for any transactions aggregating $5,000.00 or more and designed requirements for Currency Transaction Reports (CTR) and Monetary Instrument Logs. Banks and financial institutions are required to file a CTR for transactions over $10,000.00. Fletcher et al. (2021) stated that any financial transaction that may entail probable money laundering, questionable terrorist financing activities, or violate the Bank Secrecy Act must file an SAR with a law enforcement agency. The financial sector is responsible for gathering personal identifiable information about a customer including their name, address, social security number, taxpayer information, resident status, and date of birth (Fletcher et al., 2021). Finally in 2001, after the terrorist attacks on the United States soil, Congress passed the USA Patriot Act.

The USA Patriot Act

The USA Patriot Act was passed in 2001 by Congress. The USA Patriot Act stands for the Uniting and Strengthening America by Providing Appropriate Tools

Required to Intercept and Obstruct Terrorism (Rajah, 2019). The USA Patriot Act has contributed to implementing anti-money laundering rules and regulations globally by augmenting compliance requirements for all banks and financial services institutions through the Federal Financial Institutions Examination Council (FFIEC). The Federal Financial Institutions Examination Council is an organization responsible for the anti-money laundering and Bank Secrecy Act guidelines which helps banks and financial services institutions to comprehend the laws and guidelines (Rajah, 2019). The FFIEC provide the U.S. Treasury with power to impose exclusive actions against organizations and jurisdictions that are high-risk and pose money laundering apprehensions. In turn, the U.S. Department of Treasury has become a powerful agency with the ability to drive the global market. The Bank Secrecy Act along with the USA Patriot Act have created a new language and use in the form of traditional anti-money laundering compliance frameworks. Subsequently, both acts were established prior to the Covid-19 pandemic, and ought to be reassessed with new threats and predicate offense typologies emerging in the modern market worldwide.

The Anti-Money Laundering Act of 2020

The National Defense Authorization Act was passed as a bill by Congress which includes the Anti-Money Laundering Act of 2020. Since the USA Patriot Act in 2001, the Anti-Money Laundering Act of 2020 is the first amendment of the United States anti-money laundering regulation. Galeazzi et al. (2021) stated that the overarching objective of the Anti-Money Laundering Act of 2020 is to modernize anti-money laundering and counter-financing of terrorism laws. This act focuses on enhancing communication

among government and industry shareholders by accentuating the significance of risk-based anti-money laundering/counter-financing of terrorism programs. The enhanced changes in the Anti-Money Laundering Act of 2020 include increased whistleblower protection, new consequences for specific Bank Secrecy Act breaches, and two additional committees to the Bank Secrecy Act Advisory Group (Galeazzi et al., 2021).

Furthermore, an eminent change resulting from the Anti-Money Laundering Act of 2020 is reform of the Customer Due Diligence Rule. This change focuses on developing aligned requirements for beneficial ownership and instituting a database at the Financial Crime Enforcement Network to collect beneficial ownership information of legal entity customers. A database at the Financial Crime Enforcement Network will eliminate duplication and unwarranted obligations for banks, financial services institutions, and legal entity customers. Galeazzi et al. (2021) indicated that the Anti-Money Laundering Act of 2020 revokes the entire Customer Due Diligence Rule but necessitates for banks and financial institutions to implement written policies and procedures to detect and confirm the beneficial owners of their legal entity customers. The revision to the Customer Due Diligence Rule appears to be vague and perhaps future regulations will outline detailed requirements. Banks and financial institutions should consider taking a conservative approach by following the current policies and procedures in place under the Bank Secrecy Act.

The Anti-Money Laundering Act of 2020 seeks to develop the financial system by improving communication among shareholders and reforming the anti-money laundering/counter-financing of terrorism laws. The changes introduced in this act is to

simplify compliance responsibilities by providing government and law enforcement agencies with vital data. The Financial Crime Enforcement Network offers intensive guidance for banks and financial institutions to better diversify anti-money laundering/counter-financing of terrorism resources (Galeazzi et al., 2021). Although, certain ambiguity persists for banks and financial institutions concerning the Customer Due Diligence Rule changes. Nevertheless, future laws may address the ambiguity. The predominant effect of the Anti-Money Laundering Act of 2020 ought to reduce the risk of criminals within the United States financial system while evaluating the interests of involved parties subject to compliance requirements.

Money Laundering

Money laundering comprises of practices that support the conversion process of illegal funds of crime into legal proceeds (Al-Suwaidi & Nobanee, 2020). Money laundering is classified as a financial crime which may be embedded in organized criminal activity including robbery, extortion, embezzlement, fraud, human trafficking, and several others. Organized crime activities incorporate a sequence of intricate transactions which operate through financial institutions nationally or internationally. Money laundering is a practice where illegal proceeds enter financial institutions concealed as lawful transactions. Money laundering entails a three-step process to launder the funds: (a) placement, (b) layering, and (c) integration (Al-Suwaidi & Nobanee, 2020).

The first step is known as placement. Placement is the process where the money launderer deposits the illegal funds into the financial system. The second step is known as

layering. Layering is the process where experts generate several business channels such as companies, trusts, and foundations for implementation as liaisons for financial transactions to disguise illicit source of the funds. The third step is known as integration, the final step in the money laundering process. Integration is the process where liaisons use the illegal funds as lawful financial transactions without exposure. When illegal funds are integrated into lawful financial transactions, it is difficult for financial institutions to detect the criminal proceeds (Amjad et al., 2021). To detect illegal proceeds, employees of banking and financial services institutions need to follow policies and procedures to document all the transactions posted to the customer accounts by creating an audit trail. The detection process is a crucial element to an effective anti-money laundering and counter terrorist financing program.

The Financial Action Task Force (2020c) indicated that money laundering is one of the greatest challenges facing the global economy amid a worldwide pandemic. The methods used for money laundering are constantly evolving. Criminals are introducing alternative money laundering scams and ploys which adversely are affecting the global economy by distorting the financial data of domestic economies (Basit, 2020). Banks and financial institutions are classifying money laundering as a global threat to the financial system. The alternative channels to launder the funds of criminal activities has become a facilitated serious and organized crime to invade and undermine the integrity of the financial system. The criminals who are conducting money laundering activities target several victims within the financial institutions.

Money lauders can be an individual or groups of people. A stereotype for a money lauder does not exist. Money launderers have connections to criminal organizations who infiltrate financial systems with large amounts of money that require legitimization. Financial institutions around the world face the challenge of identifying a money launderer. These types of criminals represent a diverse group of people across race, education, profession, and social status which can be terrorists or terrorist organizations or experts in the financial industry. Although, money laundering activities attract large sums of money that require filtering into the banking system in a way to avoid detection. During the pandemic, an increase in cryptocurrencies as a form of payment has created a channel for money launderers (Kolachala et al., 2021). Cryptocurrency such as bitcoin create anonymity which conceal money laundering transactions and facilitate the funds. Banks and financing institutions face the challenge of monitoring and regulating financial transactions regularly to reduce the risk of money laundering.

Banks and financial institutions are faced with an increased risk of money laundering causing a difficulty to monitor legitimate clients while mitigating the risk from money launderers. Different size enterprises are exposed to money laundering especially small businesses. Small businesses operate primarily on a cash basis and the enticement to elude taxes can tempt small business owners into conducting money laundering activities (Korystin et al., 2020). For example, small business owners may conduct money laundering by depositing small unnoticeable amounts of legitimate cash mixed with illegally earned cash into bank accounts. Small-sized enterprises are ideal

businesses to conduct money laundering activities including structured check deposits. In other words, launderers deposit money orders or managers' checks into various bank accounts at different locations (Woodson, 2019). By using the deposited funds to acquire assets including real estate, jewelry, or investments, launderers erase the audit trail which could lead to the criminal. Money launderers discover new platforms to launder funds including the established channels including money transfers, banks, start-up businesses, and real estate purchases. The Financial Action Task Force (FAFT) standards have discovered that money laundering and terrorist financing are on opposing extremities of a continuum.

Terrorist Financing

Terrorist financing is a criminal offence different than money laundering and preparatory in nature. Unlike money laundering, terrorist financing activities derive from lawful and unlawful sources to fund the crime of terrorism in the future. Terrorists demonstrate a sense of adaptability and opportunism to achieve their funding requirements. Terrorists need monetary resources to purchase weapons and cover operational expenses including employment, training, communication tools, salaries, compensation, travel, logistics, and shared funding. Terrorists or terrorist organizations attempt to disguise the funding and nature of the subsidized activity.

Terrorist financing originates from legitimate sources with large lawful financial resources. To support their crime of terrorism, terrorist raise funding by abusing charitable entities, legitimate businesses, or self-financing (Al-Suwaidi & Nobanee, 2020). The mechanisms to finance terrorism include an exchange of economically

profitable incentives derived from criminal activities. Terrorists tend to trade contraband cigarettes, counterfeit goods, organized fraud, narcotics smuggling, and illicit drugs for monetary funds (Al-Suwaidi & Nobanee, 2020). Terrorists commission crime of terrorism through closed networks and ambiguous industries.

Traditionally, terrorists utilize different methods to permit them to launder their acquired assets. They move funds through nontransparent markets, remittance systems such as hawala, underground banking systems, charities, and between organizations. Terrorists move physical funds such as cash by couriers. To mitigate detection risk, terrorists adapt all the methods that exist to move money globally.

The primary objective of combating terrorist financing activities is to prevent future acts of terrorism from interrupting global societies. Some methods of combating terrorist financing activities include interrupting funding flows which lead to a hostile environment for terrorism (Fletcher et al., 2021). Moreover, hostile environments hinder the capabilities of terrorists to execute crimes of terrorism. Fletcher et al. (2021) indicated that interrupting terrorist financing requires universal defenses which shield the financial system from criminal abuse, and steer financial sanctions guided by counter-terrorism intelligence. Banks and financial institutions face the challenges of identifying terrorist financing activities because this criminal offense uses modest amounts of funds. Since terrorist financing uses low levels of funding, terrorist financing transactions tend to be mistaken for ordinary business activities by experts in the field of anti-money laundering (Financial Action Task Force, 2016).

The Bank Secrecy Act provides antiterrorism standards and recommendations for banking and financial institutions to implement through anti-money laundering/counter-financing of terrorism programs. Regulatory and law enforcement agencies require banks and financial institutions to strengthen their compliance framework to include antiterrorism provisions. A fundamental element in anti-money laundering/counter-financing of terrorism compliance program is the anti-money laundering/counter-financing of terrorism monitoring tool and processes. The monitoring tool and processes detect and secede money laundering and terrorist financing risks in customer transactions (Helmy et al., 2016). Banks and financial institutions can utilize monitoring tools to recognize criminal funds. Compliance managers governing customer transactions utilize monitoring tools to detect suspicious transactions resulting from or indicative of the presence of money laundering and or terrorist financing activities.

Money Laundering and Terrorist Financing Typologies

A fundamental understanding of how money laundering and terrorist financing transpires is necessary to effectively mitigate financial crime risks and ensure regulatory compliance. A principal skill for any compliance managers is the ability to recognize typologies. Money laundering and terrorist financing typologies illustrate the innumerable mediums, tactics, strategies, practices, schemes, and mechanisms criminals use to disguise, lauder, or move illegitimate proceeds. Typologies are a set of indicators or red flags to pay attention to when banks and financial services institutions perform their compliance duties (Plaksiy et al., 2018). The financial industry must continuously learn to recognize money laundering and terrorist financing typologies. Money

laundering and terrorist financing typologies and criminal capabilities are evolving parallelly. Typologies lead to reasonable doubt of criminal activity which can lead to heightened due diligence and additional monitoring.

Money Laundering Typologies

Money laundering typologies are techniques used to launder money. Criminals adopt creative techniques to launder money. Money laundering typologies are strongly guided by the economy, financial systems, and anti-money laundering regulations (Gilmour, 2021). Banks, financial institutions, and law enforcement agencies fighting against money laundering depend on the most recent information on typologies. The Financial Action Task Force annually conducts and observes case analysis on specific subject areas to collect current information. Based on their findings, the Financial Action Task Force articulate the trends in order to adapt recommendations to address money laundering risks. The Financial Action Task Force classified the following examples as money laundering typologies (Financial Action Task Force, 2020a): unusual customer behavior, usage of large amounts of cash, smurfing, unusual insurance claims, corruption, currency exchanges, purchase of valuable assets, unusual wire transfers, and many others.

Unusual Customer Behavior. Money laundering risks involve a great deal of customer behavior. The general apprehension is unexplained movement of incoming or outgoing funds with the customer's account history or profile. By tracking customer behavior, banks, financial institutions, and law enforcement agencies can recognize any signs of money laundering. To detect signs of money laundering activity, banks and financial organizations invest and employ advanced technologies including the Anti-

Money Laundering solution. Shaikh and Nazir (2020) revealed that the Anti-Money Laundering solution is a commonly used software system that helps banks and financial organizations identify any suspicious transactions and or unusual customer activities.

The Anti-Money Laundering solution is a rule-based system in which specific rules on transactions regulate the hard codes based on the input from compliance officers and anti-money laundering investigators (Shaikh & Nazir, 2020). The hard codes trigger alerts within the system when suspicious transactions or unusual customer behavior occurs. The indicators of unusual customer behavior include inconsistent transaction with the customer's profile, multiple accounts under multiple names, high volume of transactions within a short period, checks issued to a family member(s) living only a few miles apart (Financial Action Task Force, 2020a). Unusual customer behavior is a variable which can spot suspicious activity hard to identify.

Banks and financial institutions must mandate compliance policies and procedures to detect and identify any suspicious transactions to law enforcement agencies to counteract possible money laundering activities. The Anti-Money Laundering solution utilize preset rules to detect unusual transactions activities based on historical customer transactions information (Shaikh & Nazir, 2020). Historical customer transaction data indicates transaction patterns related to the nature of the transactions, transaction thresholds, and transaction frequency to check for money laundering activity (Gyamfi & Abdulai, 2018). The unusual customer behavior is detected based on irregular patterns. The current anti-money laundering solutions used by banks and financial organizations can detect suspicious customers and irregular transactions based on preset rules. So, the

anti-money laundering solutions are tailored to individual customers' transactional history which is stored on banks and financial institutions' databases to efficiently identify abnormal and suspicious transactions.

Usage of Large Amounts of Cash. The expenditure of large amounts of cash is a red flag in the realm of money laundering. The overall concern is large cash deposits from unknown sources and large cash withdrawals for unexplained usage. Due to the large amounts of cash transaction daily, banks and financial services institutions constantly face the challenge of detecting suspicious activity with tangible evidence. Singh and Best (2019) suggested that suspicious financial transaction may be discovered by restricting consumer thresholds. Certain transactions surpassing preset thresholds necessitate compliance investigation. An unfavorable outcome is that money launderers change their behavior to prevent this control.

A money laundering indicator is a customer conducting large cash deposits or withdrawals. If a customer's nature of business primarily transacts with cash, the usage of large amounts is classified as suspicious activity. Some red flags indicatives of the use of large amounts of cash include large cash deposits or withdrawals, large cash deposits utilized for investment, large amounts of currency exchange, large amounts of cash from unknown sources, and many others (Financial Action Task Force, 2020a). The Financial Action Task Force recommended banks and financial institutions to file detailed reports indicative of suspicious activities or large cash transactions with financial intelligence units (Singh & Best, 2019). Banks and financial institutions are obligated to file suspicious activity reports (SARs), currency transaction reports (CTRs), and cash and

monetary instruments reports (CMIRs) for unusual financial activity involving large amounts of cash transactions above a preset threshold. These reports act as audit trails to capture limited footprints of many money laundering activities.

Smurfing. Smurfing also known as structuring is an indicator of money laundering activities. Smurfing is a money laundering typology that commonly occurs during the three different stages of money laundering: placement, layering, and integration. Criminals who are smurfing funds through financial institutions are known as smurfs. It is a technique which involves numerous high volumes of small transactions including deposits, withdrawals, and transfers through different accounts (Financial Action Task Force, 2020a). For example, multiple cash deposits on the same day at different branch locations to avoid detection. The inherent risk of this money laundering typology poses is that criminals use smurfing to evade threshold reporting requirements.

To evade threshold reporting requirements, smurfs conceal transaction amounts, source, and target account (Whisker & Lokanan, 2019). Smurfing is related to fraud with the purpose of avoiding detection. By conducting multiple small value transactions, smurfs can place, layer, and integrate large amounts of illicit proceeds into the modern financial system. Since the low value of a single transaction becomes compliant with legal reporting limits, smurfs avoid detection and use illicit proceeds to fund terrorist activities (Whisker & Lokanan, 2019). Smurfing is a typology which continues to be a challenge for financial intelligence units. The process to uncover the money trail raises privacy issues. To counteract the enhanced detection, smurfs continue to lower the values of deposits, withdrawals, and transfers of funds. To identify smurfing activities, banks

and financial institutions need to invest in data-driven anti-money laundering tools and systems.

Unusual Insurance Claims. The unusual claim of insurance is classified as a money laundering typology. In this case, criminals use insurance policies to integrate illicit proceeds into the financial system. Some red flags of unusual insurance claims are when individuals cash out insurance policies in a different location than the jurisdiction of purchase, purchase an insurance policy with large amounts of cash, make regular claims on payments less than the premium, and purchase an insurance policy and immediately surrender it (Financial Action Task Force, 2020a). The underlying financial crime risk is that insurance claims are exploited to obscure the profits of crime.

Corruption. Corruption is the outcome of poverty, greed, unemployment, and vulnerable institutions and legislations (Bahoo, 2020). It is identified as a money laundering typology which involves the act of bribing officials. Corruption is a method used to enable money laundering by challenging anti-money laundering and counter-financing of terrorism processes with the influence of a politically exposed persons (Financial Action Task Force, 2020a). Criminals target politically exposed persons with a lack of morality or who are easily bribed or persuaded to permit money laundering activities to take place. Corrupt business leaders and government officials enable criminals to conceal and launder their illicit proceeds. Historically, banks with weak corporate governance, lack of transparency and due diligence, incapable bank leadership, and engagement in corrupt activities has caused the insolvency of financial institutions including Bear Stearns, Lehman Brothers, Enron Corporation, and many others (Bahoo,

2020). Different determinants influence corruption amongst banks and financial institutions.

Corruption is driven by several types of factors. The distinctive determinants of corruption are cultural and legal differences. The understanding of bribery is different across different jurisdictions worldwide. Each country has its own definition of corruption and bribery. Cultural differences tend to cause confusion amongst bank employees who may commit a violation by giving high-value, extravagant gifts to foreign officials in the process of building a professional relationship. Though it is challenging to detect each corruption activity that passes through banks and financial institutions, strong anti-money laundering programs with built-in key risk indicators or red flags will ensure detection.

Banks and financial institutions must adhere to anti-money laundering regulations which are in place to detect, identify, and report corruption. To counteract corruption in banks and financial institutions, law enforcement agencies have introduced anti-corruption laws. The United States has initiated and articulated domestic-level laws against corruption and bribery (Bahoo, 2020). Amongst many laws, the Foreign Corrupt Practices Act has been passed to avert financial crime such as corruption (Meinert, 2019). By eliminating corruption, banks and financial institutions will effectively reduce money laundering.

Terrorist Financing Typologies

Terrorist financing typologies demonstrate the techniques and trends used to transfer funds amongst organizations to finance crimes of terrorism (Financial Crimes

Enforcement Network, 2021). Anti-money laundering and counter-financing of terrorism organizations use the list of typologies provided by the Financial Action Task Force in their efforts to fight against and mitigate the risk of terrorist financing. The typologies specific to terrorist financing are the abuse of non-profit organizations, new payment technologies, and virtual assets.

Abuse of Nonprofit Organizations. The Financial Action Task Force has identified the abuse of non-profit organizations as a terrorist financing typology. Terrorists use non-profit organizations to raise and conceal terrorist funds. Non-profit organizations disguise terrorist finances allowing terrorist to source, move, and execute terrorist acts across any jurisdiction (Financial Action Task Force, 2020a). The financial crime risk of abusing non-profit organizations is the lack of detection within and between financial institutions increasing the risk of terrorist acts.

New Payment Technologies. Technology is advancing and providing terrorist with new techniques and trends to source and move funds to execute acts of terrorism. Emerging payment technologies such as cell phone-based remittance and payment systems or online banking have become platforms for terrorist organizations to hack and use for their purposes (Financial Action Task Force, 2020d). The central financial crime risk related to new payment technologies is the global accessibility of these systems and the ability to retrieve unlawful money without a possible audit trail to its source.

Virtual Assets. As money laundering and terrorist financing activities develop and change, regulatory gaps in anti-money laundering and counter financing of terrorism frameworks continue to exist. Moreover, a lack of regulation and knowledge of virtual

asset service-providers allows terrorists to exploit compliance and governing gaps and fund terrorist activities. A high-risk virtual asset is cryptocurrency which has become popular during the Covid-19 pandemic. It is a growing threat to the anti-money laundering regulatory system (Haq et al., 2021). Cryptocurrency is a medium of digital currency payment infrastructure that operates on a computer network (Ibrahim, 2019). Cryptocurrency is highly susceptible to money laundering, efficiently unregulated, and criminal in nature.

Criminals, both individuals and entities, are increasingly abusing this virtual asset by engaging in illegal crypto trade and other illicit use of cryptocurrencies. Cryptocurrency provides an element of ambiguity and allows criminals to cover their logistical and financial tracks. Additionally, the use of this digital means allows criminals to conduct offline transactions increasing the challenges for law enforcement agencies to trace illicit transactions. To conduct these illicit transactions, criminals are using the dark web or net which is a network of encrypted websites (Ibrahim, 2019). Prior to cryptocurrency, global crime syndicates trusted the hawala system as a technique to launder illicit funds through financial transactions worldwide. As criminals continue to push the envelope and execute high-risk activities, cryptocurrency has become a viable option and ideal replacement for the hawala systems. Cryptocurrency is used to implement several illegal activities including human trafficking, drug dealings, and corruption.

The growing trend in cryptocurrency has forced the Financial Action Task Force and law enforcement agencies in foreign countries to reevaluate their anti-money

laundering and counter terrorist financing regulations and legislations. The legal discrepancies across jurisdictions in terms of the cryptocurrency is causing gaps in compliance frameworks amongst banks and financial institutions (Ibrahim, 2019). Countries must adopt new regulations which address risks of cryptocurrency. By taking proactive initiatives, financial intelligence units can detect and mitigate the risks of money laundering and terrorist financing activities.

Economic globalization has increased opportunities for trade, investment, and movement of labor and capital across state borders. Modernization of telecommunication, banking, and financial systems, criminals find it easy to move people, money, or goods across state borders compared to historical data. Criminals are establishing businesses to expand their illicit activities. They use different typologies to obtain access to new markets by subsidizing the inconsistencies among the legislatures of countries in different areas of the world. Today, criminals and organized crime groups are adaptable, innovative, cunning, and engaged in illegal and legal activity. Criminals are known to apply criminal strategies and behavior by using typologies to succeed in their legal or illegal business mission and vision.

The Economic Theory of Criminal Behavior

The question of whether an opportunity leads an individual to conduct predicate offenses is intriguing. To understand the reasoning behind predicate offenses, it is necessary to dive deeper into the economic theory of criminal behavior. Earlier literature explains that the economic theory of criminal behavior perceives a criminal act as a logical choice (Becker, 1968; Ehrlich, 1973; Posner, 1985). Criminals conduct a crime

whensoever the estimated benefits exceed the costs. According to the economic theory of criminal behavior, a cost-benefit ratio is a driving factor which determines the margin for any crime (Brabenec & Montag, 2018). In economics, the economic theory of criminal behavior is commonly acknowledged as a framework for examining illegal activity. This theory rationalizes the phenomenon that deteriorated financial markets will lead individuals towards illegal activities. Financial market crises are often associated with increases in crime.

The basis of the economic theory of criminal behavior is developed by two prominent stages. First, an individual offender's decision-making process to commit a crime (Miceli, 2017). In the decision-making process, crime offenders compare the benefits of conducting a criminal act to the anticipated punishment. Offenders calculate the provision of offenses which policy makers use to establish the collectively ideal penalty. The economic approach consists of selecting the likelihood of crime and the penalty on conviction to amplify a social welfare act. The social welfare act depends on (a) the cost of arrest, (b) the cost of the crime to society, and (c) the cost of penalty (Miceli, 2017). Theories about the elements of the predicate offenses differ from an emphasis on criminal behavior.

Essentially, all the different theories agree that though the variables are constant, an increase in a person's likelihood of sentence or penalty would largely decrease based on the number of predicate offenses (Miceli, 2017). Additionally, this theory supports the idea that a change in the probability has a greater effect on the number of predicate offenses than a change in the punishment. Theorists have asserted that an individual

executes a predicate offense if the expected benefit exceeds the benefit they may gain by utilizing resources and time on other activities (Miceli, 2017). An individual engages in criminal behavior based on a cost-benefit analysis. The underlying inference of this theory is relative to the number of predicate offenses by an individual to their likelihood of sentence, punishment, proceeds from legal or illegal activities, the regularity of irritant detentions, and an individual's motivation to perpetrate a criminal act.

The economic theory of criminal behavior has an appealing explanation of a larger retort to change than reprimand. An increase in punishment, if there is no change in the predicted proceeds from a predicate offense, could change the anticipated benefit since the risk level would change (Becker, 1968; Miceli, 2017). It is undoubtedly demonstrated that an increase in punishment would reduce the anticipated benefit, and hence the number of predicate offenses decreases. Typically, according to historical criminal behavior, criminals are more dissuaded by the possibility of conviction than by the punishment. Society has conceived inventive punishments for convicted criminals including death, torture, branding, fines, imprisonment, restriction on movement, loss of citizenship, and many others (Becker, 1968; Miceli, 2017). In the United States, low risk predicate offenses are penalized by fines, probation, or imprisonment. Perpetrators who commit other less serious predicate offenses face minor constraints such as temporary suspension of a person's driver's license (Becker, 1968; Miceli, 2017). The high-risk predicate offenses face severe punishment including a combination of parole, imprisonment, fines, occupational restrictions, and many more.

Criminals analyze the cost of different punishments by examining them according to monetary worth, measured in terms of fines (Becker, 1968; Miceli, 2017). For instance, the cost of an imprisonment is the value of profits relinquished and constraints on freedom. Subsequently, the value of profits relinquished and constraints on freedom differ between each person, so the cost of imprisonment for a given period is different but typically greater. A criminal who can earn more outside of prison will conduct a cost-benefit analysis. In essence, the criminal behavior of economics epitomizes to the cost versus benefit of executing a predicate offense. Does the benefit of committing a predicate offense outweigh its cost? The choice of committing a predicate offense relies heavily on punishments which ultimately affects the criminal and society. Thus, the neoclassical approach supports the notion that choice is the driving force among criminals.

The Neoclassical Approach to Criminal Behavior

The foundation for the neoclassical approach is the notion of utility as the guiding factor in the choice of criminals. The rationale is based on one's capability to maximize utility (Klimczak et al., 2021). Criminals are described as reasonable utility maximizers in terms of financial crime risk. The neoclassical approach considers the impact of intrinsic and extrinsic interventions on behavior. Becker (1968) evaluated criminal behavior in accordance with motivation and punishment. Financial institutions should consider intrinsic and extrinsic motivation in their compliance frameworks. Intrinsic and extrinsic motivation signify objectives that guide criminal behavior. The social nature of

criminals may benefit others implicitly and secondarily. Criminal's decision-making processes may be influenced by different types of motivation.

Many studies have confirmed the organizational benefits of intrinsic and extrinsic motivations. Intrinsic motivation creates a perception of independence and expertise. It largely promotes innovation performance (Li et al., 2015). In addition, extrinsic motivation enriches well-being, performance, and productivity. Extrinsic motivation allows criminals to foresee higher profitability and satisfaction with lower costs. Criminal actors could be motivated to commit a high-risk predicate offense, while pursuing to earn proceeds for themselves (Klimczak et al., 2021). It is important to assess the correlation between extrinsic and intrinsic motivations. Despite situational difference, it appears that extrinsic rewards distort intrinsic motivations. Thus, the neoclassical economic approach of the self-interested and extrinsically motivated criminal actor offers a very limited account of actual behaviors.

The neoclassical approach and its broadening perspective into law imposes a limited effectiveness of prevention measures (Klimczak et al., 2021). To enhance the legislations, law enforcement agencies need to exclusively examine intrinsic and extrinsic motivations driving criminal behavior. The probability of conviction and punishment will demotivate predicate offenses and increase social welfare. Social welfare measured by legislative effectiveness will decrease predicate offenses by demotivating criminal behavior. In the current legislation framework in the United States demonstrates devastatingly positive illicit financial activities. By reassessing the legislative framework, the government and law enforcement agencies will provide eminent guidelines for U.S.

banking and financial service company compliance managers to identify predicate offenses and reduce the risks of money laundering and terrorist financing activities.

Summary and Conclusions

As suggested by the key concepts reviewed in this literature review, predicate offenses are evolving as prevailing conditions of society change. A major global challenge in recent times is the Covid-19 pandemic crisis which has increased financial crime risks worldwide. Understanding the different types of predicate offenses and typologies portrays a holistic process of how criminals launder money or finance terrorist acts. A review of the existing literature demonstrated intensive research on the topic of financial crime but there is a gap in the current legislative and financial risk management framework. The legislative and financial risk management framework detects economic uncertainties and risk factors requiring a reevaluation of financial crime risk measurement methodologies to mitigate the risk consequences of money laundering and terrorist financing activities. A best practice to provide a sound framework to manage financial crime risks is for U.S. banking and financial service company compliance managers to identify predicate offense typologies. To provide a deeper understanding of how compliance managers can identify predicate offense typologies and indicators to reduce the risks of money laundering and terrorist financing, it is necessary to understand the seminal work of Gary Becker on the economic theory of criminal behavior which leads to the neoclassical approach. A comprehensive insight into the driving forces behind criminal behavior is crucial to develop effective financial crime risk management strategies.

The reasoning behind this study was to illustrate how the Covid-19 pandemic has led to greater risks of financial crime in the current economic environment. The challenging Covid-19 economic environment provided new opportunities for criminals to engage in money laundering, terrorist financing, and other criminal activity by the advent of government stimulus packages, escalated online banking and financial services activities, and remote working measures. In Chapter 3, I will discuss the methodology and research design and rationale. The methodology for this study was qualitative descriptive case study which may provide a deeper understanding of how identifying predicate offenses can help compliance managers reduce the risks of money laundering and terrorist financing activities. Furthermore, I will discuss in greater detail the rationale behind participant selection, instrumentation, and the procedures relating to recruitment, participation, and data collection. Also, I will discuss the data analysis plan and illustrate the validity of this study.

Chapter 3: Research Method

Introduction

The purpose of this qualitative descriptive case study was to identify predicate offense typologies that U.S. banking and financial services company compliance managers use to reduce the risks of money laundering and terrorist financing activities. The Covid-19 pandemic has led to greater risks of financial crime in the current economic environment. The challenging Covid-19 economic environment provided new opportunities for criminals to engage in money laundering, terrorist financing, and other criminal activity due to the advent of government stimulus packages, escalated online banking and financial services activities, and remote working measures (Olofinbiyi, 2022). Leaders of banking and financial institutions need to reassess their risk management frameworks to prevent financial crime activities. A best practice to provide a sound framework to manage financial crime risks is for U.S. banking and financial service company compliance managers to identify predicate offense typologies (Al-Suwaidi & Nobanee, 2020).

Although there has been intensive research on the topic of financial crime risk management (Ekberg, 2020; Goldbarsht & de Koker, 2022; Kerusauskaite, 2022), there is a gap in the literature on predicate offense typologies that U.S. banking and financial services company compliance managers can use to reduce the risks of money laundering and terrorist financing. To provide a deeper understanding of how compliance managers can identify predicate offense typologies and indicators to reduce the risks of money laundering and terrorist financing, I conducted a qualitative descriptive case study on

U.S. banking and financial services companies that uses a holistic methodology, based on predicate offense and financial crime risks conceptual frameworks. I selected a group of experts to provide details on predicate offense typologies that can reduce the risks of money laundering and terrorists financing activities. The descriptive case study is an approach that is used to identify patterns in a shared phenomenon that transcends individual experience (Burkholder et al., 2016). The insights that emerge may inform compliance managers about strategic changes they can implement to stimulate long-term sustainable growth and economic value.

In this chapter, I will present comprehensive information on the research method and rationale for using a descriptive case study approach to meet the purpose of the study and provide data to answer the overarching RQ. Also, I will present a rationale for the process of selecting the participants and an overview of the data collection and analysis strategies. Additional information included in this chapter include discussion of the role of the researcher, issues of trustworthiness, and ethical procedures. Chapter 3 concludes with a summary section.

Research Design and Rationale

By using qualitative research methodology, researchers are able to gain an in-depth understanding of a specific phenomenon through participants' experiences, actions, behaviors, and perspectives (Ravitch & Carl, 2016). In conducting this study, I focused on obtaining a deeper understanding of predicate offense typologies that help compliance managers lower the risks of money financial crime. I crafted the study's overarching RQ to explore how identifying predicate offense typologies may help compliance managers

to reduce money laundering and terrorist financing activities. The methodology of this study was qualitative in nature; I used a descriptive case study approach to explore the identification process of predicate offense typologies that increase the risks of money laundering and terrorist financing activities. O'Boyle et al. (2012) noted significant differences in the features of qualitative and quantitative research. The quantitative methodology validates theories based on statistical measures whereas the qualitative methodology relates directly with the participants' experiences (Ravitch & Carl, 2016). The use of a case study design generated valuable results.

Research Design

There are five major types of qualitative research designs: narrative, grounded theory, phenomenology, ethnography, and case study (Burkholder et al., 2016). The phenomenological design centers on a description of the events and experiences of participants by observing people, situations, and experiences (Manen, 2016). A phenomenological researcher focuses on understanding the lived experiences and perspectives of participants to derive the universal meaning of those experiences. This means exploring factors that affect the population from which the participants or cases were drawn (Manen, 2016). The challenge with a phenomenological approach is that the findings are contingent on the capability of the participants to remember and convey events. The design was not appropriate for this study because the study did not entail an examination of the lived experiences of participants.

Additionally, the ethnographic design was not appropriate for this study. This design entails the study, over a specific period, of a group of people or an entire cultural

group who share similar beliefs and behavior (Weis & Fine, 2012). This design was not appropriate because the objective of this research study was not to explore a culture or group. The grounded theory design involves compound levels of data collection related only to participants' views, without contemplating their opinions to develop a theory (Kolb, 2012). The aim of this study was not theory development but rather the identification of predicate offense typologies to help compliance managers reduce the risks of money laundering and terrorist financing activities. As such, I opted against the use of a grounded theory approach. Last, the aim of the narrative design is to collect data from stories articulated by the participants (Converse, 2012). The study did not center on stories, but the analysis of a problem faced by compliance managers. The narrative design was therefore inappropriate for the study.

A case study design was appropriate for this research because it involves exploration of a modern phenomenon within its real-life context. A case study researcher develops a comprehensive analysis of a program, an event, a case, or multiple cases. Also, the case study design allows for the use of different data sources (Yin, 2018). It was the most suitable approach for this study. The other qualitative research designs were not suitable because a comprehensive understanding was essential to identify predicate offense typologies that U.S. banking and financial services company compliance managers may use to reduce the risks of money laundering and terrorist financing activities.

Research Rationale

Use of the descriptive case study design allows the researcher to collect knowledge that yields meaning to an individual (Manen, 2016). The source of the knowledge stems from observations that an individual makes about an event or situation. The case study design consists of five steps, according to Yin (2018): stating the RQ, developing plans, distinguishing the unit of analysis, connecting data to plans, and explaining the findings. In using the descriptive case study design, I sought to explore and expand knowledge of opinions and reasonings related to predicate offense typologies.

The descriptive case study allows the researcher to identify patterns in a shared phenomenon that transcends individual experience (Burkholder et al., 2016). In this study, I interviewed 15 compliance managers who had extensive knowledge of the principles of money laundering and terrorist financing and anti-money laundering and counter terrorist financing policies and procedures. I also collected data from observations and reviews of organizational documents. I collected data from semistructured interviews, observations, and document review analysis. In the descriptive case study, researchers draw conclusions about their research question based on direct interactions and observations to describe the experience of the subjects. The descriptive case study was appropriate for this study because the purpose of the study was to explore how compliance managers identify predicate offense typologies to reduce the risks of money laundering and terrorist financing activities.

Role of the Researcher

The role of a researcher is to conduct scholarly research by selecting participants, compiling data, conducting data analysis, and analyzing the findings (Taylor et al., 2015). As a researcher, I chose a research methodology and design, select compliance managers, communicate with voluntary participants, interview voluntary participants, and evaluate their responses. Cui (2015) indicated that a qualitative researcher plays an insider-outsider role. Researchers are responsible for gathering, assessing, evaluating the data, and interpreting the findings. During the data analysis process, researchers are responsible for articulating clear, unbiased, and succinct data (Malagon-Maldonado, 2014). In this descriptive case study, I played a significant role in data collection by collecting, coding, analyzing, and interpreting the data myself.

As a researcher, I interviewed 15 compliance managers of U.S. banking and financial services organizations to reach the point of data saturation. In addition, I was an anti-money laundering investigator with over three years of experience in the banking and financial services industry. As a researcher, my money laundering and terrorist financing knowledge and anti-money laundering experience can subject me to biases. A researcher's background knowledge and experience can cause bias. Leedy and Ormrod (2015) explained that bias is a foreseeable issue which might distort the evaluation of data in a qualitative study. In this study, bias may stem from my preexistent knowledge and understanding of anti-money laundering investigations due to my professional experience of three years at banking and financial services companies. In most research studies, researchers with a robust subject matter expertise and experience in the subject

inadvertently introduce bias into the study (Taylor et al., 2015). To reduce bias, I eliminated my strong background in the subject matter through a process known as bracketing. Malagon-Maldonado (2014) suggested employing bracketing, a process that allows researchers to suppress their preexistent preconceptions throughout the planning, interviewing, analyzing, and interpreting stages to reduce bias.

Despite my experience in the industry, I ensured to select research participants with whom I have no personal or professional relationship. Kruth (2015) suggested that qualitative research depends on a researcher's interview skills and diligence to collect data. As a qualitative researcher, I conducted the data collection process through interviews, but I will not be a participant in the study. To ensure that the research data is trustworthy, I strived for objectivity and maintain good ethical practices during the data analysis process. The disclosure of my assumptions, limitations, delimitations, personal opinions, and sharing data collection procedures and analysis results with the participants will help to eliminate my biases.

Methodology

The methodology of this study was qualitative in nature; I used a descriptive case study approach to gain a comprehensive understanding of how identifying predicate offense typologies help compliance managers to reduce the risks of money laundering and terrorist financing activities. The qualitative research methodology was the most appropriate approach instead of a quantitative or mixed methods approach because the capability to gather information from interviewing participants helps to enhance the interpretation of human experience than analyzing statistical variables. The ideological

process of comprehending social phenomena based in a natural setting is the overall essence of qualitative research (Ravitch & Carl, 2016). The qualitative method relates directly with the participants' experiences (Ravitch & Carl, 2016) and expand knowledge of opinions and reasonings related to predicate offense typologies. On the other hand, the quantitative method validates theories based on statistical measures. The quantitative method is not appropriate because this study is not deductive. I did not test or measure any statistical variables for acceptance or rejection of theory (Frankfort-Nachmias et al., 2015). I concluded that the qualitative methodology will be optimum for this study because it explores participants' varied opinions and experiences relevant to predicate offense typologies and the risks of money laundering and terrorist financing activities. To gain a deeper understanding of a specific phenomenon or human experiences, Marshall and Rossman (2015) indicated that the qualitative research methodology is the most appropriate approach rather than the quantitative research methodology because it focuses on human interaction through participants' experiences, actions, behaviors, and perspectives.

The primary data collection sources were semistructured interviews, semistructured observation, and document review analysis. To conduct document review analysis, I searched Google Scholar and business and finance academic journals for peer-reviewed articles between 2018 to 2022 using the following keywords: anti-money laundering, counter terrorist financing, predicate offense typologies, AML red flags, and compliance strategies. I reviewed annual reports of the Financial Action Task Force between 2018 to 2022 for current trends and typologies and articles generated by the

Financial Crimes Enforcement Network for potential indicators. The data collection and analysis of multiple data sources present extent in triangulation.

Participant Selection Logic

Population

The research participants in this study included compliance managers of U.S. banking and financial services organizations. The sample population consisted of 15 individuals who will represent the case. Yin (2018) cautioned that the ability to enter data saturation is more important than the size of the sample. To achieve a saturation level, scholars have different views on the adequacy of the sample size. Since the sample size depends on several factors, including the RQs and the purpose of the study, Wahyuni (2012) argued that there must be at least 15 participants to have sufficient data saturation in a qualitative research study. Fusch and Ness (2015) explained that there is no one-size-fits-all method to reach data saturation. Also, data saturation is more about the richness and thickness than the size of the sample. Data saturation is attained when there is adequate information, and no additional data or themes arise.

Compliance mangers and anti-money laundering investigators with years of experience are the individuals with the most relevant knowledge and subject matter expertise. U.S. banks and financial services corporations modify policies and procedures on economic compliance based on the current money laundering and terrorist financing activities. The individuals who engage in the process of identifying predicate offense typologies are in supervisory roles and anti-money laundering investigators with extensive work experience. Employees within that category must fall under the inclusion

criteria including professional role, function in the organization, length of service, years of experience, and an indirect relationship with myself.

The target population was appropriate because such leadership employees are characteristically responsible for ensuring effective compliance regulations and reducing the risks of money laundering and terrorist financing activities in banking and financial services organizations. The purposeful sampling strategy was appropriate because the nature of study entails compiling responses from a particular group of individuals.

Sampling Strategy

In case studies, the concept of replication is an essential characteristic. Yin (2018) indicated that replication allows researchers to replicate, compare, and expand on a case which is considered an independent and different experiment. Case studies are nonexperimental in nature; hence, researchers rely on real-world context. The nature of case studies considers replication an appropriate means to meet the purpose of this study of obtaining a greater understanding of how compliance managers identify predicate offense typologies to reduce the risks of money laundering and terrorist financing activities.

In the context of studies, researchers select cases to present insight into the research topic, so purposeful sampling is an appropriate sampling strategy. Purposeful sampling is commonly used in qualitative research to identify and select research participants. To identify the participants from a targeted population, I used a purposeful sampling strategy and selected 15 participants who helped me to reach data saturation. The purposeful sampling of 15 compliance managers formed the case. At the point where

I obtained rich and thick data and continued to see similar data patterns repeatedly, I assumed I have reached data saturation. At that point, I no longer needed to conduct further interviews and I began analyzing the data.

Purposeful sampling is a non-probability method of selecting the phenomenon of interest based on predetermined characteristics of a population and the objective of the study. The predetermined criterion may include years of experience, professional role, background knowledge, and other factors (Maxwell, 2013; Sharafizad & Coetzer, 2016). Furthermore, researchers use a referral sampling approach also known as the snowball technique or chain sampling strategy. The snowball technique entails the selected participants to recruit future subject from within their networks (Ravitch & Carl, 2016). The snowball technique helps researchers to build their sample population and reach the data saturation level with sufficient data and information pertaining to their studies. The purposeful and snowball sampling techniques of 15 compliance managers with adequate experience in banking and compliance supervision formed the case. The sample size selection generates rich and thick data that provide new knowledge and a comprehensive understanding of a phenomenon.

Procedures for Recruitment, Participation, and Data Collection

Recruitment

The target participants for this study were compliance managers and anti-money laundering investigators of U.S. banking and financial services organizations who have a primary responsibility to reduce the risks of money laundering and terrorist financing activities. An aspect of the recruitment process is to consider the characteristics of the

study, the characteristics of the study population, the willingness of the participants, the type of work, and the characteristics of the participants (Arends et al., 2014). Prior to the recruitment process, it was important to establish the participants' eligibility criteria for this descriptive case study.

A criterion will define the selection of participants. The inclusion criteria identify the study population in a coherent and independent manner (Garg, 2016). The exclusion criteria include factors or characteristics that make the recruited population ineligible for the study. These factors may be confounders for the outcome parameter. The target population comprised of individuals responsible for or involved in anti-money laundering and counter terrorist financing investigations. The criteria for inclusion in this study required participants to (a) be managers who currently work in a supervisory position in the anti-money laundering division under the compliance department, (b) be current investigators who have experience or career background in anti-money laundering for more than three years, and (c) not have a current direct working relationship with me to minimize any potential for perceived coercion. The criteria for exclusion in this study was (a) participants with no managerial experience, (b) participants with less than three years of anti-money laundering background, and (c) compliance directors and attorneys because they do not have the required knowledge and exposure to the subject. Based on this criterion, I used a purposeful sampling method to invite 15 compliance managers and anti-money laundering investigators of U.S. banking and financial services organizations to reach data saturation.

Participation

As a qualitative researcher, I worked with compliance managers and anti-money laundering investigators of U.S. banking and financial services organizations. Gaining access to the participants is like a dynamic game which requires researchers to demonstrate stability and flexibility. Peticca-Harris et al. (2016) suggested three means a researcher can obtain access to the participants: (a) identify a familiar individual, (b) contact an informant, and (c) verify an informant through a gatekeeper. For this study, I identified and networked with a familiar individual within the U.S. banking and financial services organizations. A critical strategy to have access to the organizations and research participants is to build and preserve trust with a familiar individual.

According to the strategy, I established a professional relationship with the targeted participants. First, I discussed and communicated the purpose of this study with the prospective participants. I explained the aim of this study and asked for their approval to comply with Walden University Institutional Review Board's (IRB) regulations. Second, I emailed each prospective participant the invitation to participate in this study. Once a participant indicated their interest, I emailed the research participant a consent form that they needed to sign and return to me prior to the interview. Afterwards, I outlined a schedule for the interviews by establishing the place and time. I established a means of communication to gather feedback from the participants after sharing the compiled data.

The interview process involved a one-on-one interview with each targeted participant. I scheduled each interview to last between 30 to 60 minutes via the platform

Zoom. Each interview was conducted virtually to protect the health safety of each participant. At the beginning of each interview, I asked for the interviewee's permission to record their interview for transcription purposes. Also, I provided specific instructions and information such as the purpose of the interview, length of the interview, and how I will use the answers for data analysis. At the end of each interview, the interviewees had an opportunity to provide additional information and ask relevant questions.

Researchers should build a professional relationship with the research participants by identifying a mutually agreed-upon designated location, acquiring written consent, and establishing a working rapport. Leedy and Ormrod (2015) suggested providing research participants ample amount of time to assess information and make an informed decision. I built a working relationship with the research participants. Also, I ensured to acquire an informed consent form from each participant. Furthermore, I communicated the following to each participant: objective of this study, contents of the signed consent forms and the purpose of the interview, process to protect the privacy and identity of each research participant, and the total amount of required time for the semistructured interview. Additionally, I protected the participants' identities by giving each individual an assigned code number. Last, I placed all the compiled data in a secure location (i.e., filing cabinet) to protect the privacy and identity of the research participants.

Data Collection

Friedrich-Baasner et al. (2018) suggested that researchers can use interviews, observations, and document analysis to attain quality data. The data collection is an involved process with various steps including the recruiting participants, interviewing the

selected participants, and collecting the data. In this study, the targeted population consisted of 15 compliance managers of U.S. banking and financial services organizations.

The interview date, time, and location was mutually agreeable for all parties involved prior to the interview. The total interview process was anticipated to take up to two to three weeks. For those participants who hold a senior position in the companies, and I anticipated the participates will reschedule the interviews due to their roles and responsibilities. The suggested timeframe gave me sufficient time for triangulation.

To organize the data, I used Microsoft Excel spreadsheet to create a separate file location for each participant to begin an audit trail. I evaluated the data for themes and examined saturation. Furthermore, I saved the documents in appropriate file locations to guarantee ease of accessibility. Along with Microsoft Excel spreadsheets, qualitative data analysis software is a resourceful tool to organize and index data for analysis (Lincoln & Guba, 1985). I used a data analysis software to organize the unprocessed data.

Yin (2018) suggested that researchers systematize unprocessed information in a rational order to ease the transition to data analysis. The systematization a researcher implements will formulate or destroy the channeling of the themes. A method of arranging and gathering transcriptions, field notes, and answers is a crucial part of data collection. Kruth (2015) indicated that qualitative research depends on a researcher's interview skills and diligence to collect data. Triangulation of data through the semistructured interviews, semistructured observations, and document review analysis of the results of Clarke (2021), Mekpor (2019), Nizovtsev et al. (2022), annual reports of

Financial Action Task Force between 2018 to 2022 for current trends and typologies, and articles generated by the Financial Crimes Enforcement Network helped to ensure reliability and eliminate any bias. I conducted a debrief with the participants by examining about their experiences with the research to monitor adversity.

Instrumentation

In a case study, the purpose of instrumentation is to gather data from multiple sources considered valid and reliable to address the RQs presented in the study (Yin, 2018). Merriam and Tisdell (2016) advised that instrumentation should align with the purpose of the study and the conceptual framework in qualitative studies. The emerging themes from the data, gathered through the suitable choice of instrumentation, will be analyzed with the aim of identifying predicate offense typologies that help compliance managers reduce the risks of money laundering and terrorist financing activities.

The three data sources were (a) semistructured interview, (b) semistructured observations, and (c) document review analysis of the results of Clarke (2021), Mekpor (2019), Nizovtsev et al. (2022), annual reports of Financial Action Task Force between 2018 to 2022 for current trends and typologies, and articles generated by the Financial Crimes Enforcement Network. The study results derived from an appropriate data collection method to address the study's overarching RQ and four SQs. The overarching RQ was, What are the predicate offense typologies that U.S. banking and financial services company compliance managers identify to reduce the risks of money laundering and terrorist financing activities? The four SQs were as follows:

SQ1. How do anti-money laundering investigators identify predicate offense typologies?

SQ2. How successful are the investigators in identifying predicate offense typologies?

SQ3. What characteristics classify money laundering and terrorist financing as predicate offense typologies?

SQ4. How does identifying predicate offense typologies reduce money laundering and terrorist financing?

In the qualitative research process, triangulation is a systematic tactic that confirms or contradicts the collected data. In this research study, I used multiple sources of evidence during the data collection process. Data triangulation from multiple sources can ensure the trustworthiness and dependability of the results in a case study (Halkias & Neubert, 2020). During the data analysis process, I conducted a triangulation of data sources to establish trustworthiness of this study.

Semistructured Interviews

In a qualitative research study, Friedrich-Baasner et al. (2018) suggested that researchers can use semistructured interviews, observations, and document analysis to attain quality data that corresponds to the coding scheme and evaluates any undetermined effects. Observing study participants, taking field notes during interviews, and collecting documents provided by participants are suitable data collection techniques. Semistructured interview is a primary data collection method for a qualitative descriptive case study. For this research study, I used a semistructured interview technique with

open-ended interview questions to provide a profounder understanding of how compliance managers identify predicate offense typologies to reduce the risks of money laundering and terrorist financing activities.

Interviews are an excellent way for researchers to gather detailed information about a phenomenon (Ravitch & Carl, 2016; Rubin & Rubin, 2012; Yin, 2018). The interview process takes the interviewer through a personal learning process. Semistructured interviews allow participants to elaborate on their experiences of beliefs in a way that is not necessarily possible with other methods and allows participants an opportunity to share their own experiences in their own words and from their own perspectives (Laureate Education, 2016; Ravitch & Carl, 2016; Rubin & Rubin, 2012). Because semistructured interviews are designed to elicit detailed information, they are especially useful when a researcher's aim is to study the "how" of a social phenomenon (Creswell, 2013; Ravitch & Carl, 2016; Rubin & Rubin, 2012).

Yin (2018) explained the several types of interviews for a case study. The major types of case study interviews are shorter, lengthy case study, and survey interviews. The data collection process occurs over an extensive period. Jamshed (2014) indicated that researchers strongly support the use of prolonged case study interview and mutually agree that this type of interview is ideal to share meaning with participants. For this research study, I implemented prolonged case study interviews which allow for flexibility in data collection. First, the semistructured interviews took place between 30 to 60 minutes. Prior to each interview, a technology test was performed to confirm that all recording equipment used was operating appropriately and error free. At the beginning of

each interview, I asked for the interviewee's permission to record. Also, I provided specific instructions and information such as the purpose of the interview, length of the interview, and how the answers will be used for data analysis. At the end of the interview, the interviewees had an opportunity to provide additional information and ask relevant questions. To attain high-quality results, I used several types of technology such as audio recording devices to collect the data and capture the discussions. Finally, I conducted follow-up meetings with the participants to discuss the interview transcriptions which occurred for up to 15 minutes. To confirm and triangulate the data collected from semistructured interviews, I utilized field notes from the semistructured observations.

Semistructured Observations

The second type of instrument I used for data collection will be semistructured observations of the predicate offense typology identification process and compliance manager behavior. The objective of conducting semistructured observations is to create new knowledge based on the description of the participants' daily processes. I observed the target participants during each interview and sought to learn how they identify predicate offense typologies to reduce the risks of money laundering and terrorist financing activities. A related qualitative case study RQs by Shah (2021) have also been answered using observations to triangulate interview data.

Document Reviews

Last, the third type of instrument I used for data collection will be document review. Researchers conducting a case study can use multiple sources of data collection. I searched Google Scholar and business and finance academic journals for peer-reviewed

articles between 2018 to 2022. I conducted a word search using the following terms: anti-money laundering, counter terrorist financing, predicate offense typologies, AML red flags, anti-money laundering policies and procedures, and compliance strategies. These journal article sources were utilized to ensure triangulation, answer the RQ, and establish credibility and trustworthiness of this study's findings. Related qualitative case study RQs by Shah (2021) and Juntunen and Teittinen (2022) have also been answered using document review analysis to triangulate interview data. I reviewed annual reports of the Financial Action Task Force between 2018 to 2022 for current trends and typologies and articles generated by the Financial Crimes Enforcement Network for potential indicators to ensure triangulation of data. Subsequently, to provide a deeper understanding of what predicate offense typologies compliance managers identify to reduce the risks of money laundering and terrorist financing activities.

Data Analysis Plan

The process of condensing data to its narrative and understanding is data analysis. During the data analysis phase, I organized formerly gathered data from semistructured interviews, semistructured observations, and document review by summarizing and categorizing information based on patterns and themes. In qualitative research, analysis and transcription of meaning offers interpretation, transformation, and understanding of the data.

Coding

The data collected from the semistructured interviews was transcribed into a document for data analysis purposes. Ravitch and Carl (2016) prescribed the use of

interview transcripts to aid in the coding process. Coding is the process of assigning an evocative, essence-capturing, salient, succinct, and a summative attribute to a section of visual or language-based data (Saldãna, 2016). First, I began coding the interview transcript in Word by analyzing the text for keywords or phrases which stand out. Second, I assigned a word or phrase to a data point related to an idea, concept, or quality in the text transcription to form patterns and themes. The initial coding of the data will include coding into groups which is reflective of the purpose of the research, exhaustive, mutually exclusive, sensitive to category content, and conceptually congruent with one another (Kawulich, 2004; Ravitch & Carl, 2016; Rubin & Rubin, 2012). This data analysis approach will create a structure for the data.

Coding provides the researcher with the ability to process, organize, and reorganize qualitative data into categories. A category is a sort of bucket where coded data which share attributes, qualities, or meaning are placed together as a representation of some concept (Kawulich, 2004; Ravitch & Carl, 2016; Rubin & Rubin, 2012). Categorizing can be defined as identifying and giving a name to basic units or groups of coded data (Ravitch & Carl, 2016). Categories help the researcher determine the conceptual and relational analysis of different data units (Rubin & Rubin, 2012). A category in qualitative research will attempt to group patterns that are observed in the data along with clumping together groups of data that have been previously coded into themes (Saldãna, 2016). The categorization of codes reflects themes. A theme is developed from categories and represents a concept related to the research phenomenon, which is either directly observable or an underlying element.

In-vivo coding will allow the researchers to use the participants' words to label data segments instead of the researcher creating words or phrases (Ravitch & Carl, 2016). Semistructured interviews and observations can note concepts the researcher may wish to explore more systematically (Rubin & Rubin, 2012). In addition, I used quotations to establish notable themes that might help answer the RQ. The analysis process of different data source will ensure triangulation and build credibility and trustworthiness.

Qualitative Software

I used Dedoose, a qualitative data analysis software, to code, categorize, and coordinate the data by identifying codes in the study. Additionally, I conducted hands-on coding to ensure the data accurately depict the participants' experiences and the true intentions behind their work. Hand-coding is a necessary method to ensure dependability of the coding completed by a qualitative data analysis software.

Thematic Analysis

Researchers closely examine transcribed data to identify common themes and patterns from transcribed data (Lochmiller, 2021). A theme helps the researcher develop, identify, and analyze the interpretations of patterns of meanings that evolve into themes (Saldãna, 2016). I used thematic analysis to identify recurring central themes from the coded data that directly addresses the overarching RQ. Along with the Dedoose software, I used thematic analysis to categorize the data to establish significant themes. Triangulation of the data analysis sources is important to ensure accuracy.

Content Analysis

Content analysis is a valuable research tool that defines the existence of words, themes, or concepts within the collected data. Researchers use content analysis to assess the presence and meaning of words, themes, or concepts (Lindgren et al., 2020). I used content analysis to analyze the data collected from document reviews and interpret meaning from the content of text data. I examined relative journal articles to determine the presences of words, categories, and themes. Content analysis strengthens the trustworthiness of qualitative data analyses by focusing on the perception and interpretation during the data analysis stage (Lindgren et al., 2020). The data analysis plan conducts methodological triangulation. During the data analysis process, I ensured to accurately report the data.

To answer the RQs, I analyzed the data from semistructured interview transcripts, the notes from the semistructured observations, and information from the document reviews by using an amalgamation of multiple schemes such as coding, categorizing, thematic analysis, and content analysis to ensure data analysis triangulation (Yin, 2018). For this study, I used the steps recommended by Yin (2018) which are (a) begin by reading through all the data, (b) sort and organize the data for analysis, (c) start a comprehensive analysis, using a coding scheme, by labeling the compiled data into manageable units, (d) summarizing and categorizing the data into a sequence of patterns and themes, (e) interpreting, and (f) developing a meaningful data set. The analysis plan built my credibility as a responsible and trustworthy qualitative researcher.

Issues of Trustworthiness

Researchers must establish trustworthiness in qualitative research. Trustworthiness is a notion that illustrates the credibility and reliability of a phenomenon (Ravitch & Carl, 2016; Shenton, 2004). Quantitative and qualitative researchers use different methods to establish trustworthiness (Frankfort-Nachmias et al., 2015). In terms of qualitative research, researchers develop the integrity of the research by ensuring that the data is credible, transferable, dependable, and confirmable. Credibility sets the groundwork of research and establishes trust with the research participants (Ravitch & Carl, 2016). It confirms that the researcher and gathered information are plausible and the interaction between the researcher and the participants is apt (Rubin & Rubin, 2012). Overall, credibility creates an opportunity for the researcher to interact with participants that will add value to the research which will lead to social change (Laureate Education, 2016). Transferability aides in ensuring that the results of the data collected can be applied to a larger population. Dependability is essential to ensure the quality of the research conducted could be repeated and result in a similar outcome (Korstjens & Moser, n.d.). Ravitch and Carl (2016) stated that confirmability results from others corroborating that the outcome of the research is accurate and there is no bias presented that might distort findings.

The objective for all researchers is to maintain trustworthiness using various strategies. The conditions to help develop establish trustworthiness include credibility, authenticity, transferability, and confirmability of issues relating to internal and external validation, reliability, and objectivity. When a researcher can demonstrate that the data

collected can be used among various populations while maintaining transferability the researcher is able to maintain credibility and trustworthiness (Ravitch & Carl, 2016). Comparing similar experiences between participants of the study helps to evaluate the credibility of the study. The methods to ensure dependability and confirmability in a research study involve the use of audit trail and reflexivity. Some factors including population size, research process, transparency, openness, and richness and thickness of the data collected affect trustworthiness.

Credibility

Credibility sets the groundwork of research and establishes trust with the research participants (Ravitch & Carl, 2016). It confirms that the researcher and gathered information are plausible and the interaction between the researcher and the participants is apt (Rubin & Rubin, 2012). To enhance the credibility of a research study, a researcher's conclusions must truthfully represent the sentiments and life experiences of the sample population observed, surveyed, or interviewed and participants' information should be thoroughly examined with integrity, and any shift in the nature of the data collected must be documented.

To ensure the research is credible, the researcher needs to acknowledge reflexivity. Reflexivity is the awareness of any personal biases that could affect the interpretation of participant experiences, and therefore, the results of the study (Lincoln & Guba, 1985; Stewart & Hitchcock, 2016). When utilizing life experiences as the data measured, researchers must acknowledge that multiple realities exist within the scope of the RQ their study aims to answer (Stewart & Hitchcock, 2016). Recognizing each of

these limitations and presenting the participants' data as truthfully as possible ensures the research is valid and credible. To mitigate bias, a reflexive journal can help to reflect the thoughts and feelings of a researcher's perception.

Credibility creates an opportunity for the researcher to interact with participants that will add value to the research which will lead to social change. To ensure credibility, I devoted adequate time to each participant during the interview process to obtain comprehensive knowledge of the case under investigation. Furthermore, I focused on the emerging themes to notice repetition. Once I reach the data saturation level, I captured the incidences that offer rich and thick data. Moreover, I transcribed the interviews verbatim and ensure participant checking takes place prior to the data analysis process. I highlighted and immediately addressed any discrepancies. Other techniques to ensure credibility included following up with participants through a telephone call after each interview before beginning the data analysis process, asking the participants to confirm my interpretation of their responses, always protecting the participants' confidentiality, and allowing the participants to discontinue their participation in the study at any time.

Transferability

Transferability aides in ensuring that the results of the data collected can be applied to a larger population. Transferability is established by providing readers with evidence that the research study's findings could be applicable to other contexts, situations, times, and populations. To ensure transferability of the study, researchers can provide a detailed analysis of the participants selection, recruitment of participants, data collection, and the methods used to verify the information and ensure accuracy of the

data collected. Yet, transferability cannot be guaranteed. Triangulation is a tactic of trustworthiness, which encompasses data gathering methods to assemble multiple perceptions (Ravitch & Carl, 2016). To ensure transferability of this research study, I provided a detailed and thick analysis of the participants selection, recruitment of participants, data collection, and the methods used to verify the information and ensure accuracy of the data collected. I used triangulation to ensure the study was believable and transferable.

Dependability

Dependability in qualitative research refers to the consistency of the results of a study over time, as a comparable RQ is answered employing the same research methods and analysis (Stewart & Hitchcock, 2016). The researcher's findings should be clear enough for another researcher in the field to replicate the study with a similar method and sample population (Golafshani, 2003; Stewart & Hitchcock, 2016). When the results of a study prove consistent over time, it enforces the validity of the methods used to gather data and the study itself (Stewart & Hitchcock, 2016). For qualitative research, reliability is more about dependability. If a study is conducted multiple times within a specific period with consistent results, it is safe to assume the data collection method is stable (Golafshani, 2003). Stability and consistency are the basis for reliability in qualitative research, but the transparency of the researcher is also essential to achieving and maintaining reliability in a qualitative study. To ensure dependability, I conducted external audits. A method of external audit is peer debriefing. Peer debriefing is a process which requires the researcher to collaborate with colleagues who hold unbiased views of

the study. The unbiased colleagues assess the researcher's transcript, findings, and methodology to provide effective feedback (Janesick, 2015). Feedback is given to enhance the study's credibility and ensure validity of the findings.

Confirmability

Confirmability of the research findings provides the trustworthiness of the researcher providing the ideas and experiences of the research participants and does not reflect the preferences of the researchers (Ravitch & Carl, 2016; Shenton, 2004). One way for qualitative researchers to ensure the confirmability of their research data is the use of triangulation of data. Utilizing different methods of gathering data (interviews, focus groups, document reviews, etc.) provides the qualitative researcher with different methods of gathering data which allows him/her to engage in triangulation of the data gathered to further validate the research results (Ravitch & Carl, 2016; Rubin & Rubin, 2012; Shenton, 2004).

In addition, another method to ensure confirmability is to use an audit trail. An audit trail demonstrates a data-driven approach to the recommendations of the research study which reduces any levels of predisposition (Shenton, 2004). Audit trails provide a comprehensive method to demonstrate the results based on the participants' experiences and descriptions. It inaugurates transparency of the data by explaining how the researcher gathered and evaluated the data. Audit trails are a form of confirmability that allow the reader to substantiate the findings and draw conclusions from the data. The fundamental connotations of trustworthiness and credibility in terms of the methodology of the research study corroborate quality in qualitative research (Ravitch & Carl, 2016; Salmon,

2013; Shenton, 2004). Overall, it involves a level of accountability of the story of the phenomenon being related by the researcher and the purpose of the research that is being conducted (Laureate Education, 2016; Salmon, 2013). To ensure confirmability, I interpreted the participants' ideas and experiences without any bias.

By using triangulation of data, I warranted confirmability of the data collected and validate of the findings. The different data collection approaches I used were semistructured interviews, semistructured observations, and document reviews from business and finance academic journals for peer reviewed articles related to anti-money laundering and counter terrorist financing typologies and red flags, Financial Action Task Force trends, and Financial Crimes Enforcement Network potential indicators. As a researcher, I ensured a level of accountability of the story of the phenomenon being related and the purpose of the research that is being conducted.

Ethical Procedures

Researchers are responsible for conducting a study that abides by all the elements on the IRB approval checklist. The research must use an appropriate method that allows the researcher to discover the subject comprehensively. In qualitative research, the methods used in the research improve the possible exposure of participants who engage (Ravitch & Carl, 2016; Rubin & Rubin, 2012). It is important to determine the type of study and how to conduct the study. Special precautions need to be taken related to the potential ethical concerns which may arise when conducting the research.

The participants in this study were compliance managers and anti-money laundering investigators of U.S. banks and financial services institutions. It is an ethical

procedure to protect the privacy and confidentiality of each participant. I used a numeric code to identify each participant. The information gathered about each participant and the associated code number was documented in an Excel spreadsheet.

The participants for the semistructured interviews were recruited from my professional network. I used the snowball sampling to complete the recruitment process. A monetary incentive was given for participation. An invitation to participate in the study was sent to each prospective participant (see Appendix A). After the recruitment process was completed, each participant signed an informed consent form prior to the interview. The consent forms were collected via email before scheduling the interviews. The consent form included information about the study and informed the participants that they have a right to withdraw from the study at any time and that their personal information will not be shared with anyone. After I obtained IRB approval (no. 04-19-22-0607102), I began data collection.

To maintain the health safety of the participants, each interview was conducted virtually and audio recorded using the platform Zoom. Participants reviewed their interview transcripts for precision to ensure their experiences and shared knowledge or information were accurately reflected. A numeric code was assigned to each interview participant to protect their privacy and confidentiality. The data were stored in three different places including the OneDrive cloud, my laptop, and a Passport drive. Each location is secured with a password-protection, and only I have access to these storage places. According to the IRB requirements, the data will be kept secured and destroyed 5 years after the completion of the study.

Researchers must be willing to be flexible, transparent, and driven by a strong moral compass. It is the moral compass of the researcher that provides for their professional ethical code and professional policies (Rubin & Rubin, 2012). Ethics involves the researcher doing good and avoiding harm (Ravitch & Carl, 2016). One of the primary responsibilities of the researcher is to apply the ethical principles of qualitative research while protecting human participants in the research study. It is the researcher's responsibility to have the participants' best interests in mind while protecting them from potential harm. The researcher must also comply with laws and ensure integrity as a professional researcher.

Summary

Chapter 3 introduced the research methodology and provides the information about the methodology used that allows the study to replicate. Furthermore, this chapter discussed the research design, the role of a researcher, participant selection, sampling selection, maintaining confidentiality, data collection and analysis. The qualitative method enabled me to describe, explore, and understand the problems that compliance managers face in identifying the predicate offense typologies to reduce the risks of money laundering and terrorist financing activities. I indicated the inappropriateness of the quantitative methodology and the other qualitative research designs namely narrative, grounded theory, phenomenology, ethnography.

The descriptive case study design allows for the use of multiple data sources to further enhance the trustworthiness of the research. In the research study, the proposal was to conduct semistructured interviews with compliance managers of U.S. banking and

financial services organizations. The data compiled may give insight into the problems the compliance managers face that has led to the ongoing, increased issues of money laundering and terrorist financing activities.

A comprehensive understanding of the problem may help compliance managers identify predicate offense typologies to reduce the risks of money laundering and terrorist financing activities. Chapter 4 included a summary of the findings in light of the RQs and an analysis of the data. Chapter 5 addressed the limitations of interpretation, implications of the study, recommendations for professional excellence, and suggestion for future research.

Chapter 4: Results

Introduction

The purpose of this qualitative descriptive case study was to identify predicate offense typologies that U.S. banking and financial services company compliance managers use to reduce the risks of money laundering and terrorist financing activities. In alignment with the purpose of this study, the central RQ for this qualitative descriptive case study was, What are the predicate offense typologies that U.S. banking and financial services company compliance managers identify to reduce the risks of money laundering and terrorist financing activities? The sub-RQs for the study were

SQ1. How do anti-money laundering investigators identify predicate offense typologies?

SQ2. How successful are the investigators in identifying predicate offense typologies?

SQ3. What characteristics classify money laundering and terrorist financing as predicate offense typologies?

SQ4. How does identifying predicate offense typologies reduce money laundering and terrorist financing?

The research may contribute to positive social change by informing compliance managers of strategies they can use to reduce the risk of bank failures. The study may also highlight opportunities to strengthen existing regulatory mechanisms. These changes may protect the public by reducing the number of bank failures.

In this chapter, I present the study results. The chapter also includes a description of the research setting, participant demographics, discussion of the data collection and analysis procedures, and evidence of trustworthiness. Applying purposive sampling, I selected 15 compliance managers and anti-money laundering investigators from U.S. banking and financial services companies to participate in semistructured interviews. All 15 participants answered 11 open-ended questions. The open-ended nature of the issue prompted comprehensive responses from the participants. I assessed the results of the semistructured interviews and semistructured observations together with findings from a document review analysis that I conducted. For the document review, I analyzed scholarly works by Clarke (2021), Mekpor (2019), and Nizovtsev et al. (2022); annual reports of the Financial Action Task Force between 2018 to 2022 for current trends and typologies; and articles generated by the Financial Crimes Enforcement Network. The evaluation of these documents, the participants' responses, and observations were the basis for the findings of this study.

Research Setting

To collect valuable data, it was important to recruit participants with a suitable background, experience in anti-money laundering, and knowledge on the subject. During the data collection process, I found that the participants were not comfortable with an in-person interview due to the prolonged effect of the Covid-19 pandemic in May of 2022. I used Zoom, an online videoconferencing platform software, to conduct the interviews. The 15 target participants who met the eligibility criteria and indicated their willingness to participate in the research study received an informed consent form. Each participant

answered the RQs and provided comprehensive information on the predicate offense typologies that compliance managers identify to reduce the risks of money laundering and terrorist financing activities. During the interviews, I did not ask the participants to reveal their personal or organizational information. I have no knowledge of any personal or organizational information that may have influenced participants at the time of this study.

Demographics

The target population comprised individuals responsible for or involved in anti-money laundering and counter terrorist financing investigations. The criteria for inclusion in this study required participants to (a) be managers who currently work or previously worked in a supervisory position in the anti-money laundering division under the compliance department, (b) be current investigators who have experience or career background in anti-money laundering for more than 3 years, and (c) not have a current direct working relationship with me to minimize any potential for perceived coercion. For this study, I used these three eligibility criteria to recruit individuals, from within my professional network, amongst U.S. banking and financial services organizations.

I used the informed consent form as supporting documentation to validate the participants' background, level of experience, and lack of working relationship with me. I refrained from collecting any other personal demographics apart from the confirmation from each participant about meeting the study eligibility criteria. I demonstrated the eligibility criteria met by the target participants, see Table 1.

Table 1

Number of Target Participants Who Met the Study's Eligibility Criteria

Eligibility criterion	No. of participants
Manager who currently works in a supervisory position in the anti-money laundering division under the compliance department	5
Current investigator who has experience or career background in anti-money laundering for more than 3 years	10
Does not have a current direct working relationship with me	15

Data Collection

My recruitment approach involved complying with the IRB requirements for participant selection. I ensured that the selected participants were adults. Moreover, after data retrieval, I took measures to protect the identity of each participant and to meet the confidentiality requirements designated by the IRB in terms of the data collected. To select participants, implemented two conventional approaches: purposive sampling based on actor types and snowball sampling to recruit professionals who could participate in the interviews (Hirschhorn, 2019). I used the purposeful sampling method to recruit 15 compliance managers and anti-money laundering investigators of U.S. banking and financial services organizations to answer the RQs. The overarching RQ was, What are the predicate offense typologies that U.S. banking and financial services company compliance managers identify to reduce the risks of money laundering and terrorist financing activities? To gain a deeper understanding of the phenomenon under study, I developed the following SQs:

SQ1. How do anti-money laundering investigators identify predicate offense typologies?

SQ2. How successful are the investigators in identifying predicate offense typologies?

SQ3. What characteristics classify money laundering and terrorist financing as predicate offense typologies?

SQ4. How does identifying predicate offense typologies reduce money laundering and terrorist financing?

The participants provided information on the predicate offense typologies that U.S. banking and financial services company compliance managers identify to reduce the risks of money laundering and terrorist financing activities.

The professionals who participated in the semistructured interviews were either (a) managers who currently work or worked in a supervisory position in the anti-money laundering division under the compliance department or (b) current investigators who have experience or career background in anti-money laundering for more than 3. Also, participants did not have a current direct working relationship with me to minimize any potential for perceived coercion. To protect the identity of the participants, I used pseudonyms to characterize the participants from Participant 1 to Participant 15, see Table 2.

Table 2

Participants' Professional Characteristics

Participant no.	Rank	Years of experience	Direct working

			relationship with the researcher
1	Anti-money laundering investigator	3+	No
2	Anti-money laundering investigator	3+	No
3	Anti-money laundering investigator	3+	No
4	Compliance manager	7+	No
5	Anti-money laundering investigator	3+	No
6	Anti-money laundering investigator	3+	No
7	Anti-money laundering investigator	8+	No
8	Compliance manager	7+	No
9	Anti-money laundering investigator	3+	No
10	Anti-money laundering investigator	3+	No
11	Anti-money laundering investigator	3+	No
12	Anti-money laundering investigator	3+	No
13	Compliance manager	5+	No
14	Compliance manager	5+	No
15	Anti-money laundering investigator	3+	No

I used the snowball sampling technique by asking the interviewees to recommend other participants. To comply with the IRB requirements, I divided my list of prospective participants into subsequent classifications on a Microsoft Excel spreadsheet, which is stored in secured location with limited access; the spreadsheet contains the (a) name, (b) email address, and (c) phone number of each individual (see Hirschhorn, 2019). I communicated with these individuals by emailing them the research study invitation and asking for their participation. I sent the email from a Gmail or Yahoo account to the participant's personal email address. The individuals who met the eligibility criteria and indicated their willingness to participate in the research study received an informed consent form including sample interview questions. I obtained each participant's consent prior to scheduling the interview. The informed consent protocol required the obtainment

of each participant's explicit permission to engage in the study prior to the collection of any data.

The participant recruitment process began on May 17, 2022. I allocated two weeks to recruit participants to ensure ample time for any follow-up emails or calls. The participants who participated in this study were recruited through my professional network. I contacted about 25 people by sending them the study invitation to their personal emails. In total 15 individuals indicated their willingness to participate in the research study which is a response rate of 60%. The 15 participants were emailed a copy of the informed consent form and sample interview questions. By June 10, 2022, 15 individuals assented to participate, allowing me to reach the target sample size of 15 participants in this study.

Contrary to expectations, none of the participants recommended an in-person interview due to the rise in Covid-19 cases. I conducted all the interviews using Zoom, an online videoconferencing platform. Each interview was completed within 30-60 minutes. All the interviews were audio-recorded only on Zoom and Recorder, a recording application. Though the interviews were audio-recorded, I took detailed notes to ensure a comprehensive transcript for further data analysis. During the interviews, I clarified the responses to certain questions by repeating the answers provided by the participants to confirm and clarify my understanding of their responses related to the question(s).

At the start of each interview, I provided a basic introduction and outline of the interview protocol. Also, I ensured to answer any questions the participants had to put

them at ease and gain their confidence prior to diving into the questions. The participants answered the following open-ended questions during the interviews:

1. What characteristics classify financial crimes as a predicate offense?
2. What are the typologies in money laundering and terrorist financing and how many typologies are there in total?
3. What current strategies do you use to identify predicate offenses?
4. What are the indicators or red flags that help you to detect a predicate offense?
5. What technologies do you use to identify predicate offenses?
6. How successful are your investigators in identifying predicate offenses?
7. How does identifying predicate offense typologies reduce the risks of money laundering and terrorist financing activities?
8. Which predicate offense typology gives rise to a charge of money laundering or terrorist financing?
9. What is the impact of failure to detect a predicate offense during an anti-money laundering investigation?
10. What is the effect of the Covid-19 pandemic on your strategies to identify predicate offense typologies?
11. What obstacles do you face due to the Covid-19 pandemic that could prevent your investigators from identifying predicate offenses during an anti-money laundering investigation?

The participants addressed the questions openly and provided detailed responses. I only audio-recorded the interviews using the Zoom and Recorder applications. Zoom is a

videoconferencing platform which allows the user to download the audio-recorded only meeting. Furthermore, the Recorder application auto transcribed the interviews. This software allows the user to play, rewind, fast forward, and skip the recording. The length of each transcription differed from one another based on the amount of data collected for each interview question. After reviewing the transcriptions, I sent them to the respective participants for member checking. Each participant provided their approval and or feedback.

The second type of data source I used was semistructured observations of the predicate offense typology identification process and compliance manager behavior. I observed the target participants during each interview and sought to learn how they identified predicate offense typologies to reduce the risks of money laundering and terrorist financing activities. I recorded keywords or ideas that were repeated amongst the participants.

The third type of data source I used was document review analysis. I searched Google Scholar and business and finance academic journals for peer-reviewed articles between 2018 to 2022. I reviewed eleven total documents and documented keywords or terms relative to predicate offense typologies. I reviewed Clarke (2021), Mekpor (2019), Nizovtsev et al. (2022), five annual reports of the Financial Action Task Force between 2018 to 2022 for current trends and typologies, and two articles generated by the Financial Crimes Enforcement Network for potential indicators to ensure triangulation of data. Relative information provided in the journal article, annual reports, and articles were documented. The information noted included types predicate offense typologies,

money laundering and terrorist financing activities, methods of financial crimes, criminal behaviors, red flags, and key indicators of predicate offense typologies.

The document review analysis revealed shared information and ideas amongst the eleven documents. I assessed the number of documents that indicated common types of information. I identified a theme if at minimum three of the documents provided shared information such as a common idea or keyword. Seven documents referred to structuring, five documents referred to fraud, three documents referred to cybercrime, five documents referred to human trafficking/smuggling, seven documents referred to illicit arms trafficking, eight documents referred to illicit drug trafficking, four documents referred to real estate money laundering, and two documents referred to trade-based money laundering. Furthermore, seven documents referred to red flags and key indicators of predicate offense typologies, five referred to typology-specific common signs, and zero referred to 95% or above. Tables 7 and 8 show the main themes and subthemes, respective categories, and respective codes derived from the documents. The emerging themes addressed the overarching RQ and four SQs, as further discussed later in this chapter. The next step was to analyze the collected data.

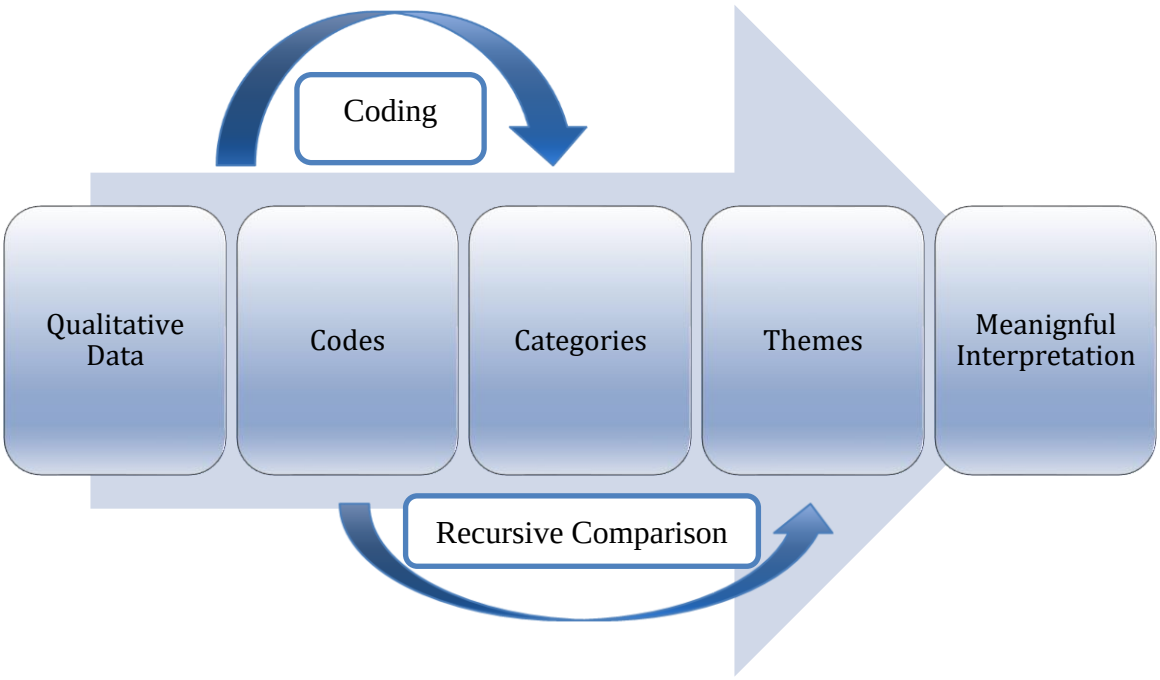
Data Analysis

Data analysis is an integral part of this qualitative descriptive case study. The compliance managers and anti-money laundering investigators answered open-ended questions which were qualitatively evaluated, coded, major themes recognized categorized, and the data retrieved contributed to the study findings. The qualitative descriptive case study consisted of semistructured interviews, semistructured

observations, and document review of Clarke (2021), Mekpor (2019), Nizovtsev et al. (2022), annual reports of Financial Action Task Force between 2018 to 2022 for current trends and typologies, and articles generated by the Financial Crimes Enforcement Network. The data collection methods generated comprehensive amount of data. Yin (2018) suggested using the following steps to conduct data analysis: (a) begin by reading through all the data, (b) sort and organize the data for analysis, (c) start a comprehensive analysis, using a coding scheme, by labeling the compiled data into manageable units, (d) summarizing and categorizing the data into a sequence of patterns and themes, (e) interpreting, and (f) developing a meaningful data conclusion. I used Microsoft Excel to organize the data which helped me to quickly conduct data analysis. I used the thematic analysis process to identify and analyze the themes, see Figure 1. The interpretation of patterns of meanings was the basis for the emergent themes (see Saldãna, 2016).

Figure 1

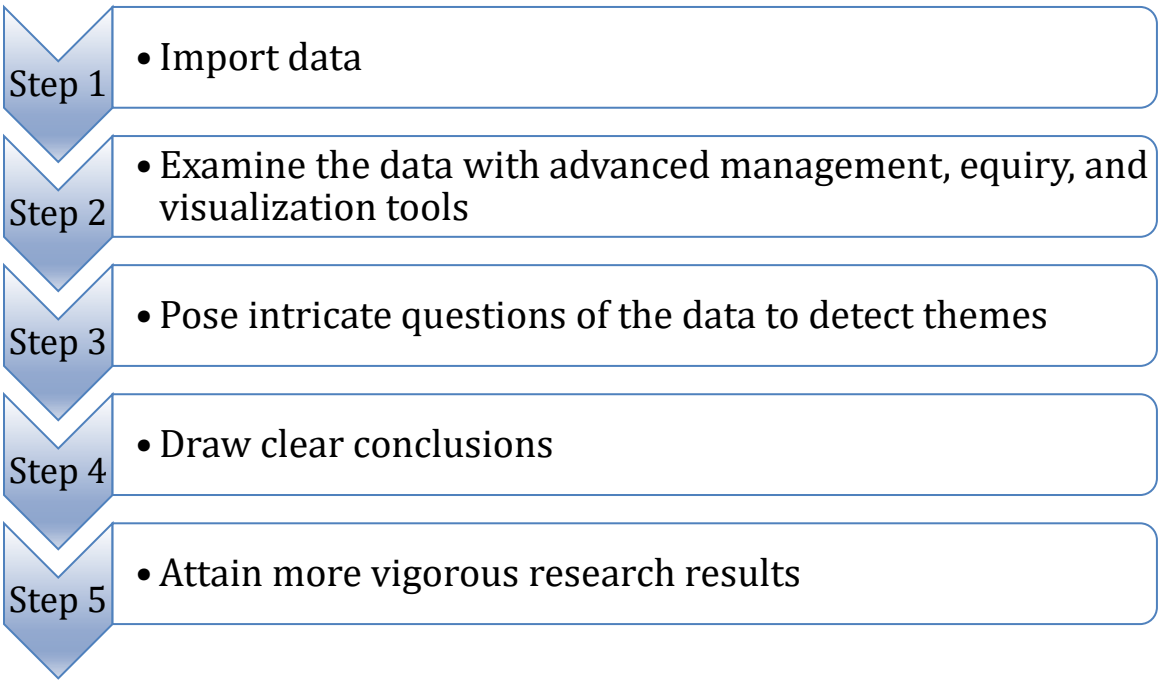
Thematic Analysis



In the data collection process, I reviewed the transcripts and assigned codes. Second, I separated the data to retrieve the codes from the participants' responses. After I analyzed the data, I coded the information gathered from the interview questions and correlated the themes to classification recognized in the conceptual framework and literature. Third, I congregated the data to derive themes. Fourth, I interpreted the data to identify themes which formed clusters of common themes. Last, I arranged a list of the most common and frequent themes. I used Dedoose to evaluate the collected data. The transcribed data were imported into Dedoose to organize, evaluate, and uncover insights in unstructured data, and generate clearly formulated, justifiable findings supported by accurate data. I took five steps to conduct data analysis, see Figure 2.

Figure 2

Steps in Data Analysis



To generate clearly formulated, justifiable findings, I created codes for each interview question, drew keywords from the participants' responses, and summarized emerging themes.

The first step is to sort and organize the data, by coding it in some way (Seers, 2011). When a researcher immerses him or herself in the data, patterns may start to emerge, which is the first step in making sense of the data. In-vivo coding uses the participants' words to label data segments instead of the researcher creating words or phrases (Ravitch & Carl, 2016). Early memos on interview transcriptions can provide a researcher with opportunities to reformulate RQs (Rubin & Rubin, 2012). Researchers can also note concepts the researcher may wish to explore more systematically (Rubin & Rubin, 2012). Sometimes quotations provide a notable theme that might help answer the

RQ (Rubin & Rubin, 2012). The analysis process of the interview data is not only vital to render useful research insights but also essential to build your credibility as a responsible and trustworthy qualitative researcher.

Coding is basically the process of assigning an evocative, essence-capturing, salient, succinct, and a summative attribute to a section of visual or language-based data (Saldãna, 2016). First, I began coding the interview transcript in Word by analyzing the text for keywords or phrases which stand out. Second, I assigned a word or phrase to a data point related to an idea, concept, or quality in the text transcription to form patterns and themes (Ravitch & Carl, 2016; Rubin & Rubin, 2012). The initial coding of the data included coding into groups which are reflective of the purpose of the research, exhaustive, mutually exclusive, sensitive to category content, and conceptually congruent with one another (Kawulich, 2004; Ravitch & Carl, 2016; Rubin & Rubin, 2012). This data analysis approach created a structure for the data.

Thematic data analysis acts as a data comparison tool. Thematic coding captures and unifies recurring central themes from the coded data that directly addressed the overarching RQ (Saldãna, 2016). The responses to the interview questions were assessed and coded to identify significant themes and trends. The categorization of codes reflects themes. A theme is developed from categories and represents a concept related to the research phenomenon, which is either directly observable or an underlying element. Themes are essentially summary statements, causal explanations, or conclusions that offer an explanation as to why a phenomenon happens, what a phenomenon means, or how the participant feels about the phenomenon (Rubin & Rubin, 2012). A theme

normally shows the relationship between two or more concepts. Themes are thus more abstract concepts, reflecting the researcher's interpretation of patterns across the data.

Qualitative content analysis is a simple and useful resource tool. Content analysis determines the relations between perception and explanation of codes, categories, and themes derived from text data. I used content analysis to assess a journal article and in this descriptive case study. Prior to the analysis, I arranged the data to identify the common predicate offense typologies. I categorized the data into themes based on the content of the journal article and annual reports: the main focus of the journal article and annual reports was the types of money laundering and terrorist financing activities in the United States, while others examined the societal consequences and causes of the predicate offenses. After coding the data, I organized the codes into categories. I refined the categories in an iterative manner as I found interesting aspects in the data. I identified categories for the main predicate offense typologies. This categorization marked which journal articles presented the most significant insights into the evolving criminal processes and predicate offense typologies.

To recap the process, from codes, categories can be formed, and from categories, more encompassing themes are developed to describe the data in a form that summarizes it, yet retains the richness, depth, and context of the original data (Seers, 2011). Using quotations to illustrate both categories and themes helps keep the analysis firmly grounded in the data (Seers, 2011). The bigger categories of grouped, coded data are the overarching themes while sub-categories are supporting themes. As suggested by Seers (2011), I grouped similar codes into categories and identified a common theme amongst

those categories. The codes derived from the conceptual framework along with the emergent perceptions from the interview transcription, semistructured observation notes, and document reviews.

The codes emerged into categories which formulated certain themes. I was able to derive eight reoccurring main themes and four subthemes from the semistructured interviews, semistructured observations, and document review analysis. I outlined the codes associated with the categories along with the emergent main themes, see Table 3.

Table 3

Main Themes, Categories, and Codes for Semistructured Interview Data

Theme	Category	Code
Structuring	High volumes of small transactions	Cash deposits
		Cash withdrawals
		Multiple cash activities
		Split cash activity
		Different branch locations
		Below the reporting threshold
Fraud	Unusual customer behavior	Credit card
		PPP loan
		SBA loan
		Unusual wire activity
		Unemployment status
Cybercrime	Unusual customer behavior	Cryptocurrency
		Gift card
		Cyber laundering
		Telemarketing
		Romance scams
		Third party scams
		Digital payment systems
Human trafficking/smuggling	Trafficking	Credit card charges close to borders
		Cash in and out
		Redbox charges
		Hotel expenses
		Fast food charges
		Gas station charges
		Vending machine charges
		Late night charges
		Taxi/cab services
		Low dollar amount
		Quick money movement
Illicit arms trafficking	Trafficking	Weapons
		Firearms
Illicit drug trafficking	Trafficking	Substances
		Narcotics
		Drug cartel
Real estate money laundering	Real estate	Cash payments
		Overvaluation of property
		Undervaluation of property
		Housing market
		Shell companies
Trade-based money laundering	Trade-based	Over-or-under invoicing
		Goods
		Services
		International trade
		Quality misrepresentation

Note. PPP = Paycheck Protection Program; SBA = Small Business Administration.

I illustrated the codes associated with the categories along with the emerging subthemes for semistructured interview source, see Table 4.

Table 4

Subthemes, Categories, and Codes for Semistructured Interview Data

Theme	Category	Code
Red flags	Type of activity	Cash
		Wire
		Credit cards
		Prepaid cards
		Bitcoin
		Cryptocurrency
		Virtual currency
		Third party processors
		Automated clearing houses (ACHs)
		Transnational charges
		International large charges
		Excessive food, transport, and accommodations
		Big-ticketed item purchase or sale
		International shipping
Key indicators	Type of activity	Deposits
		Withdrawals
		Transfers
		Changes to customer profile
		New account openings
		Inconsistent wealth profile
		Unknown financial instrument use
95% or above	Quality	Quality assurance
		Quality control
		95%-100%
		High quality AML investigations

Note. AML = anti-money laundering.

I depicted the codes associated with the categories along with the emerging main themes for semistructured observation source, see Table 5.

Table 5

Main Themes, Categories, and Codes for Semistructured Observation Data

Theme	Category	Code
Structuring	High volumes of small transactions	Cash deposits
		Cash withdrawals
Fraud	Unusual customer behavior	Credit card
		PPP loan
		SBA loan

		Unusual wire activity
		Unemployment status
Cybercrime	Unusual customer behavior	Cryptocurrency
		Gift card
		Cyber laundering
		Telemarketing
		Third party scams
		Digital payment systems
Human trafficking/ Smuggling	Trafficking	Redbox charges
		Hotel expenses
		Fast food charges
		Late night charges
		Taxi/cab services
		Gas station charges
		Cash in and out
		Vending machine charges
		Quick money movement

Note. PPP = Paycheck Protection Program; SBA = Small Business Administration.

I displayed the codes associated with the categories along with the emerging subthemes for semistructured observation source, see Table 6.

Table 6

Subthemes, Categories, and Codes for Semistructured Observation Data

Theme	Category	Code
Typology-specific common signs	Type of typology	Structuring
		Fraud
		Cybercrime
		Trafficking
		Real estate
		Trade-based
95% or above	Quality	Quality assurance
		Quality control
		95%-100%
		High quality AML investigations

Note. AML = anti-money laundering

I portrayed the codes associated with the categories along with the emerging main themes for document review source, see Table 7.

Table 7

Main Themes, Categories, and Codes for Document Review Analysis Data

Theme	Category	Code
Structuring	High volumes of small transactions	Split cash activity Below the reporting threshold
Fraud	Unusual customer behavior	Credit card PPP loan SBA loan Unemployment status
Cybercrime	Unusual customer behavior	Cryptocurrency Cyber laundering Digital payment systems
Human trafficking/smuggling	Trafficking	Redbox charges Hotel expenses Fast food charges Late night charges Taxi/cab services Gas station charges
Illicit arms trafficking	Trafficking	Weapons Firearms
Illicit drug trafficking	Trafficking	Substances Narcotics
Real estate money laundering	Real estate	Housing market Shell companies Misvaluation of property
Trade-based money laundering	Trade-based	Inaccurate invoicing Goods Services

Note. PPP = Paycheck Protection Program; SBA = Small Business Administration.

I portrayed the codes associated with the categories along with the emerging subthemes for document review source, see Table 8.

Table 8

Subthemes, Categories, and Codes for Document Review Analysis Data

Theme	Category	Code

Red flags	Type of activity	Cash Wires Credit cards Virtual currency Third party processors Automated clearing houses (ACHs) International large charges
Key indicators	Type of activity	Deposits Withdrawals Transfers Changes to customer profile New account openings
95% or above	Quality	Quality assurance Quality control 95%-100% High quality AML investigations

Note. AML = anti-money laundering.

The data for the study was collected through the three data sources: semistructured interviews which resulted in a total of 15 completed interviews, semistructured observations, and document review analysis of the results of Clarke (2021), Mekpor (2019), Nizovtsev et al. (2022), five annual reports of Financial Action Task Force between 2018 to 2022 for current trends and typologies, and two articles generated by the Financial Crimes Enforcement Network. I used a comprehensive data analysis process to assess the information by using a hand-coding approach, thematic analysis, and content analysis. Finally, I used the results of the interview transcripts, observation notes, and document reviews to interpret the participants' experiences and expertise on predicate offense typologies and summarize their fundamental meanings.

Evidence of Trustworthiness

In terms of qualitative research study, an important criterion is ensuring trustworthiness which depends on the credibility and reliability of the study. As a

researcher, to establish trustworthiness and the integrity of the study, I took the following steps to warrant credible, transferable, dependable, and confirmable data.

Credibility

In qualitative research, different components develop the trustworthiness of the study including credibility. Credibility establishes whether the research findings represent plausible information drawn from the participants (Stewart & Hitchcock, 2016). First, to ensure credibility, I devoted adequate time to each participant during the interview process to obtain comprehensive knowledge of the case under investigation. Furthermore, I followed up with participants through a telephone call after each interview before beginning the data analysis process. Second, I validated the participants' responses during the data collection process. During each interview, I clarified the responses to certain questions by repeating the answers provided by the participants to confirm and clarify my understanding of their responses related to the question(s). Additionally, I implemented the member checking process prior to the data analysis process. After transcribing the interviews and reviewing the transcriptions, I emailed them along with my interview notes to the respective participants for member checking and to confirm my interpretation of their responses. Each participant provided their approval and or feedback. Third, once I reached the data saturation level, I captured the incidences that offer rich and thick data. Furthermore, I focused on emerging themes to notice repetition. Fourth, other techniques I used to ensure credibility were always protecting the participants' confidentiality and allowing the participants to discontinue their participation in the study at any time.

Transferability

An element of trustworthiness is transferability. Transferability is established by providing readers with evidence that the findings of the study could be applicable to other contexts, situations, times, and populations (Nowell et al., 2017). To ensure transferability of the study, I provided a detailed analysis of the participant selection, recruitment of participants, data collection, and the methods used to verify the information and ensure accuracy of the data collected. Transferability is achievable by validating the applicability of the research findings (Ravitch & Carl, 2016). To ensure transferability of this research study, I provided a detailed and thick analysis of the study allowing the reader to assess the conclusions drawn and its transferability to other contexts, situations, times, and populations. The detailed and thick description describes, in greater detail, the critical steps I took in this research study thus giving future researchers adequate information to assess the study. Last, I used triangulation to ensure the study was believable and transferable.

Dependability

In a qualitative research, dependability refers to the consistency of the results of a study over time (Fusch & Ness, 2015). It is the process of utilizing logical and consistent research methods and analysis. Dependability is essential to ensure the quality of the research conducted could be repeated and result in a similar outcome (Korstjens & Moser, n.d.). In this study, to ensure dependability, I used coherent procedures for participant selection, data collection, and data analysis to ensure that the protocols were reliable and aligned with appropriate methodology standards. For instance, I audio-

recorded all the interviews by using two different devices. Furthermore, I used the member checking process to verify that all the transcriptions and my interpretations accurately represent the participants' experiences and understanding of the concepts. Last, I used an audit trail by keeping raw data, interview notes, transcriptions, themes, findings, and conclusions to maintain the integrity of the data. Overall, I stored and kept all the collected data in secure locations for a period of at least five years.

Confirmability

The last element of trustworthiness is confirmability. Confirmability ensures that the data collected does not reflect the bias and preference of the researcher (Ravitch & Carl, 2016). It results from others corroborating that the outcome of the research is accurate and there is no bias presented that might distort findings. To ensure confirmability of this research study, I used triangulation of data. By using different methods of data collection including semistructured interviews, semistructured observations, and document reviews allowed me to engage in triangulation of the data to further validate the research results. By using triangulation of data, I warranted confirmability of the data collected and validation of the findings. Another method I used to ensure confirmability is an audit trail. I used an audit trail to demonstrate the results based on the participants' experiences and descriptions. I interpreted the participants' ideas and experiences without any bias. Moreover, I used member checking to eliminate any bias. Audit trails are a form of confirmability that allow the reader to substantiate the findings and draw conclusions from the data. As a researcher, I ensured the fundamental

connotations of trustworthiness to enhance the credibility of this qualitative descriptive case study and ensure validity of the findings.

Results of the Study

The data collected from the participants and documents was substantial and valuable information. The key findings derived from the interview questions, semistructured observations, and document reviews analysis aligned with the overarching RQ and four SQs. The overarching research question and four SQs were designed to identify predicate offense typologies that U.S. banking and financial services company compliance managers use to reduce the risks of money laundering and terrorist financing activities. In this section, the thematic findings are systematized by the overarching RQ and the four SQs. I aligned the categories and themes with the overarching RQ and four SQs amongst all the data sources, see Table 9.

Table 9

Alignment of Themes to Research Question and Subquestions

Research question	Interview theme	Observation theme	Document theme
RQ: What are the predicate offense typologies that U.S. banking and financial services company compliance managers identify to reduce the risks of money laundering and terrorist financing activities?	Structuring Fraud Cybercrime Human trafficking/smuggling Illicit arms trafficking Illicit drug trafficking Real estate money laundering Trade-based money laundering	Structuring Fraud Cybercrime Human trafficking/ smuggling	Structuring Fraud Cybercrime Human trafficking/smuggling Illicit arms trafficking Illicit drug trafficking Real estate money laundering Trade-based money laundering
S1: How do anti-money laundering investigators identify predicate offense typologies?	Red flags Key indicators	Typology-specific common signs	Red flags Key indicators Typology-specific common signs
S2: How successful are the investigators currently in identifying predicate offense typologies?	95% or above	95% or above	
S3: What characteristics classify money laundering and terrorist	Structuring Trafficking	Structuring Fraud	Structuring Fraud

financing as predicate offense typologies?	Cybercrime Real estate money laundering Trade-based money laundering	Cybercrime	Cybercrime Trafficking Real estate money laundering Trade-based money laundering
S4: How does identifying predicate offense typologies reduce money laundering and terrorist financing?	Red flags Key indicators	Typology-specific common signs	Red flags Key indicators

Triangulation of Data Sources

I collected data from semistructured interviews, semistructured observations, and document reviews. The interviews of 15 participants via an online videoconferencing platform consist of the majority of the data for this study. The semistructured interview consisted of 11 open-ended questions and follow-up questions to address the research participants' concerns. Notetaking during the semistructured interviews helped to capture the tone of each participant and provided an additional form of data. All the data sources mentioned in this study were utilized to ensure triangulation and establish credibility of participant responses and stated experiences. Each interview was transcribed and analyzed using the coding method to assign words or phrases to derive meaning from the collected data and thematic analysis to discover patterns and themes in the interpreted data. The semistructured observation notes and journal notes from the document reviews were coded in the similar manner as the interview transcripts. The initial coding process across all the data sources produced 90 codes that were reduced to 75 codes. The data analysis process resulted in five categories and eight main themes for the overarching RQ and four subthemes for the SQs.

The themes in relation to the literature review and conceptual framework address the overarching RQ and the four SQs. I presented the predicate offense typologies, the

total number of participants supporting the main themes from the interviews and observations, and the number of documents exemplifying the main themes from the document reviews, see Table 10.

Table 10

Main Themes, Supporting Participants, and Number of Documents

Main theme	No. of participants	No of documents
Structuring	15	3
Fraud	15	5
Cybercrime	14	4
Human trafficking/smuggling	15	5
Illicit arms trafficking	12	3
Illicit drug trafficking	13	5
Real estate money laundering	15	5
Trade-based money laundering	14	4

I provided a list of the subthemes, the total number of participants supporting the subthemes from the interviews and observations, and the number of documents exemplifying the subthemes from the document reviews, see Table 11.

Table 11

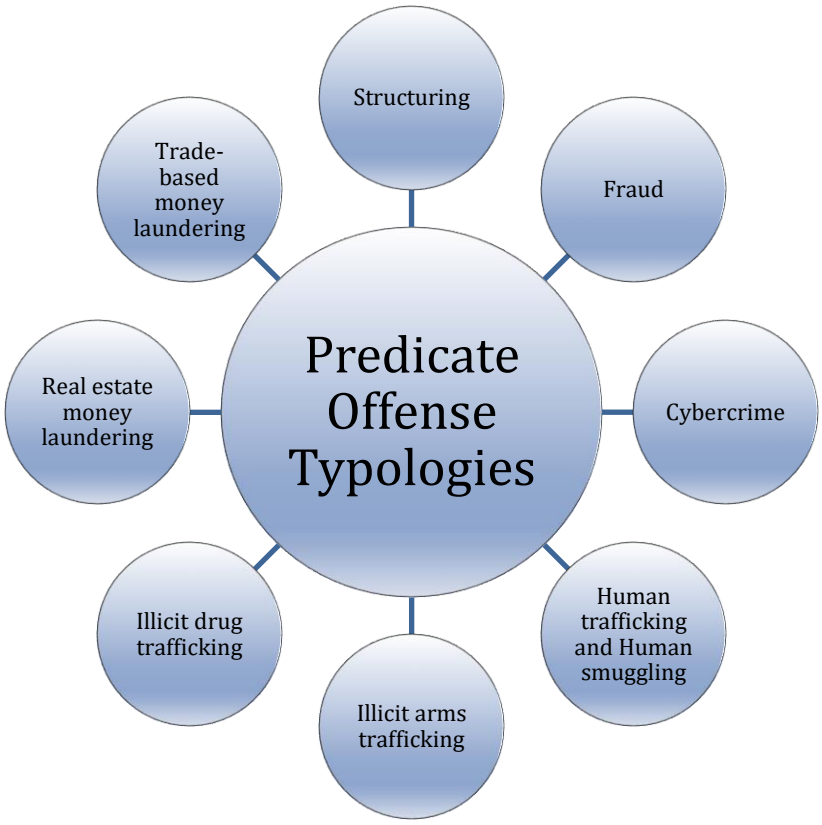
Subthemes, Supporting Participants, and Number of Documents

Subtheme	No. of participants	No. of documents
Red flags	15	7
Key indicators	15	7
Typology-specific common signs	15	5
95% or above	15	0

I depicted the predicate offense typologies identified by the research participants and document review analysis, see Figure 3.

Figure 3

Predicate Offense Typologies



Category 1: High Volumes of Small Transactions

The first emergent theme, structuring, addresses the RQs by presenting an evident rationalization of the research phenomenon. The codes for the theme were

- different branch locations
- multiple cash activities
- cash deposits
- cash withdrawals
- split cash activity

- below the reporting threshold

The research participants identified structuring as a common predicate offense typology that increases the risk of money laundering activities. During the document review, the following documents identified structuring as a predicate offense typology: Financial Action Task Force (2017), Financial Action Task Force (2018), and Financial Action Task Force (2020d). The theme was derived from the following six codes: different branch locations, multiple cash activities, cash deposits, cash withdrawals, split cash activity, and below the reporting threshold.

SQ1: Means by Which Anti-Money Laundering Investigators Identify Predicate Offense Typologies. Compliance managers and anti-money laundering investigators focus on certain red flags or indicators during anti-money laundering investigations to identify activities indicative of structuring. Participant 7 indicated that

> the key red flags or indicators of structuring are the following: (a) customer(s) tries to convince a bank teller not to file a currency transaction report, (b) customer(s) hesitates to provide personal information needed to file a currency transaction report, (c) customer(s) uses multiple automated teller machines at different locations to conduct deposits or withdrawals below the threshold, (d) customer(s) deposits proceeds into several accounts, [and] (e) customer(s) splits a large currency transaction by depositing or withdrawing funds a week apart below the threshold.

Essentially, the frequency, time, location(s), and amount of funds are key red flags or indicators of structuring activity. Often criminals open multiple small accounts to conduct

small amount transactions and launder illicit proceeds (Financial Action Task Force, 2017). Other key indicators of structuring are (a) small amount transactions, (b) numerous high-value transactions conducted in a newly opened or inactive account within a 24-hour window, and (c) irregular financial pattern (Financial Action Task Force, 2020d). The compliance managers and anti-money laundering investigators attested that the red flags and indicators, stated above, have proved to be successful strategies in identifying structuring activities during their investigations.

SQ2: Current Success Rate in Identifying Predicate Offense Typologies. A compliance strategy that has proven to be successful is red flag indicators. All research participants that were anti-money laundering investigators revealed that "their anti-money laundering investigations quality control rate is 95% or above with the use of red flags tailored to each predicate offense." Anti-money laundering investigators are successfully able to conduct high quality investigations by using a robust strategy to identify money laundering transactions. Banks and financial services institutions are obligated to deal with cybercrime threats.

SQ3: Money Laundering and Terrorist Financing Characteristics. Participant 8 defined structuring, also known as smurfing in the banking industry, "as the act of conducting a series of financial transactions including multiple deposits, withdrawals, or purchases of monetary instruments totaling $10,000.00 or less to avoid reporting requirements." Money launders structure transactions to avoid filing the currency transaction report (CTR) which is a reporting requirement established by the Bank Secrecy Act. Under the Bank Secrecy Act (31 USC 5324), an individual is prohibited to

structure transaction for the purpose of evading the currency transaction report or a geographical specific order reporting requirements (Halloran, 2020). The anti-money laundering programs at banks and financial services institutions due diligently investigate and attempt to mitigate the risk of structuring.

Participant 1 explained that "the characteristics of structuring as the act of performing one or more transactions (a) in cash totaling any amount, (b) at one more banks or financial services institutions, (c) on one or more days to evade the currency transaction report filing requirements." An example of structuring is when a money launder conducts a cash deposit in the amount of $5,000.00 on Thursday at Branch X and conducts another cash deposit in the amount of $3,500.00 the following Tuesday at Branch Y. According to the characteristics of structuring, the example above clearly illustrates this typology.

World events is an influential factor of money laundering and terrorist financing activities. Participant 11 explained that "the current globe events that occur in different parts of the world, largely influence, increase, and or decrease money laundering and terrorist financing activities in the banking sector." Money launders are continuously evolving their criminal skills and strategies to cultivate new ways to structure substantial amounts of cash to avoid the currency transaction report filing requirements. Evolved money launders are structuring through commercial entities and transferring funds through loan contracts (Financial Action Task Force, 2018). Structuring occurs during the second stage of money laundering which is layering. Layering is the act of transforming illicit profits derived from criminal activity into lawful forms of financial instruments

which generally involves some aspect of structuring (Al-Suwaidi & Nobanee, 2020). The research participants identified structuring as one of the most commonly reported predicate offense typology.

Category 2: Unusual Customer Behavior

Theme 2: Fraud

The second emergent theme, fraud, addresses the RQs by increasing awareness of the phenomenon. The codes for the theme were

- unusual wire activity
- credit card
- PPP loan
- SBA loan
- unemployment status

The research participants identified fraud as a predicate offense typology based on the experiences and expertise of compliance managers and anti-money laundering investigators employed at U.S. banks or financial services institutions. The following documents have identified fraud as a predicate offense typology: Nizovtsev et al. (2022), Financial Action Task Force (2020c), Financial Action Task Force (2017), Financial Crimes Enforcement Network (2021), and Financial Crimes Enforcement Network (2020e). One of the most common and largely producing predicate offense typology in the United States is fraud generating approximately $100 billion annually (Financial Crimes Enforcement Network, 2021). The theme was derived from the following five codes: unusual wire activity, credit card, PPP loan, SBA loan, and unemployment status.

SQ1: Means by Which Anti-Money Laundering Investigators Identify Predicate Offense Typologies. Types of predicate offenses include credit card fraud, unemployment fraud, and loan fraud.

***Credit Card Fraud*.** Illicit funds are commonly associated with payment card fraud. In 2020, 4,301 money mules were identified executing criminal crimes including fraud (Nizovtsev, 2022). Banks and financial services institutions use certain red flags and indicators to detect credit card fraud activities during anti-money laundering investigations. Participant 5 disclosed that

> some of the red flags or indicators of credit card fraud include but not limited to: (1) unusually large orders in comparison to the customer profile and historic monthly card statements, (2) multiple orders with same shipping address but charges on different credit cards and vice versa, (3) incorrect expiration date, (4) expediated shipping on large orders, (5) international shipping, (6) big-ticket items, (7) order for same product but in different colors or sizes, and many more.

The financial intelligence units at these U.S. banks and financial services institutions triage money laundering generated activities according to certain red flags and indicators. The red flags and indicators are a successful strategies that help anti-money laundering investigators identify and classify fraud activities. Participant 9 acknowledged that “as consumer purchasing habits alter, money launders and scammers are inventing new opportunities to target and con people into giving away their money.” Credit card fraud is rapidly becoming an emerging threat for society.

Unemployment Fraud. Unemployment fraud activity is occurring across multiple states. Many criminals employ exploitative schemes to take advantage of unemployment benefits from lawful businesses (Financial Crimes Enforcement Network, 2020). Banks and financial services institutions focus on certain red flags or indicators to detect incoming or outgoing funds derived from unemployment fraud activity. Participant 8 indicated that

> the red flags or indicators that help compliance managers detect unemployment fraud are the following: (1) the name on the account and the automated clearing house transaction does not match, (2) the total monthly deposits from unemployment exceed $5,000.00, (3) the customer receives unemployment funds from the issuing state which is different than the resident state, (4) the customer receives both unemployment deposits and payroll deposits concurrently, (5) funds deposited for unemployment benefit are quickly wired to foreign account(s) located in countries with inadequate anti-money laundering controls, and several others.

In recent times, a by-product of the Covid-19 pandemic is an increase in unemployment fraud activity that has escalated amongst U.S. banks and financial services institutions.

In 2021, there were about 557.4 million unemployment fraud claims nationally (Greszler, 2021). Greszler (2021) revealed that during the Covid-19 pandemic 18 out of every 10 unemployed individuals received unemployment benefits. The exceptional integration of federal funds unlocked doors to financial crime opportunities for criminals to exploit. The combination of easy accessibility to personal information and weakness in

the compliance frameworks of banks and financial services institutions allowed money launders to defraud financial systems.

***Loan Fraud*.** In 2020, PPP application fraud sought more than $5.5 million in loans (Financial Action Task Force, 2020c). Certain red flags and indicators helped compliance managers and anti-money laundering investigators detect loan fraud during anti-money laundering investigations. Participant 15 revealed that "(1) falsified information on a PPP loan application, (2) creating multiple PPP loan applications for multiple lenders, (3) inappropriate use of the PPP funds, (4) lying to federal agents during a PPP audit, and (5) failure to implement PPP compliance guidelines are substantial red flags or indicators of loan fraud activity." All the research participants agreed that "using red flags and indicators help them successfully identify fraud activities and analyze their investigation findings." The most successful and effective strategy is utilizing red flags and indicators in anti-money laundering and counter terrorist financing investigations.

SQ2: Current Success Rate in Identifying Predicate Offense Typologies. A compliance strategy that has proven to be successful is red flag indicators. All research participants that were anti-money laundering investigators revealed that "their anti-money laundering investigations quality control rate is 95% or above with the use of red flags tailored to each predicate offense." Anti-money laundering investigators are successfully able to conduct high quality investigations by using a robust strategy to identify money laundering transactions. Banks and financial services institutions are obligated to deal with cybercrime threats.

SQ3: Money Laundering and Terrorist Financing Characteristics. Several individuals became victims of credit card fraud executed by money launders. Credit card fraud is a type of identity theft. In other words, money launders steal credit card information of other individuals seeking to make purchases to the account or confiscate and or transfer funds to their account. A lack of customer due diligence on the financial institutions' part leads to identity theft. Financial institutions should assess the level of fraud risk against money laundering and terrorist financing risks to determine appropriate enhance due diligence measures (Financial Action Task Force, 2017). This process may mitigate any risk of fraud. Rashid et al. (2022) defined fraud as a criminal practice of gaining illicit funds through actions of deception or dishonesty and laundering the illegal funds into the financial system to conceal its illegitimate source. Due to the Covid-19 pandemic, all the research participants identified fraud as a common predicate offense typology in money laundering. The Financial Action Task Force categorized fraud along with other predicate offense typologies as a Covid-19-related crime (Financial Action Task Force, 2020c). Participant 2 indicated that "there are many different types of fraudulent financial activities that fall under the fraud umbrella." In money laundering, the different types of fraud include but are not limited to bank fraud, credit card fraud, unemployment fraud, loan fraud, securities fraud, tax fraud, and several others. Participant 4 revealed that "the Covid-19 pandemic caused an increase in credit card fraud, unemployment fraud, and loan fraud activities." An adverse consequence of the Covid-19 pandemic is credit card fraud.

A second type of fraud newly on the rise is unemployment fraud. The government has experienced a surge in fraudulent unemployment claims. Criminals are using stolen identities or their own identity to deceptively collect benefits of unemployment. Participant 10 presented an example in that "a criminal, also known as the claimant, will file for unemployment in their resident state whilst being employed in another state." In other words, criminals and money launders are simultaneously collecting financial benefits from unemployment claims and payroll.

In the midst of the Covid-19 pandemic, the United States government intervened to stabilize the economic environment. During this crisis, the Small Business Administration (SBA) created loan programs called the Economic Injury Disaster Loans (EIDLs) and the Paycheck Protection Program (PPP) to relieve small businesses from the detrimental financial impact of the Covid-19 pandemic. Lopez and Spiegel (2021) disclosed that in 2020, the nation-wide quarantine and work-from-home instructions jeopardized about 47% of total employment and 41% of private-sector payrolls. Thus, the Paycheck Protection Program lent forgivable loans to eligible businesses to help them stay in business by covering their operating expenses including payroll. The overall aim was to help businesses keep their labor force employed during the global Covid-19 crisis. The eligible businesses who received funds from the Paycheck Protection Program were obligated to follow specific procedures indicating specific means of allocating the funds.

Though, Participant 14 identified loan fraud as "the greatest scam that impaired America's economy." Schwellenbach and Summers (2021) indicated that the Justice Department filed criminal charges against 209 individuals totaling 119 cases related to

the Paycheck Protection Program fraud. Participant 3 explained that “the PPP loan fraud transpires when an individual or business submits a loan application with deceptive information for the purpose of obtaining funds from the federal PPP.”

Business claimed fake corporations, businesses, employees, tax documents, and payroll documentation to obtain funds from the Paycheck Payroll Program. Overall, the issue with the Paycheck Protection Program was a lack of anti-fraud measures and inadequate oversight. The Paycheck Protection Program was a federal effort to stabilize the U.S. economy after the worldwide pandemic. Yet, the government faces millions of dollars in losses caused by the pandemic loan fraud leading to criminal investigations.

Theme 3: Cybercrime

The third emergent theme, cybercrime, addresses the RQ by providing additional insight of a financial crime. The codes for the theme were

- romance scams
- telemarketing
- cyber laundering
- cryptocurrency
- third party scams
- gift card
- digital payment systems

The research participants identified cybercrime as a predicate offense typology based on the experiences and expertise of compliance managers and anti-money laundering investigators employed at U.S. banks or financial services institutions. During the

document review analysis, the following documents identified cybercrime as a predicate offense typology: Nizovtsev et al. (2022), Financial Action Task Force (2020), Financial Action Task Force (2020d), and Financial Crimes Enforcement Network (2021). The theme originated from the following seven codes: romance scams, telemarketing, cyber laundering, cryptocurrency, third party scams, gift card, and digital payment systems.

SQ1: Means by Which Anti-Money Laundering Investigators Identify Predicate Offense Typologies. Financial Crimes Enforcement Network (2021) conveyed red flags that can help banks and financial services institutions to identify and prevent cybercrime. According to the compliance managers and anti-money laundering investigators, cybercrime exhibit "red flag" characteristics that help them detect and avert money laundering activities and augment their compliance performance. Participant 12 and Participant 13 disclosed that

> the red flags of cybercrime include but are not limited to (1) parties conducting online transactions high risk jurisdictions, (2) numerous payments using prepaid cards or cryptocurrency including Bitcoin, (3) new accounts receiving large deposits or conducting large transactions that are inconsistent with the customer's transactional behavior, profile, and account history, (4) large volumes of unusual online transactions, (5) illegitimate charitable organizations using email or social media solicitation schemes, and (6) suppliers sending correspondence to customers with misspellings or incorrect addresses.

Anti-money laundering investigators rely on red flags to identify cybercrime activities.

Universally, red flags for cybercrime are often related to cyber-related scams including email, SMS phishing schemes, business email compromise scams, and ransomware attacks (Financial Action Task Force, 2020). Other red flags or indicators include (a) unknown source of funds, (b) insufficient information on the owner and beneficiary of the funds transfer, (c) funds transfer to or from online gambling services, (d) large amounts of fiat currency, and (e) multiple use of credit or debit cards (Financial Action Task Force, 2020d). Red flags and indicators significantly aid banks and financial services institutions to detect fraudulent activities.

SQ2: Current Success Rate in Identifying Predicate Offense Typologies. A compliance strategy that has proven to be successful is red flag indicators. All research participants that were anti-money laundering investigators revealed that "their anti-money laundering investigations quality control rate is 95% or above with the use of red flags tailored to each predicate offense." Anti-money laundering investigators are successfully able to conduct high quality investigations by using a robust strategy to identify money laundering transactions. Banks and financial services institutions are obligated to deal with cybercrime threats.

SQ3: Money Laundering and Terrorist Financing Characteristics. In the 21st century, money lauders and terrorist largely rely on technological advancements to execute their financial crime plans or conduct criminal activities. The new age technological advancements have allowed criminals to use the internet for laundering purposes. Thus, cybercrime is defined as the use of cyberspace to facilitate criminal acts including money laundering, fraud, identity theft, and several others (Wronka, 2022).

Cybercrime is classified as a predicate offense in money laundering because it produces illicit funds that need to be concealed by laundering prior to entering into the legal financial system. Criminals use computer technology to conceal the traces of illegal funds across geographical jurisdictions and borders (Nizovtsev et al. (2022). Participant 6 informed me that "the European Union's 6th Anti-Money Laundering Directive identified and categorized cybercrime as a money laundering predicate offense." The Financial Crimes Enforcement Network vigilantly attempted to respond to new emerging cybercrime threats during the global pandemic.

Category 3: Trafficking

Theme 4: Human Trafficking and Human Smuggling

The fourth emergent theme, human trafficking and human smuggling, addresses the RQ by presenting evidence related to the concepts. The codes for the theme were

- hotel expenses
- fast food charges
- gas station charges
- taxi/cab services
- credit card charges close to borders
- Redbox charges
- quick money movement
- cash in and out
- low dollar amount
- vending machine charges

- Late night charges

The research participants identified human trafficking and human smuggling as a predicate offense typology based on the experiences and expertise of compliance managers and anti-money laundering investigators employed at U.S. banks or financial services institutions. The following documents identified human trafficking and or human smuggling as a predicate offense typology: Mekpor (2019), Financial Action Task Force (2019), Financial Action Task Force (2020d), Financial Crimes Enforcement Network (2020), and Financial Crimes Enforcement Network (2021). Financial Action Task Force (2020d) indicated that human trafficking is one of the most common type of predicate offense typology misused by criminals. The theme was drawn from the following 11 codes: hotel expenses, fast food charges, gas station charges, taxi/cab services, credit card charges close to borders, Redbox charges, quick money movement, cash in and out, low dollar amount, vending machine charges, and late-night charges. Human trafficking and human smuggling is a predicate offense typology that generates large amounts of income for criminals (Mekpor, 2019) The end goal of any business is a profitable bottom line. Financial Crimes Enforcement Network (2021) reported that one of the highest lucrative criminal business in the United States is human trafficking and human smuggling. Human trafficking and human smuggling are often performed through forced labor, organ removal and sexual exploitation (Financial Crimes Network Enforcement, 2020). No one indicator alone helps to identify human trafficking and or human smuggling.

SQ1: Means by Which Anti-Money Laundering Investigators Identify Predicate Offense Typologies. A best practice that compliance managers and anti-

money laundering investigators employ to identify traces of human trafficking is red flags. Participant 3, Participant 7, and Participant 14 indicated that

> "these red flag indicators include: (1) patterns of credit card charges between 10pm-6am, (2) large deposits and immediate withdrawals in cities near country borderlines, (3) several victims with same bank account information including emails, social media handle, phone numbers, or addresses, (4) unexpected changes in account activity from customer's profile, (5) use of unknown financial instruments such as prepaid cards or cryptocurrency to pay bills, (6) cash deposits with no automated clearing house withdrawals, (7) customer attempts to avoid reporting requirements, and (8) the use of third-party payment systems that disguise the originators and beneficiaries of the transaction."

Financial Action Task Force (2018) mentioned that to identify financial transactions related to this predicate offense typology are (a) excessive accommodations and vacationing expenses, (b) substantive transportation expenses (airline tickets, taxi fares, train tickets, etc.), and (c) unusual consumer financial behavior. These red flags are some signs that point to human trafficking activity.

Forced Labor. Human traffickers often recruit victims by presenting an incentive of profitable or better paying jobs abroad. Participant 2 explained that "after recruitment, human traffickers force victims into work through various tactics including violent behavior, coercion, confiscation of identity papers, or threats of disclosure to immigration authorities." Human trafficking in the form of forced labor is categorized as modern

slavery. In some cases, the victims receive a minimal amount of wage or no wage for their work. Participant 4 disclosed that

> probable red flags of human trafficking associated with forced labor include: (1) a single bank account used to make payroll payments to several employees, (2) income deposited into a single account and immediately withdrawn or transferred into an account to another account, and (3) a person who handles or controls the finances and official documents of an individual when dealing with government or regulatory officials.

Another form of human trafficking is organ removal.

Organ Removal. Human traffickers will recruit victims for the sole purpose of organ removal. This process tends to involve complex logistics and economic structure. It comprises of several involved parties including medical services. Participant 7 revealed that "according to the Financial Action Task Force, organ removal is classified as a less common form of human trafficking but nevertheless endangers the victims." There are two types of financial opportunities from organ removal: (a) infrastructure funds and (b) funds to compensate people involved in the offense. An example of infrastructure funds involves coordinating for medical accommodations and resources with unaccredited medical organizations. Furthermore, funds to compensate people involved in the offense is paying surgeons, medical staff, and agents who employ victims and coordinate logistical details. Participant 1 revealed that "human traffickers can substantially profit from a single organ removal. For example, the price of removing kidneys is about $200,000 in certain markets." Sadly, criminals profit by forcing or paying victims to

remove their organs. Yet, the most inhumane form of human trafficking is sexual exploitation.

Sexual Exploitation. Criminals of human trafficking sexual exploit victims on a continuing basis for profit. Sexual exploitation is the act of coercing victims into prostitution over a prolonging period of time. A key element to detecting human trafficking for sexual exploitation is that human traffickers must offer the basic welfare necessities of their victims. For example, sexual exploitation victims are provided with food, accommodation, and transport. Thus, by using red flag indicators, this type of human trafficking activity is identifiable by following the money in bank accounts. Participant 5, Participant 8, Participant 11, and Participant 13 shared that

> the red flag indicators for human smuggling are: (1) excessive expenses for food, transport and accommodation, (2) virtual currency transactions or money transfers, (3) cell phone numbers associated with escort service marketing instruments, and (4) bank accounts with excessive cash deposits that are inconsistent with the customer's wealth profile.

In the effort to fight against human trafficking for sex exploitation, firms are relying heavily on red flag indicators to identify this predicate offense typology and stop offenders from conducting this crime.

Banks and financial services institutions have the utmost responsibility to detect individuals or businesses receiving unusually large amounts of money which are inconsistent with the customer's employment profile and historical wage activity. Since human trafficking is a predicate offense to money laundering, the financial red flags also

may be indicative of human smuggling. The Financial Crimes Enforcement Network advises firms to use red flags to detect this predicate offense typology but avoid focusing on a particular red flag. A single red flag is not a clear indication of human trafficking, though each red flag can help identify human trafficking or human smuggling activity (Financial Crimes Enforcement Network, 2020). It is imperative that banks and financial services institutions take into consideration additional factors such as a customer's historic financial activity and the current predicate offense typologies or other red flag indicators when conducting anti-money laundering investigations on transactions that might be correlated with human trafficking.

SQ2: Current Success Rate in Identifying Predicate Offense Typologies. A compliance strategy that has proven to be successful is red flag indicators. All research participants that were anti-money laundering investigators revealed that "their anti-money laundering investigations quality control rate is 95% or above with the use of red flags tailored to each predicate offense." Anti-money laundering investigators are successfully able to conduct high quality investigations by using a robust strategy to identify money laundering transactions. Banks and financial services institutions are obligated to deal with cybercrime threats.

SQ3: Money Laundering and Terrorist Financing Characteristics. Money launders have been trafficking human beings and smuggling immigrants for decades. Human trafficking is the criminal act of recruiting vulnerable humans by duress, scam, or force and exploiting them for financial gains (Onufer, 2022). Human trafficking is classified into three categories: (a) forced labor, (b) removal of organs, and (c) sexual

exploitation (Financial Action Task Force, 2018). Whereas human smuggling is the criminal act of transporting unauthorized aliens to or into the United States (Financial Crimes Enforcement Network, 2020). Perpetrators will transport victims between different locations within a country or across international borders. Unlike human smuggling, human trafficking does not require physical movement. Human traffickers tend to exploit a person within the borderlines of a country or the walls of a victim's own home.

These criminals use money laundering to convert their illicit financial income into lawful proceeds. Human trafficking and human smuggling are high-risk and challenging predicate offenses to detect and follow the money because the capital flows from human trafficking and human smuggling are diverse. Thus, the financial intelligence units rely on a range of financial red flags to better position their anti-money laundering investigations to identify human trafficking and human smuggling.

Theme 5: Illicit Arms Trafficking

The fifth emergent theme, illicit arms trafficking, addresses the RQ by highlighting and identifying a key financial crime risk associated with the phenomenon. The codes for the theme were weapons and firearms. The research participants recognized illicit arms trafficking as a predicate offense typology based on the experiences and expertise of compliance managers and anti-money laundering investigators employed at U.S. banks or financial services institutions. Mekpor (2019), Financial Action Task Force (2020), and Financial Crimes Network Enforcement (2021)

identified illicit arms trafficking as a predicate offense typology. The theme originated from two codes including weapons and firearms.

SQ1: Means by Which Anti-Money Laundering Investigators Identify Predicate Offense Typologies. Participant 9 explicated that "to detect the financial aspect of illicit arms trafficking activity, it is necessary for banks and financial services institutions to closely work with law enforcement and customs and border control agencies." The process of tracing of illicit arms trafficking is a systematic process. Participant 6 indicated that "the flow of funds produced from illicit arms are complex to detect in the financial systems because this predicate offense typology lacks a legal flow." The country in which the illicit arms are originated for transportation purposes differs from the country in which the illicit arms are converted to legal funds. U.S. agencies have detected U.S.-based individuals who launder money to support overseas violence (Financial Crimes Network Enforcement, 2021). These individuals' travel expenses to foreign and high-risk jurisdictions is a key indicator of illicit arms trafficking. Another red flag to detect illicit arms trafficking using bitcoin to purchase firearms (Financial Crimes Network Enforcement, 2020). Law enforcement should invest their time and energy on shipping details to detect illicit arms trafficking activity.

SQ2: Current Success Rate in Identifying Predicate Offense Typologies. A compliance strategy that has proven to be successful is red flag indicators. All research participants that were anti-money laundering investigators revealed that "their anti-money laundering investigations quality control rate is 95% or above with the use of red flags tailored to each predicate offense." Anti-money laundering investigators are

successfully able to conduct high quality investigations by using a robust strategy to identify money laundering transactions. Banks and financial services institutions are obligated to deal with cybercrime threats.

SQ3: Money Laundering and Terrorist Financing Characteristics. Amjad et al. (2021) reported that $10 billion are generated from the sale of illicit arms trade. Illicit arms trafficking is the criminal act of trading and transporting small arms, guns, weapons, and ammunition from a legal to illegal market (Weigand, 2021). The main risk associated with arms trafficking is the power that a trafficker has to amplify the detrimental impact to the buyer who purchases illicit weapons. Participant 1 mentioned that "contrary to illicit trades in drug trafficking or counterfeit goods, illicit arms trafficking tends to generate little money and requires less involvement of individuals or groups who enact as purchasers or traffickers." Perpetrators find it easy to disguise and transport small arms and weapons. Criminals use money mules better known as cash couriers to transport illicit arms across country borders (Mekpor, 2019). The underlying purpose illicit arms trafficking is to launder income generated from this predicate offense and fund terrorist acts. Thus, illicit arms trafficking is a lucrative business which, in turn, promotes and finances other types of predicate offense typologies.

Overall, arms trafficking can have a detrimental, political and societal impact. The arms traffickers have the ability to involve and promote political violence or organized crime by distributing weapons. History typically repeats itself as gun violence and massacres occur again and again carried out by an individual or small group of people using powerful firearms.

Theme 6: Illicit Drug Trafficking

The sixth emergent theme, illicit drug trafficking, addresses the RQ by explaining an example of a key concept discussed in the literature review. The codes were substances, narcotics, and drug cartel. The research participants classified illicit drug trafficking as a predicate offense typology based on the experiences and expertise of compliance managers and anti-money laundering investigators employed at U.S. banks or financial services institutions. The documents that identified illicit drug trafficking as a predicate offense typology are the following: Clarke (2021), Nizovtsev et al. (2022), Financial Action Task Force (2020b), Financial Action Task Force (2020d), and Financial Crimes Enforcement Network (2021). One of the many predicate offenses that produces bulk of illegal profits in the United States is drug trafficking (Financial Crimes Enforcement Network, 2021). The theme was derived from three codes including substances, narcotics, and drug cartel.

SQ1: Means by Which Anti-Money Laundering Investigators Identify Predicate Offense Typologies. Compliance managers and anti-money laundering investigators employ strategies to detect illicit drug trafficking activities. A best practice is to use red flags during anti-money laundering investigations to identify financial activity related to drug trafficking. Participant 10 revealed that “it is difficult to trace back the source of funds once drug traffickers transform illegal profits into clean money.” Although, drug traffickers do exploit funnel accounts to convert dirty money derived from illegal activities into legal proceeds. Participant 10 and Participant 12 shared that

> the red flag indicators for funnel accounts include (1) multiple deposits and immediate withdrawals or transfers, (2) low balance accounts with large cumulative dollar deposit activity, (3) deposits from multiple individuals, companies, and locations, (4) multiple deposits from different sources, (5) unusual account activity, (6) interstate and intrastate cash deposits and withdrawals, (7) wire transfers to high-risk jurisdictions, (8) purchases of high-valued good, (9) unusual cross-border transfer to the same person, (10) frequent foreign currency exchange transactions, (11) import and export transactions with limited information, and (12) transactions conducted with foreign nationals.

Compliance managers and anti-money laundering investigators refer to these red flags for guidance purposes. Other red flags indicative of drug trafficking include the (a) use of message fields in the language of virtual assets, (b) a customer repeatedly conducts transactions through subset of individuals, (c) unusual significant online transactions, (d) funds remitted to offshore accounts, and (e) purchase and export of high-end electronic devices (Financial Action Task Force, 2020b; Financial Action Task Force, 2020d). Any of these financial red flags may appear suspicious on their own. Though, an amalgamation of these red flags in addition to an investigation of the overall account activity and client profile may indicate drug trafficking activity.

SQ2: Current Success Rate in Identifying Predicate Offense Typologies. A compliance strategy that has proven to be successful is red flag indicators. All research participants that were anti-money laundering investigators revealed that “their anti-money laundering investigations quality control rate is 95% or above with the use of red

flags tailored to each predicate offense." Anti-money laundering investigators are successfully able to conduct high quality investigations by using a robust strategy to identify money laundering transactions. Banks and financial services institutions are obligated to deal with cybercrime threats.

SQ3: Money Laundering and Terrorist Financing Characteristics. Drug trafficking is a major revenue producing source for criminals, money launders, and organized crime groups. Drug trafficking is a worldwide black market that allows perpetrators to conduct illegal trades of prohibited substances for monetary gains (Namli, 2021). Clarke (2021) mentioned that historically many predicate offenses such as drug trafficking heavily utilized cash at the placement stage of money laundering. Criminals rather converted laundered proceeds into cash to disguise their tracks instead of depositing cash into financial institutions. Clarke (2021) revealed that drug gangs exploited the weak anti-money laundering controls of HSBC causing the bank to face a $1.9 billion fine. Perpetrators started using payment cards to launder criminally obtained funds from drug trafficking (Nizovtsev et al., 2022). The overarching theme is exploiting the supply chain used to smuggle drugs and launder criminal proceeds. The Covid-19 pandemic profoundly affected drug trafficking activity. Regulators anticipated that the travel restrictions due to the Covid-19 pandemic will decrease drug trafficking activity. Yet, law enforcement agencies confiscated greater amounts of illegal substances in comparison to historical data (Campedelli et al., 2020). Thus, drug traffickers strive to convert monetary proceeds, earned from illegal activities, into legal income sources

(Clarke, 2021). The manufacture, sale, transportation, and distribution of illicit drug trafficking has cultivated into a global phenomenon.

Category 4: Real Estate

Theme 7: Real Estate Money Laundering

The seventh emergent theme, real estate money laundering, addresses the RQ by summarizing a key finding related to the research topic. The research participants categorized real estate money laundering as a predicate offense typology based on the experiences and expertise of compliance managers and anti-money laundering investigators employed at U.S. banks or financial services institutions. Real estate money laundering was identified as a predicate offense typology in the following documents: Clarke (2021), Mekpor (2019), Financial Action Task Force (2020a), Financial Action Task Force (2020c), and Financial Crimes Enforcement Network (2020). The theme was derived from five codes, which are housing market, shell companies, overvaluation of property, undervaluation of property, and cash payments.

SQ1: Means by Which Anti-Money Laundering Investigators Identify Predicate Offense Typologies. Real estate money laundering occurs in numerous ways, so it is fundamental that compliance managers and anti-money laundering investigators focus on know your customer procedures. These protocols include conducting due diligence, identifying red flags, and reporting any suspicious activity. Participant 1 mentioned that

> the red flags indictive of real estate money laundering include: (1) unknown buyers, (2) all-cash payment from various different back accounts, (3)

overvaluation or undervaluation of property to fluctuate prices, (4) the use of shell companies, and (5) inconsistency between customer's income and value of property.

Compliance managers are gatekeepers who have the utmost responsibility to conduct customer due diligence to identify any red flag indicators that may detect real estate money laundering activities.

SQ2: Current Success Rate in Identifying Predicate Offense Typologies. A compliance strategy that has proven to be successful is red flag indicators. All research participants that were anti-money laundering investigators revealed that "their anti-money laundering investigations quality control rate is 95% or above with the use of red flags tailored to each predicate offense." Anti-money laundering investigators are successfully able to conduct high quality investigations by using a robust strategy to identify money laundering transactions. Banks and financial services institutions are obligated to deal with cybercrime threats.

SQ3: Money Laundering and Terrorist Financing Characteristics. Several money laundering methods exist, but criminals discover new money laundering strategies based on current social and economic conditions. Money launders use goods and services to place, layer, and integrate illegal proceeds into the legal financial system (Bieler, 2022). One of the most common, modern, and emerging methods of money laundering is real estate (Mekpor, 2019). Launders and terrorists target distress and vulnerable businesses such as the real estate market (Financial Action Task Force, 2020c). The real estate sector is subject to rapid changes and growing amounts of money that circulate

throughout the financial system. Criminals exploit and invest in real estate to produce cash and disguise criminal proceeds (Financial Action Task Force, 2020a; Financial Crimes Enforcement Network). Similar to goods, real estate is a preferred market for criminals because large amounts of money changes numerous hands in a single deal. It is a predicate offense typology that uses different methods to covert dirty money into clean money (Clarke, 2021). The American dream of owning a home with a white picket fence provides the homeowner with many rewards; remarkably, these same advantages cause real estate to be an alluring method for money laundering. Overall, banks and financial services institutions need to ensure their compliance departments are demonstrating robust anti-money laundering screening and compliance procedures.

Category 5: Trade-Based Money Laundering

Theme 8: Trade-Based Money Laundering

The eighth emergent theme, trade-based money laundering, addresses the RQ by exemplifying a type of financial crime and supporting the conceptual framework. The research participants identified trade-based money laundering as a predicate offense typology based on the experiences and expertise of compliance managers and anti-money laundering investigators employed at U.S. banks or financial services institutions. Trade-based money laundering was classified as a predicate offense typology in the following documents: Financial Action Task Force (2018), Financial Action Task Force (2020a), Financial Action Task Force (2020b), and Financial Crimes Enforcement Network (2021). The theme originated from four codes: goods, services, over-or-under invoicing, and international trade.

SQ1: Means by Which Anti-Money Laundering Investigators Identify Predicate Offense Typologies. An effective strategy to identify predicate offense typologies is using red flag indicators. Participant 2 revealed that

> the red flags of trade-based money laundering activities includes: (1) payments exceeding the value of commodities, (2) shipment of commodities with greater value, (3) unusual third-party payments to importers, (4) use of shell or front companies, (5) transfer pricing, (6) inaccurate description of goods, (7) customer's inability to generate appropriate documentation, (8) falsification of the quality of goods, (9) implicit course of shipment and financial transactions, (10) large transactions that are inconsistent with business profile and historical account activity, and (11) last-minute changes to payment methods by trading companies.

Trade-based money laundering occurs in various sectors. Criminals commonly target the following types of trade-based products: auto parts and vehicles, agricultural products, clothing, electronics, gold, precious metals, and textiles. The key indicators amongst sectors to identify trade-based money laundering are (a) products with wide pricing margins, (b) shipments across several jurisdictions, and (c) goods causing difficulties for custom authorities (Financial Crimes Enforcement Network, 2021). Numerous red flags and key indicators help to identify and uncover trade-based money laundering activities and techniques.

SQ2: Current Success Rate in Identifying Predicate Offense Typologies. A compliance strategy that has proven to be successful is red flag indicators. All research participants that were anti-money laundering investigators revealed that "their anti-

money laundering investigations quality control rate is 95% or above with the use of red flags tailored to each predicate offense." Anti-money laundering investigators are successfully able to conduct high quality investigations by using a robust strategy to identify money laundering transactions. Banks and financial services institutions are obligated to deal with cybercrime threats.

SQ3: Money Laundering and Terrorist Financing Characteristics. The global pandemic caused an economic crisis leading to an increase in trade-based money laundering. Trade-based money laundering is defined as the criminal of act of concealing and legalizing the illicit funds by exploiting trade to change the value of transactions (Financial Action Task Force, 2020b). In the process of conducing trade-based money laundering, perpetrators may employ other predicate offense activities.

The general purpose of trade-based money laundering is not focused on the movement of goods, but rather the movement of money which is implemented through trade transactions. Currency exchange services act as money brokers in trade-based money laundering schemes. Covered institutions are targeted by money launders. The goal of trade-based money launders is to produce profits and transmit funds through gatekeepers, front or shell companies, exchange houses, or the illicit exploitation of international trade (Financial Crimes Enforcement Network, 2021). The types of trade-based money laundering activities include falsifying invoices and shipping documents, inaccurately marking goods to evade controls, and violating customs and tax protocols (Financial Action Task Force, 2018). Banks and financial services institutions need to

identify red flags, assess their risk factors, and understand their compliance framework to detect trade-based money laundering activities.

Participant 4 mentioned that “though banks may learn to detect trade-based money laundering activities by using red flag indicators, the real challenge lies in the range of compliance risks.” These compliance risks are understanding pricing and goods, licensing, document verification, circumvention, and paper transactions. Criminals take advantage of the complexity of international trading systems by enhancing their methodologies. A decline in global trade volumes resulted in international organized crime schemes. Money launders are exploiting the global supply chains to funnel illegal funds (Financial Action Task Force, 2020a). The complexity of trading systems mainly involves multiple parties and jurisdictions. Therefore, it becomes complex for compliance managers to conduct know your customer, customer due diligence, and anti-money laundering checks during their investigations. Trade-based money laundering is one of the most concerning predicate offense typology.

SQ4: Reduction in Money Laundering and Terrorist Financing Due to Identification of Predicate Offense Typologies. The ability to identify predicate offense typologies help reduce money laundering and terrorist financing. Recognizing predicate offense typologies is a necessary skill for any U.S. banking and financial service company compliance manager to effectively fight against money laundering and terrorist financing activities and ensure regulatory compliance. Participant 4 revealed that “predicate offense typologies show numerous procedures, techniques, methods, and instruments criminals use to disguise, launder, or move illegal proceeds.” Predicate

offense typologies are largely influenced by the economy, financial markets, and anti-money laundering and counter terrorist financing programs. Participant 9 stated that "identifying predicate offense typologies help compliance managers develop sets of red flags and indicators specific to each predicate offense typology." Through this process, compliance managers can understand consumer behavior and recognize transactional patterns. Participant 2 indicated that "compliance managers are able to monitor sudden changes in customers' transaction patterns especially high-risk jurisdiction transactions." It gives compliance managers the ability to effectively detect and address money laundering and terrorist financing activities infiltrating into their financial institutions. Criminals are constantly evolving their methods and means to execute money laundering and terrorist financing activities. The identification of predicate offense typologies reduces money laundering and terrorist financing by enhancing due diligence and ensuring updated consumer risk profile (Federal Financial Institutions Examination Council, 2021; Financial Action Task Force, 2017). By developing a list of predicate offense typologies, compliance managers are able to ensure a robust and secure compliance framework by assuring adequate anti-money laundering programs, achieving institutional compliance regulations, safeguarding the financial systems, and placing preventative measures.

Summary

Chapter 4 demonstrates an overview of the data collection process, data analysis, and the results of the study. The purpose of this qualitative descriptive case study was to identify predicate offense typologies that U.S. banking and financial services company

compliance managers use to reduce the risks of money laundering and terrorist financing activities. The overarching RQ and four SQs underpinned this research study. The goal was to address the overarching RQ and the four SQs. The overarching RQ was, What are the predicate offense typologies that U.S. banking and financial services company compliance managers identify to reduce the risks of money laundering and terrorist financing activities? The four SQs were

SQ1. How do anti-money laundering investigators identify predicate offense typologies?

SQ2. How successful are the investigators in identifying predicate offense typologies?

SQ3. What characteristics classify money laundering and terrorist financing as predicate offense typologies?

SQ4. How does identifying predicate offense typologies reduce money laundering and terrorist financing?

The research design was descriptive case study; thus, to analyze the data I used a qualitative software for coding, and thematic analysis and content analysis to identify patterns in a shared phenomenon that transcends individual experience (Burkholder et al., 2016). The results yielded the following main themes: (a) structuring, (b) fraud, (c) cybercrime, (d) human trafficking and smuggling, (e) sex exploitation, (f) illicit arms trafficking, (g) illicit drug trafficking, (h) real estate money laundering, and (i) trade-based money laundering. The identified subthemes were (a) red flags, (b) key indicators, (c) typology-specific common signs, and (d) 95% or above. Furthermore, the results from

the 15 participants and document review analysis provided extensive knowledge of the principles of money laundering and terrorist financing and the predicate offense typologies identified and used by compliance managers to reduce the risks of money laundering and terrorist financing activities. Chapter 5 will present an interpretation of the findings, conclusions, limitations, recommendations, and implications for social change.

Chapter 5: Discussion, Conclusions, and Recommendations

Introduction

The purpose of this qualitative descriptive case study was to identify predicate offense typologies that U.S. banking and financial services company compliance managers use to reduce the risks of money laundering and terrorist financing activities. I used a descriptive case study design because of the nature of the RQs. By using this design, I was able to explore the phenomenon through participants' experiences, actions, behaviors, and perspectives. I collected data from compliance managers and anti-money laundering investigators. I gathered data from multiple sources including semistructured interviews, semistructured observations, and document reviews. The key findings from the study are summarized into eight main themes and four subthemes. The eight emergent themes were the following: (a) structuring, (b) fraud, (c) cybercrime, (d) human trafficking and smuggling, (e) illicit arms trafficking, (f) illicit drug trafficking, (g) real estate money laundering, and (h) trade-based money laundering. The four subthemes were the following: (a) red flags, (b) key indicators, (c) typology-specific common signs, and (d) 95% or above. In this chapter, I will discuss the interpretation of findings, limitations of the study, recommendations, and implications for social change.

Interpretation of Findings

Amid increasing globalization, financial crimes continue to rise making it difficult for banks and financial services institutions to detect criminal activities. Socioeconomic factors largely influence financial crimes across the globe. The interconnectedness of people, goods, services, finance, and technology is a leading cause of money laundering

and terrorist financing activities (Amjad et al., 2021). Since its declaration in early 2020, the Covid-19 pandemic has caused a fluctuation in money laundering and terrorist financing activities. Criminals and terrorists took advantage of this global crisis and quickly adapted to the new environment. Money launders organized crime groups to conduct new Covid-19 related illegal activity. These money launders targeted vulnerable businesses on the verge of bankruptcy (Financial Action Task Force, 2020a). Terrorists used financial sanctions and economic interruptions to disrupt supply chains and compliance systems (Fletcher et al., 2021). They utilized illicit proceeds as liquidity to purchase real estate sold due to financial vulnerability or economic despair (Financial Action Task Force, 2020c). The global lockdown had a negative effect on businesses resulting in a great degree of unemployment, dismissal of employees, loss of government revenue, and a widespread economic recession that affected businesses and individuals' financial and social behavior.

In the literature review, I discussed how the banking and financial services industries are subject to intricate regulatory regulations. These institutions are responsible to oblige to federal and state regulations developed by oversight bodies and legislation. One intergovernmental regulator is the Financial Action Task Force, which is primarily responsible for analyzing and combating financial crimes. The Financial Action Task Force focuses on detecting and exploiting potential threats of financial crimes executed by criminals and terrorists. Based on the current global financial crimes trends, this organization provides recommendations acknowledged as the global anti-money laundering and counter terrorist financing standard. A recommendation made by the

Financial Action Task Force to banks and financial services institutions was to focus their efforts on detection, prevention, and suppression to combat money laundering and terrorist financing activities (Financial Action Task Force, 2018). The recommendations made by the Financial Action Task Force is a set of measures to identify and counter money laundering and terrorist financing threats. To identify and counter money laundering and terrorist financing threats, it is important to understand the criminal mind and behavior.

To understand the criminal mind, it is necessary to refer to the economic theory of criminal behavior developed by Gary Becker (1968). This theory explains one aspect of the economic and criminological analysis of financial crimes. The economic theory of criminal behavior is well known in science and a foundational aspect in the development of global collaboration in the fight against money laundering and terrorist financing. Another possibly more meaningful view of the economic and criminological essence of money laundering and terrorist financing, is the recognition of predicate offense typologies (Rusanov & Pudovochkin, 2021). The ability to identify predicate offense typologies helps compliance managers to detect money laundering and terrorist financing activities. By understanding the financial mechanism of crime, compliance managers can develop a strategy that involves patterns and interconnections to counter the development of financial crimes (Rusanov & Pudovochkin, 2018). Furthermore, the identification of predicate offense typologies support the implementation of measures to counter financial crimes. In the fight to combat money laundering and terrorist financing, the identification

of predicate offense typologies may help compliance managers reduce the risks of money laundering and terrorist financing activities.

Researchers have assessed the effectiveness of money laundering controls (Cash, 2020; Pol, 2020; Yeoh, 2020) and the impact of technological advancements on modern anti-money laundering and counter terrorist financing methods (Carayannis et al., 2021; Han et al., 2020; Kurum, 2020; Li, 2019). There was an opportunity, however, to explore the lived experiences of compliance managers who lead efforts to identify predicate offense typologies in the fight to reduce the risks of money laundering and terrorist financing activities (see Al-Suwaidi & Nobanee, 2020). I sought to address this gap in the literature by conducting this study.

Criminals have discovered new and innovative means to conduct criminal activities causing a rise in money laundering and terrorist financing. Rusanov and Pudovochkin (2021) noted that perpetrators are investing about 15%-20% of laundered money into new criminal activities. Criminal activity is growing because criminals have uncovered various means to legalize illicit proceeds into the financial system (Rusanov & Pudovochkin, 2021). An aftermath of the Covid-19 pandemic is the growth of predicate offenses that rapidly increased the process in which dirty money is transformed into clean money. As modern crime increases, compliance managers need to identify predicate offense typologies to reduce the risks of money laundering and terrorist financing activities. The data analysis and results of this study yielded eight main themes and four subthemes. The eight main emergent themes were structuring, fraud, cybercrime, human trafficking and human smuggling, illicit arms trafficking, illicit drug trafficking, real

estate money laundering, and trade-based money laundering. The four subthemes were red flags, key indicators, typology-specific common signs, and 95% or above. The goal of this study was to identify predicate offenses that U.S. banking and financial services compliance managers use to reduce the risks of money laundering and terrorist financing. Each theme identified specific money laundering and terrorist financing activities that categorized into a predicate offense typology. Appendix B lists the 44 codes associated with the main themes. Appendix C lists the 31 codes associated with the subthemes. It is important to highlight best practices for each predicate offense typology that may help compliance managers reduce the risks of money laundering and terrorist financing activities.

Structuring

Structuring has become a global phenomenon in the context of financial crimes. Compliance managers with an awareness of structuring techniques may be able to revise the financial crime risk management framework to effectively detect money laundering activities within their financial institutions. Structuring is a predicate offense typology that may indicate underlying illegal activity. An effective anti-money laundering program of banks and financial services institutions involves the identification and prevention of structuring activities. Some best practices that compliance managers can implement are adopting know your customer guidelines, using anti-money laundering tools, and implementing an effective money laundering program:

- Adopt know your customer guidelines: It is necessary for compliance managers to ensure their anti-money laundering programs adopt stringent

know your customer guidelines. Know your customer is an effective tool to build a customer's profile and collect crucial background information. This tool will authenticate the identity, suitability and risks involved with the customers prior to the onboarding process and further development of a professional relationship.

- Use anti-money laundering tools: Another best practice is to use anti-money laundering tools and detection algorithms to help compliance managers and anti-money laundering investigators to combat structuring activities. An anti-money laundering internal alert system mitigates the risk of human errors associated with manual investigations (Clarke, 2021). Predicate offense typology-specific alerts trigger within the internal alert system which helps compliance managers and anti-money laundering investigators perform precise risk assessments.
- Implement an effective anti-money laundering program: Anti-money laundering programs are designed to detect and report money laundering and terrorist financing activities. The most effective anti-money laundering program is tailored to specific predicate offense typologies. An effort to ensure the institution is compliant with the suspicious activity reporting requirements of the Bank Secrecy Act is a best practice. Moreover, compliance managers need to set explicit parameters when monitoring accounts and transactional behavior to identify suspicious activity.

Anti-money laundering programs should be adequate with the compliance framework of the institution. As banks and financial services institutions face new emerging threats, compliance managers must ensure that their suspicious activity monitoring and reporting systems are reflecting the current socioeconomic environment.

Fraud

A key component of compliance with the banking and financial systems is fraud. An increased fluctuation in fraud cases has more institutions combating fraud-related activities. Compliance managers and anti-money laundering investigators, under the anti-money laundering functions, are attempting to identify patterns indicative of fraud. The investigating system-generated alerts are triggering according to specific criminal behavior. Along with the red flag indicators mentioned in the results of this study, compliance managers should adopt best practices to identify fraud to reduce the risks of money laundering and terrorist financing activities.

A best practice to mitigate the risk of fraud is to perform a comprehensive identity verification check. This process reduces the risk of incompliant regulations and the placement and layering of dirty money. Another best practice is conducting scenario-based tailored training. Compliance managers should conduct training sessions with audit and fraud employees about the new trends and patterns and predicate offense typology will help them identify fraud-related activities during their investigations. Last, a third best practice is performing internal, independent testing of anti-money laundering compliance. The testing should focus on a specific scope and frequency pointing to fraudulent transactions.

Fraudsters are deploying innovative means to launder money and fund terrorism. Money launderers and terrorists are capable of discovering weak elements in anti-money laundering and know your customer processes of banks and financial services institutions. Weak compliance frameworks help them to conceal illicit source of funds. To safeguard the financial systems, compliance managers should ensure counter and preventative measures by making their compliance framework more robust and secure.

Cybercrime

The rise of cybercrime threats has compliance managers reevaluating their compliance framework and risk assessments. As money launders and terrorist discover new means of cybercrime-related activities, compliance managers need to deploy applicable anti-money laundering and counter terrorist financing measures. In the context of cybercrime, the financial intelligence units of banks and financial services institutions must emphasize their efforts to identify their customers. Additionally, it is crucial for firms to routinely monitor their customers' account activity and financial behavior enhancing the following anti-money laundering and counter terrorist financing processes:

- Customer due diligence: Criminals exploit the ambiguity aspect of online transactions. Thus, compliance managers should reinforce certain levels of customer due diligence by verifying and authenticating customer identities and the nature of businesses for online-conducted transactions (Clarke, 2021).
- Transaction monitoring: The key element of cybercrime is quick funds transfers to several accounts located in different parts of the world. With this possibility of money movement, compliance managers should use cybercrime-

specific red flag indicators to monitor their customers' transactions for traces of money laundering and terrorist financing activities.

- Sanctions screening: Compliance managers must screen new and established customer accounts against current international sanctions lists provided by the Office of Foreign Assets and Control (OFAC). The Office of Foreign Assets and Control is a regulatory body who is responsible for overseeing and imposing the economic sanctions programs and regulations of the United States.
- PEP screening: Similar to sanctions screening, compliance managers must screen any customer to determine their politically exposed persons (PEP) status. Politically exposed persons are classified as high-risk and tend to be involved in cybercrime-related money laundering and terrorist financing activities. Compliance managers must modify their compliance counter measures for politically exposed persons.

As people become more reliant on modern technology, banks and financial services institutions become vulnerable to perpetrators looking for any online opportunity to illegally generate income and money launder the proceeds. Compliance managers are gatekeepers who try to safeguard and secure online financial transactions. They perform a critical role in achieving cybersecurity objectives by ensuring high-level customer due diligence efforts, monitoring online transactions, working with law enforcement agencies to conduct high-impact anti-money laundering investigations, and ensuring best practices and anti-money laundering tools.

Human Trafficking and Human Smuggling

Banks and financial services institutions are capable of preventing human trafficking and human smuggling by identifying financial transactions conducted by traffickers to launder their illicit monetary proceeds through financial systems. In the fight against this predicate offense typology, these institutions must enhance their anti-money laundering programs by reassessing their compliance strategies. The current anti-money laundering best practices help compliance managers to detect and avert human traffickers striving to launder money. The current anti-money laundering best practices include:

- Contextual information: Human trafficking activities are difficult to identify because criminals conduct different types of predicate offenses at the same time (Clarke, 2021). The red flags of human trafficking interconnect with many other aspects of money laundering and legal financial activities. With this particular predicate offense typology, compliance managers should consider other predicate offense red flag indicators along with available contextual information to accurately identify the predicate offense typology(s).
- Information sharing: If a bank or financial services institution receives an alert or information indicative of possible human trafficking activity, compliance managers should share the information amongst their compliance department. Information sharing will allow compliance managers to build a holistic case and gather any unknown information to possibly uncover suspicious

trafficking operations. Several legislative frameworks allow banks and financial services institutions to share information with law enforcement, regulators, and amongst themselves.

- Suspicious activity reports: The Financial Crimes Enforcement Network requires banks and financial services institutions to file a suspicious activity report (SAR) on questionable account activity. A suspicious activity report allows law enforcement agencies to conduct further investigations. At the time a firm files a suspicious activity report for human trafficking, compliance managers should highlight keywords to help law enforcement authorities in their investigation of locating traffickers.

Human traffickers and smugglers transform monetary proceeds into legal funds. The diversity in the financial streams from human trafficking and human smuggling are a challenge for banks and financial services institutions. It is a challenge for compliance managers to detect money laundering transactions from human trafficking and human smuggling. Although best practices and red flags specific to this predicate offense typology help institutions during their anti-money laundering investigations to detect any human trafficking or human smuggling activity.

Illicit Arms Trafficking

The multidimensional aspect of arms trafficking is the real issue. The complexity lies in the manufacture and trade of firearms. Firearms are manufactured and traded both lawfully and unlawfully. Consequently, it becomes complicated and challenging for compliance managers to identify illicit arms trafficking activities. Though, compliance

managers can implement preventive measures to address the international nature of this predicate offense typology. The following best practices aim to detect, prevent, combat and eliminate illicit arms trafficking:

- Documentation: Compliance managers must request information from customers regarding any international firearms transactions. It is necessary to keep a record of all the documents and licenses related to the international transactions to determine the legalization of the transaction(s).
- Information sharing: In the event a compliance manager discovers traces of illicit arms trafficking, they should share the information or anti-money laundering investigation findings with appropriate law enforcement agencies. Knowledge sharing can help law enforcement catch organized terrorist groups involved in illicit arms trafficking.

Changes in criminal behavior lead to changes in compliance frameworks which require change to reporting regulations. The reassessment of counter measures is a strategy to enhance compliance controls. To counter measure illicit arms trafficking, it is necessary for banks and financial services institutions to improve data collection efforts and support law enforcement by systematically sharing information. Compliance strategies including the best practices may help U.S. banking and financial service company compliance managers identify illicit arms trafficking to reduce the risks of money laundering and terrorist financing activities.

Illicit Drug Trafficking

Illicit drug trafficking is one of the most dominant predicate offense typologies worldwide. It produces more revenue compared to any other form of trafficking. Illicit drug trafficking is has become an international menace especially post the Covid-19 pandemic. It jeopardizes the solidity of several high-risk jurisdictions in which criminals conduct their operations to compromise the financial integrity. Financial institutions should be mindful of changes in customers' transaction patterns involving foreign-based transactions. Drug traffickers are using traditional money laundering methods. Theses traditional approaches include shell companies, couriers, and currency exchangers. The traditional methods combined with other predicate offenses create complicated and intricate money laundering schemes.

To counter measure drug trafficking activities, compliance managers should implement anti-money laundering and counter terrorist financing best practices. A best practice that financial institutions can deploy is monitoring sudden changes in customers' transaction patterns specifically high-risk jurisdiction transactions. Regulators scrutinize banks and financial institutions regarding their enhanced due diligence processes for high-risk customers. Another best practice is to reevaluate the enhanced due diligence processes to ensure they reflect the current risk profile of this predicate offense typology. A high-risk customer would include a business with a complex ownership structures indicative of shell companies executing possible drug trafficking activities. Drug traffickers maintain growing money laundering operations by infiltrating financial

systems. Banks and financial services institutions should continue to monitor financial transactions perhaps revelatory of drug trafficking-related activities.

Real Estate Money Laundering

The presence of a single risk factor, or even multiple factors, does not necessarily mean the purchaser or seller is engaging in money laundering activities. The role of compliance managers is to be knowledgeable about the risk factors, and exercise sound judgment based on their expertise of the real estate market. The best practices to combat real estate money laundering include:

- Know your customer/customer due diligence: The most crucial elements in helping compliance managers identify and reduce the risks of money laundering are know your customer and customer due diligence. Having a holistic understanding of a customer's profile and true intentions behind the purchase or sale of a property, will help compliance managers detect and reduce the risks of money laundering activities.
- Reporting suspicious activity: When anti-money laundering investigators come across suspicious activity, compliance managers are obligated to report the information to law enforcement (Clarke, 2021). Based on the red flag indicators, compliance managers are obligated to file a suspicious activity report. Certain red flags are indicative of reasonable suspicious real estate transactions that may be a means for real estate money laundering activity.
- Form 8300: Trading companies or businesses, which includes the real estate sector, must file a Form 8300 in the event the company receives more than

$10,000 in cash during a single transaction or two or more related transactions. This form collects information from trading companies or businesses to report specific information about a trade or real estate transaction.

Real estate money launders continue to use real estate in money laundering schemes which has become a huge area of concern. These best practices and compliance strategies will help compliance managers effectively detect and address real estate money laundering activities and partner with law enforcement agencies.

Trade-Based Money Laundering

Money launders have taken advantages of the Covid-19 pandemic to profit from trade-based money laundering activities. To combat their efforts, firms are intensifying their anti-money laundering controls in trade finance and correspondent banking. The complexity of this predicate offense typology makes it challenging for financial institutions to augment their anti-money laundering programs. The challenge lies in detecting trade-based money laundering since the activities are spread across different jurisdictions and organizations. A best practice that may help compliance managers identify trade-based money laundering and reduce the risks of money laundering and terrorist financing activities include:

- Creating awareness: Trade-based money laundering is a specific predicate offense typology. To mitigate this risk, it is important to build expertise by tailoring anti-money laundering programs according to the predicate offense

typology to ensure effective implementation of compliance policies and procedures.

- Red flags: A best practice in anti-money laundering and counter terrorist financing efforts is developing a list of red flags specific to the predicate offense typology. Trade-specific red flag indicators will help financial institutions easily detect new and emerging trends and patterns and collect information related to trade-based money laundering.
- Data protection: Technology is a valuable tool with great exposure to the risk of disclosing sensitive trade information. A best practice to combat trade-based money laundering is utilizing data capture instruments. Data capture systems set measures in place to systematize the structure of electronic information exchange between institutions and law enforcement agencies that is subject to applicable data protection safeguards.

Compliance managers can refer to the best practices highlighted above to identify trade-based money laundering activities. The red flags help compliance managers understand consumer behavior and recognize transactional patterns that indicate this predicate offense typologies. As a result, banks and financial services institutions can detect criminal financial activities.

A never-ending battle is the fight against money laundering and terrorist financing. All financial institutions, from large banks to small credit unions, need to be on the constant lookout for money launderers and terrorist. By implementing best practices mentioned above, compliance managers can detect, monitor, prevent, and

suppress the eight predicate offense typologies. Compliance managers of U.S. banks and financial services institutions need to highlight red flag indicators that will help them identify predicate offense typologies. Overall, to efficiently combat progressively, innovative money launders and terrorists, compliance managers need to implement real-time due diligence technology, train and inform compliance personnel about the current trends and patterns, and partner with law enforcement agencies to share information in a timely manner. A robust compliance framework prevent and reduce the risks of money laundering and terrorist financing activities in the United States and globally.

Limitations of the Study

Limitations are factors in a study that researchers cannot control. First, a limitation of this study is related to the research method and design that may possibly impact the research results. The qualitative descriptive case study was limited by time, location, and circumstance (Gray et al., 2020). The limitation was largely related to the incapability to conduct in-person interviews due to the aftermath of the coronavirus disease restrictions and rises in the Covid-19 cases. To overcome this limitation, I used Zoom, a videoconferencing platform to conduct the interviews which enabled me to collect the data and limit any exposure to the coronavirus disease protecting the health of the research participants and myself. Second, another limitation of this study is the generalization of the findings which imperils transferability to a larger population. To overcome this limitation, I provided a detailed analysis of the participant selection, recruitment of participants, data collection, and the methods used to verify the information and ensure accuracy of the data collected. Also, I used data triangulation to

support the results of this research study. The research could be replicated in other contexts, situations, times, and populations. In this qualitative research study, a sample of 15 research participants conducted semistructured interviews to reach the data saturation level. Therefore, a third limitation is researcher bias. To overcome this limitation, I used an interview guide during the data collection process and transcribed the data verbatim during the data analysis process (Yin, 2018). Additionally, I used member checking to mitigate any researcher bias. Last, compliance managers and anti-money laundering investigators are limited to express their opinions and experiences openly due to the nature of their workplace. Thus, to overcome this limitation, I received the consent of each participant prior to scheduling and conducting any interview to ensure that each research participant is willingly participating in this research study.

Recommendations

The general purpose of conducting this research was to explore and gather current information about predicate offense typologies in money laundering and terrorist financing. In this study, the research participants were compliance managers and anti-money laundering investigators from large U.S. banks and financial institutions. The predicate offense typologies identified in this study may differ from other banks largely depending on banks' risk factors. A future research recommendation is to conduct a study on small banks or midsize banks with different risk factors and customer profile. A study focusing on a specific target population could potentially identify different predicate offense typologies based on the frequency and types of financial crimes occurring in small to midsize banks.

Additionally, this study focused on U.S. banks and financial institutions which was limited to a specific region. Money launders and terrorist infiltrate banks and financial institutions across the globe. Each region may identify predicate offense typologies specific to the money laundering and terrorist financing activities occurring in that particular geographic footprint. Researchers can use the research design selected to complete this study to replicate and or conduct future studies. Another future research recommendation would be to conduct a similar study in other jurisdictions in the world or a group of countries based on a specific risk factor in a different part of the globe. For example, the compliance and legal framework is different in Cuba because the country faces economic, commercial, and financial sanctions. Thus, Cuba is classified as a riskier country than the United States. The findings may identify different predicate offense typologies based on the types of money laundering and terrorist financing activities occurring throughout the banks and financial institutions in those countries.

Those study outcomes could further extend the works of Al-Suwaidi and Nobanee (2020) and Cash (2020) to better understand the evolving criminal behavior and activities and gain a deeper understanding of the current predicate offense typologies. Based on the views of the interviewed compliance managers and anti-money laundering investigators, identifying predicate offense typologies is crucial risk management strategy in the efforts to reduce the risks of money laundering and terrorist financing activities and requires further research that should be conducted.

Finally, a qualitative descriptive case design was used to gain insight from the research participants related to how identifying predicate offense typologies help

compliance managers to reduce the risks of money laundering and terrorist financing activities. A future research recommendation would be to conduct a phenomenological study to explore current indicators and red flags which help anti-money laundering investigators identify the predicate offense typologies during anti-money laundering investigations. Criminal behavior is constantly evolving according to the changes in environments and situations. It may be of interest to gain a deeper insight into the differences in identification processes of indicators and red flags as new environmental circumstances impact anti-money laundering investigations. The findings may detect gaps in the compliance frameworks.

Implications

The findings of this study have significance for compliance leaders at large U.S. banking and financial services organizations. Large U.S. banking and financial services institution compliance leaders could augment their compliance programs to build a new set of indicators or red flags to look out for when conducting their compliance obligations. As the capabilities of criminals and money laundering and terrorist financing activities evolve, compliance officers may look to update their list of typologies and learn about new evolving typologies by focusing on risk factors relevant to their products or services. Rocha-Salazar et al. (2021) indicated that anti-money laundering and counter terrorist financing typologies are risk indicators and useful control to trigger enhanced due diligence and further monitoring. Thus, compliance managers may use the findings of this study to conduct enhanced due diligence training sessions with their anti-money laundering investigators to increase monitoring measures at their respective banks or

financial services institutions. Effective mitigation approaches could diminish the societal risks related to financial crime. There is a lack of research on modern compliance strategies (Al-Suwaidi & Nobanee, 2020). In recent times, it is perilously important for banking and financial services institutions to fully comprehend the financial crime threats and take the opportunity to undergo a latest, comprehensive health-check (Crisanto & Preno, 2020). The findings of this study may encourage compliance managers to conduct periodic, comprehensive compliance health-checks to reduce money laundering and terrorist financing risks. Banks and financial services institutions are encountering several critical anti-money laundering compliance challenges that impute flawed mitigation approaches (Cash, 2020). Organizations that neglect to preclude money laundering and terrorist financing activities tend to face decreasing profits, consumer discontent, huge monetary fines, loss of reputation, and decline in stock prices (Balani, 2019). The findings of this study may continue to emphasize anti-money laundering and counter terrorist financing activities for banking and financial services organizations, although practices can change to be more pragmatic to current situations.

Implications for Practice

The results of the study may indicate the benefits of modifying money laundering and terrorist financing risk mitigation approaches and develop new mitigating controls. By this means, the results of the study may transform and implement sound risk-based anti-money laundering and counter terrorist financing compliance programs and standards to minimize and regulate U.S. banking and financial services institutions' money laundering and terrorist financing exposure through practical approaches that

deter money launderers and terrorists from endeavoring to infiltrate their corporations. In addition, the findings of the study may encourage compliance managers to perform periodic updates on know your customer profiles to gather current information on their high-risk customers (Pai, 2021). By updating their know your customer profiles, compliance managers may evaluate and revise their current know your customer model. The results of the study may suggest enhancements in increasing transparency and closing gaps in the anti-money laundering and counter terrorist financing compliance framework (Zagaris, 2020). Corporate benefits such as improving operational efficiency and effectiveness of anti-money laundering and counter terrorist financing regulations may lower compliance costs and increase revenue for financial institutions can ensue from the study (Cash, 2020). Additionally, the study findings may increase insight for compliance managers to implement strategic changes that will stimulate long-term sustainable growth and economic value. New processes of technological advancements could sustain digital due diligence solutions to meet present and future operational risk management needs (Ekberg, 2020; Han et al., 2020). Compliance managers may understand new risks and modify operational measures to mitigate financial crime risks.

Implications for Theory

The results of this study may identify effective compliance practices that address a knowledge gap towards managing financial crime risks and contribute fundamental qualitative data to the study's conceptual framework. Notwithstanding the growing literature on the significance of money laundering and terrorist financing (Tiwari et al., 2020), there has been a failure to identify predicate offense typologies that improve and

develop effective compliance regulations and requirements thus reducing financial crime risks and risky criminal behavior (Sisira Dharmasri Jayasekara, 2021). Although economic theory of criminal behavior discusses the relationship between financial crimes and benefit-cost analysis, a descriptive case study approach meets the purpose of the study and offers distinct contributions to the theory. The descriptive case study approach provides findings from a consensual process that uses semistructured interviews to collect subject matter expert opinions to enlighten theoretical change and extend the results of prior studies. Applying economic theory of criminal behavior to U.S. banking and financial services institutions may provide a theoretical understanding of the problem relevant to the recent increase in financial crime risks and a lack of adequate compliance strategies and regulations (Gowhor, 2021). This may be a significant addition to the seminal works of Gary Becker (1968) neoclassical approach in playing a role in the motivation behind financial crimes.

Implications for Social Change

American society could benefit from the results of the study. The banking and financial industries ought to be prepared for the future and continue to adapt to new emerging threats, varying consumer classification, and changing environment. Banking and financial services institutions play a substantial role in the community. Based on the findings of this study, these organizations can work towards effective money laundering and terrorist financing prevention plans by changing and developing new compliance policies and procedures. Moreover, banks and financial services institutions can increase general knowledge and spread public awareness about predicate offense typologies by

educating their customers about financial crimes and steps to combat money laundering and terrorist financing activities (Azman Aziz & Md Daud, 2021). It is essential for compliance leaders to implement public education initiatives and help their customers recognize their role in combating money laundering and terrorist financing activities. Additionally, banks and financial services institutions may clarify and strengthen customer due diligence requirements by implementing enhanced due diligence measures to protect their organizations and reduce financial crime risks. The implications for positive social change may include the possibilities to develop new compliance strategies and strengthen existing regulatory mechanisms to help compliance managers, reduce the risk of bank failures, increase employment opportunities, and promote public awareness by educating consumer about financial crimes. Overall, the study has contributed to positive social change by identifying predicate offense typologies that can help U.S. banking and financial services company compliance managers reduce the risks of money laundering and terrorist financing activities.

Conclusion

The Covid-19 pandemic presented new opportunities for criminals to conduct money laundering and terrorist financing activities. To gain a deeper understanding of the phenomenon under study, I attempted to present a holistic overview of the unprecedented impact of the Covid-19 pandemic on criminal behavior and the rise of Covid-19 related financial crimes. The purpose of this qualitative descriptive case study was to identify predicate offense typologies that U.S. banking and financial services company compliance managers use to reduce the risks of money laundering and terrorist financing

activities. To understand rationale behind financial crimes and evolving criminal behavior, the economic theory of criminal behavior, developed by Gary Becker in 1968, provided a conceptual framework which grounded this study. The target population consisted of 15 research participants. The data were collected using semistructured interviews, semistructured observations, and document reviews from business and finance academic journals. The data were analyzed using a coding approach, thematic analysis, and content analysis. The quintessence of this study was influenced by the participants' lived experiences and expertise. The findings of the study uncovered predicate offense typologies related to financial crimes that are increasing the risks of money laundering and terrorist financing activities.

The results of the study emphasized eight emerging main themes: (a) structuring, (b) fraud, (c) cybercrime, (d) human trafficking and smuggling, (e) illicit arms trafficking, (f) illicit drug trafficking, (g) real estate money laundering, and (h) trade-based money laundering, and four subthemes: (a) red flags, (b) key indicators, (c) typology-specific common signs, and (d) 95% or above. Compliance managers have an underlying responsibility to identify predicate offense typologies to reduce the risks of money laundering and terrorist financing activities. The study has revealed to be useful to compliance managers, anti-money laundering investigators, and banking and financial services institutions. As a result, the study will have a positive social impact on society. Throughout the study, I have used the optimal method and employed best practices in conducting a systematic process to accomplish the goal of the research study. I further explained the transferability of this study in other contexts and economic environments

for the betterment of financial systems. Last, the objective of this study was predominantly achieved and I suggest further research on this concept for the betterment of banking and financial institutions and safety of the general public.

References

Albanese, J. S. (2021). Organized crime as financial crime: The nature of organized crime as reflected in prosecutions and research. *Victims and Offenders*, *16*(3), 431-443. https://doi.org/10.1080/15564886.2020.1823543

Ali, S. (2021). Criminal minds: Profiling architects of financial crimes. *Journal of Financial Crime*, *28*(2), 324–344. https://doi.org/10.1108/JFC-11-2020-0221

Al-Suwaidi, N. A., & Nobanee, H. (2020). Anti-money laundering and anti-terrorism financing: A survey of the existing literature and a future research agenda. *Journal of Money Laundering Control*, *24*(2), 396–426. https://doi.org/10.1108/JMLC-03-2020-0029

Amjad, R. M., Rafay, A., Arshed, N., Munir, M., & Amjad, M. M. (2021). Non-linear impact of globalization on financial crimes: A case of developing economies. *Journal of Money Laundering Control*, *25*(2), 358–375. https://doi.org/10.1108/JMLC-03-2021-0023

Arends, I., Bültmann, U., Shaw, W., Rhenen, W., Roelen, C., Nielsen, K., & Klink, J. (2014). How to engage occupational physicians in recruitment of research participants: A mixed-methods study of challenges and opportunities. *Journal of Occupational Rehabilitation*, *24*(1), 68–78. https://doi.org/10.1007/s10926-013-9452-y

Arnold, B. B., & Bonython, W. (2016). *Villains, victims and bystanders in financial crime*. Springer.

Azinge, N. V. (2019). A regulatory misfit? A closer look at the counter-terrorist financing strategies in African states. *Journal of Banking Regulation*, *20*, 245–259. https://doi.org/10.1057/s41261-018-0087-y

Azman Aziz, Z. Z., & Md Daud, S. A. M. (2021). Customer's awareness, trust, discomfort and acceptance of anti-money laundering practices in Malaysian Banks. *Journal of Money Laundering Control*, *25*(4), 864–881. https://doi.org/10.1108/JMLC-08-2021-0087

Bahoo, S. (2020). Corruption in banks: A bibliometric review and agenda. *Finance Research Letter*, *35*, Article 101499. https://doi.org/10.1016/j.frl.2020.101499

Balani, H. (2019). Assessing the introduction of anti-money laundering regulations on bank stock valuation: An empirical analysis. *Journal of Money Laundering Control*, *22*(1), 76–88. https://doi.org/10.1108/JMLC-03-2018-0021

Basit, A. (2020). COVID-19: A challenge or opportunity for terrorist groups? *Journal of Policing, Intelligence, and Counter Terrorism*, *15*(3), 263–275. https://doi.org/10.1080/18335330.2020.1828603

Beaunoyer, E., Dupéré, S., & Guitton, M. J. (2020). Covid-19 and digital inequalities: Reciprocal impacts and mitigation strategies. *Computers in Human Behavior*, *111*, Article 106424. https://doi.org/10.1016/j.chb.2020.106424

Becker, G. S. (1968). Crime and punishment: An economic approach. *Journal of Political Economy*, *76*(2), 169–217. https://doi.org/10.1086/259394

Bell, R. E. (2002). Abolishing the concept of "predicate offence." *Journal of Money Laundering Control*, *6*(2), 137–140. https://doi.org/10.1108/13685200310809482

Bhogal, T., & Trivedi, A. (2019). *Money laundering and sanctions*. Springer. https://doi.org/10.1007/978-3-030-24540-5_25

Bieler, S. A. (2022). Peeking into the house of cards: Money laundering, luxury real estate, and the necessity of data verification for the corporate transparency act's beneficial ownership registry. *Fordham Journal of Corporate & Financial Law, 27*(1), Article 4.

Boister, N. (2012). International tribunals for transnational crimes: Towards a transnational criminal court? *Criminal Law Forum*, *23*, 295–318. https://doi.org/10.1007/s10609-012-9182-4

Brabenec, T., & Montag, J. (2018). Criminals and the price system: Evidence from Czech metal thieves. *Journal of Quantitative Criminology*, *34*(2), 397–430. https://doi.org/10.1007/s10940-017-9339-8

Brandariz, J. A., & González-Sánchez, I. (2018). Economic crises, common crime, and penalty. *Oxford Research Encyclopedia of Criminology*. https://doi.org/10.1093/acrefore/9780190264079.013.351

Burkholder, G. J., Cox, K. A., & Crawford, L. M. (2016). *The scholar-practitioners guide to research design*. Laureate.

Cash, D. (2020). Sigma ratings: Adapting the credit rating agency model for the anti-money laundering world. *Journal of Money Laundering Control*, *23*(1), 1–10. https://doi.org/10.1108/JMLC-06-2019-0046

Campedelli, G. M., Aziani, A., & Favarin, S. (2020). Exploring the immediate effects of Covid-19 containment policies on crime: An empirical analysis of the short-term

aftermath in Los Angeles. *American Journal of Criminal Justice*, *46*(5), 704–727. https://doi.org/10.1007/s12103-020-09578-6

Carayannis, E. G., Christodoulou, K., Christodoulou, P., Chatzichrisofis, S. A., & Zinonos, Z. (2021). Known unknowns in an era of technological and viral disruptions-implications for theory, policy, and practice. *Journal of the Knowledge Economy*, *13*, 587–610. https://doi.org/10.1007/s13132-020-00719-0

Chen, T.-H. (2020). Do you know your customer? Bank risk assessment based on machine learning. *Applied Soft Computing Journal*, *86*, 586–610. https://doi.org/10.1016/j.asoc.2019.105779

Clarke, A. E. (2021). Is there a commendable regime for combatting money laundering in international business transactions. *Journal of Money Laundering Control*, *24*(1), 163–176. https://doi.org/10.1108/JMLC-05-2020-0057

Converse, M. (2012). Philosophy of phenomenology: How understanding aids research. *International Journal of Research Methodology in Nursing and Health Care*, *20*, 28–32. http://ovidsp.ovid.com/ovidweb.cgi?T=JS&PAGE=fulltext&D=ovft&CSC=Y&NEWS=N&SEARCH=00021768-201209000-00005.an

Creswell, J. W. (2013). *Qualitative inquiry and research design: Choosing among five approaches* (3rd ed.). Sage Publications.

Crisanto, J., & Preno, J. (2020). Financial crime in times of Covid-19 - AML and cyber resilience measures. BIS. https://www.bis.org/fsi/fsibriefs7.htm

Cui, K. (2015). The insider–outsider role of a Chinese researcher doing fieldwork in China: The implications of cultural context. *Qualitative Social Work, 14*(3), 356–369. https://doi.org/10.1177/1473325014545412

Ehrlich, I. (1974). *Participation in illegitimate activities: An economic analysis*. Essays in the Economics of Crime and Punishment, 68–134. Columbia University Press.

Ehrlich, I. (1973). Participation in illegitimate activities: a theoretical and empirical investigation. *Journal of Political Economy*, *81*(3), 521–565. https://doi.org/10.1086/260058

Eide, E. (1994). *Economics of crime: Deterrence and the rational offender.* Elsevier.

Ekberg, M. L. (2020). Financial crime risk management and the Covid-19 Pandemic: Issues for closer international cooperation and coordination. *Institute of International Finance*. https://www.iif.com/Portals/0/Files/content/32370132_iif_covid_amlcft_staff_paper_april_2020_final.pdf

Federal Financial Institutions Examination Council. (2021). *Assessing compliance with BSA regulatory requirements*. https://bsaaml.ffiec.gov/manual/AssessingComplianceWithBSARegulatoryRequirements/02

Financial Action Task Force. (2016). *Anti-money laundering and counter-terrorist financing measures.* https://www.fatf-gafi.org/media/fatf/documents/reports/mer4/mer-united-states-2016.pdf

Financial Action Task Force. (2017). *Anti-money laundering and terrorist financing measures and financial inclusion*. https://www.fatf-gafi.org/media/fatf/Updated-2017-FATF-2013-Guidance.pdf

Financial Action Task Force. (2020a). *Covid-19 related money laundering and terrorist financing.* https://www.fatf-gafi.org/media/fatf/documents/COVID-19-AML-CFT.pdf

Financial Action Task Force. (2018). *Financial flows from human trafficking.* https://www.fatf-gafi.org/media/fatf/content/images/Human-Trafficking-2018.pdf

Financial Action Task Force. (2020b). *Trade-based money laundering: Trends and developments*. https://www.fatf-gafi.org/media/fatf/content/Trade-Based-Money-Laundering-Trends-and-Developments.pdf

Financial Action Task Force. (2020c). *Update: Covid-19 related money laundering and terrorist financing.* https://www.fatf-gafi.org/media/fatf/documents/Update-COVID-19-Related-Money-Laundering-and-Terrorist-Financing-Risks.pdf

Financial Action Task Force. (2020d). *Virtual assets red flag indicators of money laundering and terrorist financing.* https://www.fatf-gafi.org/publications/methodsandtrends/documents/virtual-assets-red-flag-indicators.html

Financial Crimes Enforcement Network. (2021). *Anti-money laundering and countering the financing of terrorism national priorities*. https://www.fincen.gov/sites/default/files/shared/AML_CFT%20Priorities%20(June%2030%2C%202021).pdf

Financial Crimes Enforcement Network. (2020). *Supplemental advisory on identifying and reporting human trafficking and related activity.* https://www.fincen.gov/sites/default/files/advisory/2020-10-15/Advisory%20Human%20Trafficking%20508%20FINAL_0.pdf

Fletcher, E., Larkin, C., & Corbet, S. (2021). Countering money laundering and terrorist financing: a case for bitcoin regulations. *Research in International Business and Finance*, *56*. https://doi.org/10.1016/j.ribaf.2021.101387

Frankfort-Nachmias, C., Nachmias, D., & DeWaard, J. (2015). *Research methods in the social sciences* (8th ed.). Worth.

Friedrich-Baasner, G., Fischer, M., & Winkelmann, A. (2018). Cloud computing in SMEs: A qualitative approach to identify and evaluate influential factors. *International Conference on System Sciences*, 4681–4690. https://doi.org/10.24251/HICSS.2018.590

Fusch, P. I., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *Qualitative Report*, *20*(9), 1408–1416. https://doi.org/10.46743/2160-3715/2015.2281

Garg, R. (2016). Methodology for research I. *Indian Journal of Anaesthesia*, *60*(9), 640–645. https://doi.org/10.4103/0019-5049.190619

Galeazzi, M.-A., Mendelson, B., & Levitin, M. (2021). The anti-money laundering act of 2020. *Journal of Investment Compliance*, *22*(3), 253–259. https://doi.org/10.1108/JOIC-05-2021-0023

Gilmour, N. (2021). Crime scripting the criminal activities of money laundering – holistically. *Journal of Money Laundering Control*. https://doi.org/10.1108/JMLC-09-2020-0109

Golafshani, N. (2003). Understanding reliability and validity in qualitative research. *The Qualitative Report*, *8*(4), 597–606. https://doi.org/10.46743/2160-3715/2003.1870

Goldbarsht, D., & de Koker, L. (2022). *Financial technology and the law*. Springer. https://doi.org/10.1007/978-3-030-88036-1

Gottschalk, P. (2010). Categories of financial crime. *Journal of Financial Crime*, *17*(4), 441–458. https://doi.org/10.1108/13590791011082797

Gowhor, H. S. (2021). The existing financial intelligence tools and their limitations in early detection of terrorist financing activities. *Journal of Money Laundering Control*, *25*(4), 843–863. https://doi.org/10.1108/JMLC-07-2021-0075

Gray, L. M., Wong-Wylie, G., Rempel, G. R., & Cook, K. (2020). Expanding qualitative research interviewing strategies: Zoom video communications. *The Qualitative Report*, *25*(5), 1292–1301. https://doi.org/10.46743/2160-3715/2020.4212

Greszler, R. (2021). Excessive pandemic unemployment benefits are a warning against unemployment program expansion. *The Backgrounder*. https://www.heritage.org/jobs-and-labor/report/excessive-pandemic-unemployment-benefits-are-warning-against-unemployment

Gyamfi, N. K., & Abdulai, J.-D. (2018). Bank fraud detection using support vector machine. *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Information Technology, Electronics and*

Mobile Communication Conference (IEMCON), 2018 IEEE 9th Annual, 37–41. https://doi.org/10.1109/IEMCON.2018.8614994

Halkias, D., & Neubert, M. (2020). Extension of theory in leadership and management studies using the multiple-case study design. *International Leadership Journal*, *12*(2), 48–73. https://doi.org/10.2139/ssrn.3586256

Halloran, T. (2020). The role of intent in the rise of individual accountability in aml-bsa enforcement actions. *Fordham Journal of Corporate & Financial Law*, *25*(1), 239–246. https://ir.lawnet.fordham.edu/jcfl/vol25/iss1/5

Han, J., Huang, Y., Liu, S., & Towey, K. (2020). Artificial intelligence for anti-money laundering: A review and extension. *Digit Finance*, *2*, 211–239. https://doi.org/10.1007/s42521-020-00023-1

Hasham, S., Joshi, S., & Mikkelsen, D. (2019). Financial crime and fraud in the age of cybersecurity. *McKinsey Insights*. https://search.ebscohost.com/login.aspx?direct=true&AuthType=shib&db=bth&AN=138935627&site=eds-live&scope=site.

Hashim, H. A., Salleh, Z., Shuhaimi, I., & Ismail, N. A. N. (2020). The risk of financial fraud: A management perspective. *Journal of Financial Crime, 27*(4), 1143–1159. https://doi.org/10.1108/JFC-04-2020-0062

Haq, M. Z., Farzana, K. F., & Md, M. (2021). Could banning virtual assets be a breach of the doctrine of legitimate expectation? *Journal of Money Laundering Control*, *25*(4), 719–729. https://doi.org/10.1108/JMLC-07-2021-0077

Helmy, T. H., Zaki, M., Salah, T., & Badran, K. (2016). Design of a monitor for detecting money laundering and terrorist financing. *Journal of Theoretical and Applied Information Technology*, *85*(3), 425–436. http://www.jatit.org/

Hirschhorn, F. (2019). Reflections on the application of the Delphi method: Lessons from a case in public transport research. *International Journal of Social Research Methodology*, *22*(3), 309–322. https://doi.org/10.1080/13645579.2018.1543841

Hodgkinson, T., & Andresen, M. A. (2020). Show me a man or a woman alone and I'll show you a saint: Changes in the frequency of criminal incidents during the Covid-19 pandemic. *Journal of Criminal Justice*, *69*. https://doi.org/10.1016/j.jcrimjus.2020.101706

Hubbard, D. W. (2020). *The Failure of Risk Management*. John Wiley & Sons.

Ibrahim, S. A. (2019). Regulating cryptocurrencies to combat terrorism-financing and money laundering. *Journal of the Centre for Strategic and Contemporary Research*, *2*(1), 1–17. https://journal.cscr.pk/stratagem/index.php/stratagem/article/view/38

Ilahi, A. H. A., & Widowaty, Y. (2021). The optimization of corruption deterrence during the Covid-19 pandemic. *Padjadjaran Journal of Law*, *8*(1), 71–86. https://doi.org/10.22304/pjih.v8n1.a4

Jamshed, S. (2014). Qualitative research method-interviewing and observation. *Journal of Basic and Clinical Pharmacy*, *5*(4), 87–88. https://doi.org/10.4103/0976-0105.141942

Jamil, A. H., Mohd Sanusi, Z., Yaacob, N. M., Mat Isa, Y., & Tarjo, T. (2021). The Covid-19 impact on financial crime and regulatory compliance in Malaysia. *Journal of Financial Crime*, *29*(2), 491–505. https://doi.org/10.1108/JFC-05-2021-0107

Janesick, V. J. (2015). Peer debriefing. *The Blackwell Encyclopedia of Sociology*. https://doi.org/10.1002/9781405165518.wbeosp014.pub2

Juntunen, J., & Teittinen, H. (2022). Accountability in anti-money laundering – findings from the banking sector in Finland. *Journal of Money Laundering Control*. https://doi.org/10.1108/JMLC-12-2021-0140

Kawulich, B. B. (2004). Data analysis techniques in qualitative research. *Journal of Research in Education*, *14*(1), 96–113. https://www.researchgate.net/publication/258110388_Qualitative_Data_Analysis_Techniques

Keesoony, S. (2016). International anti-money laundering laws: The problems with enforcement. *Journal of Money Laundering Control*, *19*(2), 130–147. https://doi.org/10.1108/JMLC-06-2015-0025

Kemsley, D., Kemsley, S. A., & Morgan, F. T. (2021). Tax evasion and money laundering: A complete framework. *Journal of Financial Crime*, *29*(2), 589–602. https://doi.org/10.1108/JFC-09-2020-0175

Kerusauskaite, I. (2022). Editorial: Frameworks to address other issues could help us better tackle financial crime. *Journal of Financial Crime*, *29*(4), pp. 1133–1136. https://doi.org/10.1108/JFC-10-2022-278

Kesler, B. (2021). *Seven expected changes in AML after Covid-19.* https://www.acamstoday.org/seven-expected-changes-in-aml-after-covid-19/

Khan, N. I., Jani, M. A. A., & Zulkifli, A. A. (2021). The effectiveness of anti-money laundering/counter financing of terrorism requirements in fund management companies. *International Journal of Service Management and Sustainability*, *6*(2), 53–76. https://doi.org/10.24191/ijsms.v6i2.15572

Klimczak, K. M., Sison, A. J. G., Prats, M., & Torres, M. B. (2021). How to deter financial misconduct if crime pays? *Journal of Business Ethics*, *179*, 205–222. https://doi.org/10.1007/s10551-021-04817-0

Kolachala, K., Simsek, E., Ababneh, M., & Vishwanathan, R. (2021). SoK: Money laundering in cryptocurrencies. *ARES 2021: The 16th International Conference on Availability, Reliability, and Security*, *5*, 1–10. https://doi.org/10.1145/3465481.3465774

Kolb, S. M. (2012). Grounded theory and the constant comparative method: Valid research strategies for educators. *Journal of Emerging Trends in Educational Research and Policy Studies*, *3*(11), 83–86. https://www.researchgate.net/publication/307632469_Grounded_theory_and_the_constant_comparative_method_Valid_research_strategies_for_educators

Korstjens, I., & Moser, A. (n.d.). Series: practical guidance to qualitative research. Part 4: Trustworthiness and publishing. *European Journal of General Practice*, *24*(1), 120–124. https://doi.org/10.1080/13814788.2017.1375092

Korystin, O. Y., Mihus, I. P., Svyrydiuk, N. P., Likhovitskyy, Y. O., & Mitina, O. M. (2020). Money laundering: Macroeconomic assessment methods and current trend in Ukraine. *Financial and Credit Activity: Problems of Theory and Practice*, *1*(32), 341–350. https://doi.org/10.18371/fcaptp.v1i32.200865

Kruth, J. G. (2015). Five qualitative research approaches and their applications in parapsychology. *Journal of Parapsychology*, *79*(2), 219–233. https://www.proquest.com/scholarly-journals/five-qualitative-research-approaches-their/docview/1776152718/se-2

Kurum, E. (2020). RegTech solutions and AML compliance: What future for financial crime? *Journal of Financial Crime*. https://doi.org/10.1108/JFC-04-2020-0051

Larrinaga, O. V. (2017). Is it desirable, necessary and possible to perform research using case studies? *Cuadernos De Gestión*, *17*(1), 147–171. https://doi.org/10.5295/cdg.140516ov

Laureate Education (Producer). (2016). Theoretical lens and frameworks for qualitative researchers [Video file]. Baltimore, MD: Author.

Lawlor-Forsyth, E., & Gallant, M. M. (2018). Financial institutions and money laundering: A threatening relationship? *Journal of Banking Regulation*, *19*(2), 131–148. https://doi.org/10.1057/s41261-017-0041-4

Leedy, P. D., & Ormrod, J. E. (2015). *Practical research: Planning and design*. Pearson Education.

Levi, M., & Soudijn, M. (2020). Understanding the laundering of organized crime money. *Crime & Justice*, *49*(1), 579–631. https://doi.org/10.1086/708047

Li, Y. (2019). Design a management information system for financial risk control. *Cluster Computing*, *22*, 8783–8791. https://doi.org/10.1007/s10586-018-1969-6

Li, Y. (2021). Research on crime prevention based on the economics of crime. *Advances in Economics, Business and Management Research, volume 166 Proceedings of the 6th International Conference on Financial Innovation and Economic Development (ICFIED 2021)*, 167–170. https://doi.org/10.2991/aebmr.k.210319.031

Li, Y., Wei, F., Ren, S., & Di, Y. (2015). Locus of control, psychological empowerment and intrinsic motivation relation to performance. *Journal of Managerial Psychology*, *30*(4), 422–438. https://doi.org/10.1108/JMP-10-2012-0318

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry*. Sage Publications.

Lindgren, B.-M., Lundman, B., & Graneheim, U. H. (2020). Abstraction and interpretation during the qualitative content analysis process. *International Journal of Nursing Studies*, *108*. https://doi.org/10.1016/j.ijnurstu.2020.103632

Lochmiller, C. R. (2021). Conducting thematic analysis with qualitative data. *Qualitative Report*, *26*(6), 2029–2044. https://doi.org/10.46743/2160-3715/2021.5008

Lopez, J. A., & Spiegel, M. M. (2021). Small business lending under the PPP and PPPLF programs. *Federal Reserve Bank of San Francisco Working Paper*, 2-22. https://doi.org/10.24148/wp2021-10

Mackenna, P. (2017). Financial institutions fraud. *American Criminal Law Review*, *54*(4), 1333.https://link.gale.com/apps/doc/A503310703/EAIM?u=minn4020&sid=ebsco&xid=bfd6aeef

Malagon-Maldonado, G. (2014). Qualitative research in health design. *Health Environment Research & Design Journal, 7*(4), 120–134. https://doi.org/10.1177/193758671400700411

Manen, M. V. (2016). *Phenomenology of practice: Meaning-giving methods in phenomenological research and writing*. Routledge.

Marshall, C., & Rossman, G. B. (2015). *Designing qualitative research* (6th ed.). Sage Publications.

Maxwell, J. A. (2013). *Qualitative research design: An interactive approach.* Sage.

McCarthy, B. (2002). New economics of sociological criminology. *Annual Review of Sociology, 28*, 417–442. https://doi.org/10.1146/annurev.soc.28.110601.140752

Meinert, M. C. (2019). Countering corruption. American Bankers Association. *ABA Banking Journal*, *111*(3), 32-34. https://bankingjournal.aba.com/2019/04/countering-corruption/

Mekpor, E. S. (2019). Anti-money laundering and combating the financing of terrorism compliance: Are FATF member states just scratching the surface?" *Journal of Money Laundering Control*, *22*(3), 451–471. https://doi.org/10.1108/JMLC-09-2018-0057

Merriam, S. B., & Tisdell, E. J. (2016). *Qualitative research: A guide to design and implementation*. John Wiley & Sons.

Miceli, T. J. (2017). The economic model of crime. *The Economic Approach to Law*, 3, 244–260. https://doi.org/10.1515/9781503604575-051

Mugarura, N. (2014). Customer due diligence (CDD) mandate and the propensity of its application as a global AML paradigm. *Journal of Money Laundering Control*, *17*(1), 76–95. https://doi.org/10.1108/JMLC-07-2013-0024

Naheem, M. A. (2019). Local intelligence – the missing link in CTF regulation in the banking sector. *Journal of Money Laundering Control*, *22*(1), 132–144. https://doi.org/10.1108/JMLC-10-2015-0047

Namli, U. (2021). Behavioral changes amongst street level drug trafficking organizations and fluctuation in drug prices before and during the Covid-19 pandemic. *American Journal of Qualitative Research*, *5*(1), 1–22. https://doi.org/10.29333/ajqr/9691

Nizovtsev, Y. Y., Parfylo, O. A., Barabash, O. O., Kyrenko, S. G., & Smetanina, N. V. (2022). Mechanisms of money laundering obtained from cybercrime: The legal aspect. *Journal of Money Laundering Control*, *25*(2), 297–305. https://doi.org/10.1108/JMLC-02-2021-0015

Nobanee, H., & Ellili, N. (2018). Anti-money laundering disclosures and banks' performance. *Journal of Financial Crime*, *25*(1), 95–108. https://doi.org/10.1108/JFC-10-2016-0063

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods*, *16*, 1–13. https://doi.org/10.1177/1609406917733847

O'Boyle, E., Pollack, J., & Rutherford, M. (2012). Exploring the relation between family involvement and firms' financial performance: A meta-analysis of main and

moderator effects. *Journal of Business Venturing*, *27*(1), 1–18. https://doi.org/10.1016/j.jbusvent.2011.09.002

Olofinbiyi, S. A. (2022). Cyber insecurity in the wake of Covid-19: A reappraisal of impacts and global experience within the context of routine activity theory. *ScienceRise: Juridical Science*, *19*(1), 37–45. https://doi.org/10.15587/2523-4153.2022.253820

Onufer, M. (2022). *The roles and responsibilities of US financial institutions in combatting human trafficking*. In *Human Trafficking*. Routledge.

Pai, S. (2021). Anti-money laundering: Current state of play. *Governance Directions*, *73*(2), 56–60. https://search.informit.org/doi/10.3316/informit.692438496523680

Peticca-Harris, A., deGama, N., & Elias, S. R. S. T. A. (2016). A dynamic process model for finding informants and gaining access in qualitative research. *Organizational Research Methods*, *19*(3), 376–401. https://doi.org/10.1177/1094428116629218

Plaksiy, K., Nikiforov, A., & Miloslavskaya, N. (2018). Applying big data technologies to detect cases of money laundering and counter financing of terrorism. *2018 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Future Internet of Things and Cloud Workshops (FiCloudW), 2018 6th International Conference on, FICLOUDW*, 70–77. https://doi.org/10.1109/W-FiCloud.2018.00017

Pol, R. F. (2020). Anti-money laundering: The world's least effective policy experiment? Together, we can fix it. *Policy Design & Practice*, *3*(1), 73–94. https://doi.org/10.1080/25741292.2020.1725366

Posner, R. A. (1985). An economic theory of the criminal law. *Columbia Law Review*, *85*(6), 1193. https://advance.lexis.com/api/document?collection=analytical-materials&id=urn:contentItem:3S0M-9V10-00CW-72Y0-00000-00&context=1516831.

Rajah, J. (2019). Law, politics, and populism in the U.S.A P.A.T.R.I.O.T Act. *Indiana Journal of Global Legal Studies*, *26*(1), 61–85. https://doi.org/10.2979/indjglolegstu.26.1.0061

Rashid, M. A., Al-Mamun, A., Roudaki, H., & Yasser, Q. R. (2022). An overview of corporate fraud and its prevention approach. *Australasian Accounting Business & Finance Journal*, *16*(1), 101–118. https://doi.org/10.14453/aabfj.v16i1.7

Ravitch, S. M., & Carl, N. M. (2016). *Qualitative research: Bridging the conceptual, theoretical, and methodological*. Sage Publications.

Reurink, A. (2016). "White-collar crime": The concept and its potential for the analysis of financial crime. *Archives Europeennes De Sociologies*, *57*(3), 385–415. https://doi.org/10.1017/S0003975616000163

Rocha-Salazar, J.-J., Segovia-Vargas, M.-J., & Camacho-Miñano, M.-M. (2021). Money laundering and terrorism financing detection using neural networks and an abnormality indicator. *Expert Systems with Applications*, *169*. https://doi.org/10.1016/j.eswa.2020.114470

Rottenberg, S. (1973). *The economics of crime and punishment*. American Enterprise Institute.

Rubin, H., & Rubin, I. (2012). *Qualitative interviewing: The art of hearing data*. Sage Publications.

Rusanov, G., & Pudovochkin, Y. (2021). Money laundering in the modern crime system. *Journal of Money Laundering Control*, *24*(4), 860–868. https://doi.org/10.1108/JMLC-08-2020-0085

Rusanov, G., & Pudovochkin, Y. (2018). Money laundering and predicate offenses: Models of criminological and legal relationships. *Journal of Money Laundering Control*, *21*(1), 22–32. https://doi.org/10.1108/JMLC-12-2016-0048

Saddiq, S. A., & Abu Bakar, A. S. (2019). Impact of economic and financial crimes on economic growth in emerging and developing countries: A systematic review. *Journal of Financial Crime, 26*(3), 910–920. https://doi.org/10.1108/JFC-10-2018-0112

Saldãna, J. (2016). *The coding manual for qualitative researchers* (3rd ed.). Sage Publications.

Salmon, P. (2013). Assessing the quality of qualitative research. *Patient Education and Counseling*, *90,* 1–3. https://doi.org/10.1016/j.pec.2012.11.018

Schmidt, P., & Witte, A. D. (1984). *An economic analysis of crime and justice: Theory, methods and applications.* MIT Press.

Schwellenbach, N., & Summers, R. (2021). Red flags: The first year of Covid-19 loan fraud cases. *Project on Government Oversight.* https://www.pogo.org/investigation/2021/04/red-flags-the-first-year-of-covid-19-loan-fraud-cases

Schott, P. A. (2006). *Reference guide to anti-money laundering and combating the financing of terrorism*. [electronic resource] (2nd ed. and supplement on Special Recommendation IX.). The World Bank.

Seers, K. (2011). Qualitative data analysis. *Evidence Based Nursing*, *15*(1), 1–2. https://doi.org/10.1136/ebnurs.2011.100352

Shah, S. M. A. (2021). A qualitative study exploring challenges in money laundering investigations. *Journal of Money Laundering Control*. https://doi.org/10.1108/JMLC-09-2019-0070

Shaikh, A. K., & Nazir, A. (2020). A novel dynamic approach to identifying suspicious customers in money transactions. *International Journal of Business Intelligence and Data Mining*, *17*(2), 143–158. https://doi.org/10.1504/IJBIDM.2019.10010869

Sharafizad, J., & Coetzer, A. (2017). Women business owners' start-up motivations and network structure. *Journal of Management & Organization*, *23*(2), 206–223. https://doi.org/10.1017/jmo.2016.51

Shenton, A. K. (2004). Strategies for ensuring trustworthiness in qualitative research projects. *Education for Information*, *22*(2), 63–75. https://doi.org/10.3233/EFI-2004-22201

Shufutinsky, A. (2020). Employing use of self for transparency, rigor, trustworthiness, and credibility in qualitative organizational research methods. *Organization Development Review*, *52*(1), 50–58.

https://search.ebscohost.com/login.aspx?direct=true&AuthType=shib&db=bth&AN=142655477&site=eds-live&scope=site

Singh, K., & Best, P. (2019). Anti-money laundering: Using data visualization to identify suspicious activity. *International Journal of Accounting Information Systems*, *34*. https://doi.org/10.1016/j.accinf.2019.06.001

Sisira Dharmasri Jayasekara, S. G. (2021). Risk-based AML/CFT regulations for effective supervision. In Abdul Rafay, *Money Laundering and Terrorism Financing in Global Financial Systems*. Business Science Reference. https://doi.org/10.4018/978-1-7998-8758-4

Spencer Pickett, K. H., & Pickett, J. M. (2002). *Financial crime investigation and control*. John Wiley & Sons.

Stewart, M. S., & Hitchcock, J. H. (2016). *The scholar-practitioner's guide to research design* (1st ed.). Laureate Publishing.

Sykes, J. B. (2018). Trends in bank secrecy act/ anti-money laundering enforcement. *Congressional Research Service: Report*, 1–5.

Taylor, S. J., Bogdan, R., & DeVault, M. (2015). *Introduction to qualitative research methods: A guidebook and resource* (4th ed.). John Wiley & Sons.

Teichmann, F. M. J. (2020). Current developments in money laundering and terrorism financing. *Journal of Money Laundering Control*. https://doi.org/10.1108/JMLC-05-2019-0043

Tiwari, M., Gepp, A., & Kumar, K. (2020). A review of money laundering literature: The state of research in key areas. *Pacific Accounting Review*, *32*(2), 271–303. https://doi.org/10.1108/PAR-06-2019-0065

Wahyuni, D. (2012). The research design maze: Understanding paradigms, cases, methods, and methodologies. *Journal of Applied Management Accounting Research*, *10*(1), 69–80.

Weigand, F. (2021). *The Routledge Handbook of Smuggling* (1st ed.). Routledge. https://doi.org/10.4324/9781003043645

Weis, L., & Fine, M. (2012). Critical bifocality and circuits of privilege: Expanding critical ethnographic theory and design. *Harvard Educational Review*, *82*(2), 173–201. https://www.proquest.com/scholarly-journals/critical-bifocality-circuits-privilege-expanding/docview/1022988229/se-2

Whisker, J., & Lokanan, M. E. (2019). Anti-money laundering and counter-terrorist financing threats posed by mobile money. *Journal of Money Laundering Control*, *22*(1), 158–172. https://doi.org/10.1108/JMLC-10-2017-0061

Woodson, S. B. (2019). Money laundering and aspects. *International Journal of Tax Economics and Management*, *2*(11), 62-71. https://web.archive.org/web/20200321034239id_/https://journals.seagullpublications.com/ijtem/archive/f_IJ0920190356.pdf

World Health Organization. (2021). W*ho coronavirus (COVID-19) dashboard. World Health Organization*. Retrieved from https://covid19.who.int/

Wronka, C. (2022). “Cyber-laundering”: the change of money laundering in the digital age. *Journal of Money Laundering Control*, *25*(2), 330–344. https://doi.org/10.1108/JMLC-04-2021-0035

Yazan, B. (2015). Three approaches to case study methods in education: Yin, Merriam, and Stake. *The Qualitative Report*, *20*(2), 134–152. https://www.proquest.com/scholarly-journals/three-approaches-case-study-methods-education-yin/docview/2177067852/se-2

Yeandle, M., Mainelli, M., Berendt, A., & Healy, B. (2005). *Anti-money laundering requirements: Costs, benefits, & perceptions*. Z/Yen Group.

Yeoh, P. (2020). Banks’ vulnerabilities to money laundering activities. *Journal of Money Laundering Control*, *23*(1), 122–135. https://doi.org/10.1108/JMLC-05-2019-0040

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). Sage Publications.

Zagaris, B. (2020). Money laundering, bank secrecy, and asset recovery. International *Enforcement Law Reporter*, *36*(2), 44–46. https://heinonline.org/HOL/LandingPage?handle=hein.journals/ielr36&div=17&id=&page=

Appendix A: Invitation to Participate in the Study

Hello Mr./Mrs./Ms.,

There is a new study about the experiences of compliance managers with how the process of identifying predicate offense typologies helps them to reduce the risks of money laundering and terrorist financing activities. For this study, you are invited to describe your experiences identifying predicate offense typologies.

About the study:

- One 30-60 minute in-person interview that will be audio recorded
- You would receive a $20 Visa gift card as a thank you
- To protect your privacy, the published study would use code numbers

Volunteers must meet these requirements:

- Managers who currently work or worked in a supervisory position in the anti-money laundering division under the compliance department
- Current investigators who have experience or career background in anti-money laundering for more than three years
- Do not have a current direct working relationship with me to minimize any potential for perceived coercion.

This interview is part of the doctoral study for Sina Patel, a Ph.D. student at Walden University.

Please respond to this email to let me know of your interest. You are welcome to forward it to others who might be eligible to participate.

You can contact me by e-mail at [redacted] if you have any questions.

Kind regards,

Sina Patel

Appendix B: Codes Associated With Main Themes

No.	Code	Theme
1	Cryptocurrency	Cybercrime
2	Gift card	Cybercrime
3	Credit card	Fraud
4	Credit card charges close to borders	Human trafficking/smuggling
5	PPP loan	Fraud
6	SBA loan	Fraud
7	Cash in and out	Human trafficking/smuggling
8	Cash deposits	Structuring
9	Cash withdrawals	Structuring
10	Multiple cash activities	Structuring
11	Cash payments	Real estate money laundering
12	Redbox charges	Human trafficking/smuggling
13	Hotel expenses	Human trafficking/smuggling
14	Fast food charges	Human trafficking/smuggling
15	Gas station charges	Human trafficking/smuggling
16	Vending machine charges	Human trafficking/smuggling
17	Late night charges	Human trafficking/smuggling
18	Taxi/cab services	Human trafficking/smuggling
19	Unusual wire activity	Fraud
20	Split cash activity	Structuring
21	Overvaluation of property	Real estate money laundering
22	Undervaluation of property	Real estate money laundering
23	Cyber laundering	Cybercrime
24	Over-or-under invoicing	Trade-based money laundering
25	Telemarketing	Cybercrime
26	Romance scams	Cybercrime
27	Third party scams	Cybercrime
28	Housing market	Real estate money laundering
29	Shell companies	Real estate money laundering
30	Digital payment systems	Cybercrime
31	Weapons	Illicit arms trafficking
32	Firearms	Illicit arms trafficking
33	Substances	Illicit drug trafficking
34	Narcotics	Illicit drug trafficking
35	Goods	Trade-based money laundering
36	Services	Trade-based money laundering
37	Drug cartel	Illicit drug trafficking
38	International Trade	Trade-based money laundering
39	Unemployment status	Fraud

40	Different branch locations	Structuring
41	Below the reporting threshold	Structuring
42	Low dollar amount	Human trafficking/smuggling
43	Quick money movement	Human trafficking/smuggling
44	Quality misrepresentation	Trade-based money laundering

Note. PPP = Paycheck Protection Program; SBA = Small Business Administration.

Appendix C: Codes Associated With Subthemes

No.	Code	Subtheme
1	Cash	Red flags
2	Deposits	Key indicators
3	Withdrawals	Key indicators
4	Transfers	Key indicators
5	Wire	Red flags
6	Structuring	Typology-specific common signs
7	Credit cards	Red flags
8	Prepaid cards	Red flags
9	Fraud	Typology-specific common signs
10	Bitcoin	Red flags
11	Cryptocurrency	Red flags
12	Virtual currency	Red flags
13	Cybercrime	Typology-specific common signs
14	Automated clearing houses	Red flags
15	Trafficking	Human trafficking/smuggling
16	Excessive food, transport, and accommodations	Red flags
17	Transnational charges	Red flags
18	International large charges	Red flags
19	Changes to customer profile	Key indicators
20	Third party processors	Red flags
21	New account openings	Key indicators
22	Quality assurance	95% or above
23	Real estate	Typology-specific common signs
24	Inconsistent wealth profile	Key indicators
25	Quality control	95% or above
26	Big-ticketed item purchase or sale	Red flags
27	Trade-based	Typology-specific common signs
28	International shipping	Red flags
29	Unknown financial instrument use	Key indicators
30	95%-100%	95% or above
31	High quality AML investigations	95% or above

Note. AML = anti-money laundering.