THE IMPACT OF VIRTUAL ADDRESSES

On the Money Laundering Risk of Financial Institutions

WEB SHIELD®

TABLE OF CONTENTS

1. INTRODUCTION

The use of virtual addresses in connection with shell companies for money laundering or tax evasion purposes represents a growing phenomenon and has been in the focus of the public eye since the release of the Panama and Paradise Papers. Interestingly the detection or further analysis by regulators of the banking and financial industry lack clearly defined methodological tools to protect consumers from money laundering activities committed by individuals who may have membership in terrorist organizations. For the credit card payment industry however, the information contained in the Visa Europe Member Letter VE65/16 indicates that the intention to regulate money laundering activities requires enhanced due diligence relating to the location of a merchant. On January 19th. 2017, Visa updated its Merchant Location Rules and Compliance Program to clarify the criteria by which the principal place of business or the merchant location needs to be determined. More specifically, the criteria included in this recent update clarified that merchants must have a physical location to constitute for a merchant location and not a virtual one.

Restrictions included in the 2017 Visa update indicate that a physical location cannot include a post office boxes, a forwarded mail addresses, law firms affiliated with merchants, agents or vendors. Accordingly, the updated Visa regulations for merchants present a significant challenge if merchants want to establish businesses in multiple locations.

While classical businesses may sell or transfer operations to establish a new company or expand their business, this seems to be different with the online business and the raising number of service providers who rent virtual addresses to their clients suggests additional needs, aside from pure relocation or expansion.

1.1 Statement of the Problem

As this study explains, the problem of money laundering is conceptually ambiguous regarding its criminality and immorality. Yet, banking and financial institutions are not necessarily the primary agents of money laundering insofar as auditors and regulators possess the knowledge required to launch initiatives that could effectively mitigate the problem. Despite how money laundering involves so-called "dirty money" (Morris-Cotterill, 2001, p. 17), the problem extends only so far as regulators encourage merchants to establish professional relationships with clients. Merchants that accept credit and debit card transactions may establish relationships with customers by integrating third-party monitoring services into core business processes as a means of extending consumer protections.

Interestingly, the near-constant development of information and communication technologies (ICTs) exacerbates the problem. The strong expansion of various high-risk online businesses such as the exchange of virtual currencies like Bitcoin and the associated fraud warnings and online customer complaints indicate a dearth of regulatory mechanisms governing how financial institutions should establish business relationships with customers (Aboushi, 2017; Castri, 2013; Jayasree & Balan, 2017).

Key challenges related to the problem of money laundering and its relationship to virtual addresses reflect how financial institutions verify the identity of their customers who frequently are located in offshore financial centres. Accordingly, the challenge of verifying the ultimate beneficiary behind these entities entails that the regulators of banking and financial institutions should consider proposing stronger risk management frameworks to reduce or eliminate any ties with criminal organizations (Koker, 2009; Isa, Sanusu, Haniff & Barnes, 2015). Banking and financial institutions, that willingly put themselves at risk by not regulating money laundering activities, are complicit in the growing problem. However, the methodological approaches that produce findings with significant implications for ameliorating the problem of money laundering require fine-tuning insofar, as researchers address how the detection of virtual addresses, can effectively reduce the money laundering risk.

1.2 Rationale of the Study

Conducting a study that addresses the impact of virtual addresses on money laundering risk in financial institutions reflects a gap in the extant research literature. While financial institutions are responsible for knowing which business activities may or may not constitute money laundering practices, lawmakers and policy experts are equally responsible for providing them with sufficient guidance on how to identify the ultimate beneficial owner. As suggested by Seabrooke and Wigan (2017), money laundering represents an underground form of capitalism by which merchants may use virtual addresses to circumvent regulations mandating that customers leave a paper trail for regulators to consider during the auditing process. While regulators and policymakers are responsible for informing financial institutions of production processes required to fulfill legal and ethical obligations, merchants must also provide empirical evidence of how money laundering activities do not inform business operations in any way.

Countries with financial institutions that do not cooperate with existing policy frameworks instituted by national and international regulatory agencies may, therefore, present alarming statistics regarding their involvement with members of terrorist organizations (di Castri, 2013; Jayasree & Balan, 2017)). Here, Masciandaro (2005) highlighted how, in an earlier study, non-cooperative countries and territories engage in money laundering activities that are legal in some locations yet completely illegal in another. The differences in scope between policies enforced by regulatory agencies illustrate the importance of designing and employing a holistic risk-based methodology that produces results with empirical real-world implications.

1.3 Significance of the Study

This study is significant to the extent that money laundering through virtual addresses represents a problem insofar as individuals who participate in offshore banking activities contribute to crime and possible terrorism. In many cases, as Horst et al. (2014) found, the dominance of money laundering and related criminal activities indicates the lack of strong oversight by regulating agencies such as FATF and FinCEN that have emphasized the development of international standards for auditing risk in banking and financial institutions as well as enhancing consumer protections. Along these lines, this study is significant insofar as the shape of regulatory structures governing anti-money laundering practices requires attention such that compliance to ethical guideline reduces risks for merchants and consumers equally (Castri, 2013; Zoppei, 2015). Specifically, Lal and Sachdev (2015) noted how anti-laundering regulations mandate that financial institutions complete a registration process to not only produce value but also verify the identity of customers whose purchases exceed a minimum threshold.

Similarly, this study is significance by which "know your customer" policies become applicable not only for financial institutions, but also for merchants in high-risk industries, such as the exchange of virtual currencies to complete financial transactions using Bitcoin (Pieters & Vivanco, 2016, p. 2). More specifically, the content of anti-money laundering regulations entails that know-your-customer policies have strength only when financial institutions are legally and ethically compelled to enhance the quality of business relationships with consumers.

1.4 Research Questions and Hypothesis

For this project, the primary research question is: Which methodological approach should banking and financial institutions consider to reduce money laundering risk. The use of a virtual address in combination with indications for the use of a nominee director or beneficial owner seriously increases the associated money laundering risk for financial institutions. Accordingly, the ultimate beneficial ownership (UBO) remains obscure and a continuous monitoring for these virtual premises are crucial for deploying a holistic anti-money laundering approach (Kemal, 2014; Saperstein, Sant & Ng, 2015). Answering the primary research question and testing the working hypothesis will entail a detailed analysis of granular data broken down on a country-by-country basis. While the data analyzed in this study are confidential in nature, all of the 47,759 merchants from 170 countries received a manual audit by risk management and fraud prevention specialists. Moreover, answering the primary research question and testing the working hypothesis entails accounting for a direct view of which physical and virtual addresses require stronger oversight by lawmakers and policy experts who govern business activities in the banking and financial sectors.

2. LITERATURE REVIEW

Drawing from the Visa Europe Member Letter published on August 4, 2016, the research literature evaluated here pertains to how regulators in the banking and financial industry should clarify definitions of money laundering insofar as the requirements for addressing the problem enhance the quality of business relationships between financial institutions and consumers. Accordingly, the Visa Europe Member Letter requires, as of October 15, 2016, that each merchant must have a correct physical location and conform to operational regulations for utilizing virtual addresses. Three months prior to the aforementioned requirements, Visa Europe issued an official statement updating and clarifying all rules for merchants to ensure that the physical addresses remain both confidential and accurate. The intent of this literature review is to illustrate how important designing a holistic risk-based methodology is for improving decision-making processes as well as detecting behavioral patterns in completed transactions that some lawmakers and policy experts recognize as suspicious.

The Visa Europe Member Letter also recommended that financial institutions must institute due diligence requirements into core business processes before any consumers have opportunities to complete transactions. Here, consumer identification requirements receive a fair amount of attention by which acquirers can trace behavioral patterns in transactions that may raise some red flags among regulators enforcing policies at the state, national, or international levels. Even more specific to due diligence requirement is how merchants have the option of assigning different countries as outlet locations where consumers may use cash to complete transactions. Depending on the type of business conducted between merchants and customers and where they are located, the due diligence requirements have significance for designing a holistic risk-based methodology by which regulators in the banking and financial industry distinguish accurately between legitimate and criminal behaviors.

The information contained in the Visa Europe Member Letter illustrates further how acquirers may assign due diligence requirements to clean and virtual addresses in countries where money laundering activities are the likeliest to occur. Since this study evaluates the nature of money laundering activities on a country-by-country basis, the process of assigning due diligence requirements indicates that merchants should have more clean addresses than virtual addresses such that consumers who complete transactions using debit and credit cards are less likely to incur any major risks associated with making high-end purchases. Here, the research literature implies that due diligence requirements should inform the identity verification process by which each transaction has direct ties to one main source. Primarily because each location of a physical address held by merchants cannot include a post office box, a forwarded mail address, the address of law firms utilized by merchants, and an e-mail address, due diligence requirements have legal and ethical implications for ensuring that consumers can maintain a high degree of trust in businesses.

The research literature evaluated here also illustrates the value of disclosure requirements for merchants who complete business transactions predominantly in an online format. Disclosure requirements provide consumers with the transparent information required to feel safe in making large, high-end purchases on a frequent basis. While the Visa Europe Member Letter explains that this major financial institution has strengthened its disclosure requirements for merchants, the impact on consumer safety remains linked to whether lawmakers and policy experts initiate directives for ameliorating the problem of money laundering and reducing the probability of having any possible links to criminal or terrorist organizations.

The Visa Europe Member Letter also indicated that the major financial institution has a compliance program in place for assigning accurate addresses to merchants. Specific to transparency in communication, the website for Visa Europe explains how merchants must disclose a physical address for consumers who have legitimate questions or concerns about the nature of some transactions. In this regard, any due diligence requirements observed by Visa entail that acquirers should review physical and virtual business portfolios to detect any patterns in purchasing behaviors that could present red flags to regulators representing the banking and financial industry. As suggested in the following review of the research literature, the due diligence and disclosure requirements for enhancing consumer safety through anti-money laundering mechanisms reinforce the underlying significance of policy structures (Kemal, 2014; Wang & Ou, 2015; Zoppei, 2015). However, gaps between policy mechanisms enforced at the state, national, and international levels have direct impacts on how customers not only define safety yet also adopt a proactive stance toward not permitting money laundering practices to have negative impacts on economic well-being.

2.1 Money Laundering in Financial Institutions

Conceptually, money laundering has an ambiguous meaning in terms of its criminal and moral status. In an earlier study, Morris-Cotterill (2001) defined the criminality and morality of money laundering as involving activities such as hiding, moving, or investing funds in illegal operations. However, money laundering sometimes entails the use of offshore banking systems to circumvent tax regulations of any particular nation. Business leaders who engage in offshore banking activities, yet do not report the nature or existence of transactions to the appropriate authorities are guilty of money laundering insomuch as the strategies adopted to evade taxes have no legal support (Castri, 2013; Koker, 2009, 2013). Nevertheless, the business activities that legitimize money laundering illustrate the relativity of financial regulations and their applicability to each nation that has a high percentage of virtual addresses owned by major banking and financial institutions. Along these lines, Pellegrina and Masciandaro (2009) argued that laws adopted by the European Union (EU) to prevent money laundering are mostly in a premature state. Although 22 EU countries implemented anti-money laundering directives into law, the methodological approaches for regulating suspicious transactions do not lead to the production of empirical evidence that has significance for enforcing cross-national legal directives. Most empirical outcomes of anti-money laundering directives have a low probability of informing how financial researchers can predict how many suspicious transactions will appear on the radar of governing authorities.

In response to the previous critiques, Koker (2009) investigated the practical guidelines developed by the Financial Action Task Force (FATF) to combat money laundering activities by delineating the links to terrorist financing. Accordingly, the FATF guidelines, initially developed in 2003, contain 40 recommendations for employing a risk-based methodology and developing appropriate control measures for identifying and categorizing the risk that some money laundering activities finance terrorist organizations. The links between money laundering, offshore banking, and terrorist activities are, however, unknown up to this point. Despite the presence of this research gap, the FATF guidelines emphasize the mitigation of high-risk transactions that provoke the suspicions of financial regulators governing the activities of major financial institutions. Still, researchers who have studied money laundering extensively suggest that the risk-based methodology contained in the FATF guidelines recommend listing terrorist activities as a sufficient predicate.

Irwin, Slay, Choo, and Lui (2014) noted how financial activities that involve transferring money between overseas accounts could represent attempts to disguise terrorist activities. More pertinent to this study, the use of Internet technologies facilitates the ease at which terrorist organizations could engage in money laundering activities. Some of the possible activities that may represent attempts to disguise money laundering by terrorist organizations include credit card theft, phishing, hacking, and keylogging attacks (Irwin et al., 2014, pp. 50-51). The nature of these activities, in turn, presents valid concerns for measuring the empirical value of findings that indicate whether money laundering activities have any direct links to terrorist organizations.

Concerning the problem of money laundering, Lo (2016) observed how regulators who oversee activities in the banking and financial industry find technological innovation somewhat threatening. Particularly in the United States, the Bank Secrecy Act (BSA) of 1970 is only one of several regulations that focus primarily on the need for merchants to document transaction activities in physical databases. Specific to this regulation, FinCEN is responsible for enforcing regulations designed to prevent merchants and individuals from engaging in money laundering activities (Lo, 2016; Luther, 2016). While FinCEN is largely responsible for controlling the nature of money business services, at least six exemptions allow merchants to transmit money by using virtual addresses.

These exceptions, as follows, include the provision of network infrastructures to money transmitters, specific types of payment processors, specific types of clearance and settlement systems, the physical transportation of currency, providers of prepaid access, and individuals who accept and transmit funds considered integral to sustaining merchandise functions (Lo, 2016, p. 114). Accordingly, these exceptions contain no legal mechanisms capable of protecting broader consumer interests. Based on this information, an important inference to make is that several legal loopholes allow FinCEN to overlook the nature of some money laundering activities by categorizing them as legitimate business activities under state, federal, and even international law (Levi, 2015). Such loopholes imply further that efforts to enact anti-money laundering laws are mostly ineffective in their prematurity.

The research literature suggests that compliance frameworks concerning risk management applied on the merchant level, deliver more consumer protections based on due diligence requirements. Helmy, Zaki, Salah, and Badran (2016) commented on how money laundering regulations containing due diligence requirements effectively contribute towards building lasting relationships with customers and recognize suspicious activity wherever possible. In the same regard, due diligence requirements mandate that merchants should know which institutions facilitate strong and lasting professional relationships (Flores, Angelopoulou & Self, 2013).

Jia, Zhao, and Zhang (2013), in an earlier study, noted how due diligence requirements represent internal mechanisms by which merchants verify the identity of each customer and audit the nature of suspicious transactions accordingly. Here, a risk management framework is applicable toward designing a holistic methodology that merchants may integrate into business practice to mitigate suspicious transactions involving virtual addresses from having negative implications for maintaining relationships with customers (Isa et al., 2015). Such a framework entails on-site auditing procedures that inform regulators who oversee the banking and financial industry as well as members of the intelligence community who may identify potential links between suspicious transactions and membership in terrorist organizations.

Drawing from the previous information, researchers have commented on how information and communication technologies (ICTs), while vital, play a major role in fostering the conditions for money laundering and other types of illegal financial activities. Budik and Schlossberger (2015) addressed how the misuse of financial systems for money laundering purposes continues to require interventions from both regulators of the banking and financial industry and lawmakers. Specific to the Czech Republic, a law enacted in 2008 illustrates how merchants may exercise discretion in requiring that customers whose transactions equal or exceed a threshold provide information to complete a verification process. Considering the rapidity at which ICTs develop, the risk management strategies integrated into practice to verify the identity of customers should receive more detailed attention insofar as money laundering practices occasionally involve the theft of intellectual property (Isa et al., 2015). Yet, the specific requirements for addressing virtual addresses in the use of money laundering activities reinforce the problem based largely on policy inconsistencies applied at the state, national, and international levels.

2.2 Requirements for Addressing Virtual Addresses in Money Laundering

A substantial portion of the research literature highlights *de minimis* requirements that indicate a low risk for merchants as having any involvement in money laundering activities linked to customers who may represent terrorist organizations. Specifically, Koker (2009) described *de minimis* requirements as indicating that some banking and financial institutions tolerate money laundering activities to some degree yet have formal policies in place to reduce the risks incurred from maintaining business relationships with individuals who practice offshore banking or have some connections to members of terrorist organizations. Along these lines, Jakobi (2015) commented on how the requirements for employing a risk-based approach to prevent money laundering should depend less on assessing whether individual transactions constitute money laundering but, instead, on whether broad guidelines can effectively delegate responsibility for identifying key patterns indicating problematic behaviors. Taken together, the research literature reviewed here provides valuable information about the fragmented nature of policy frameworks allowing regulators to oversee business activities.

In relation, the research literature illustrates the importance of constructing models that govern anti-money laundering policies to detect merchant compliance with industry regulations considered applicable at the national and international levels. Here, Wang and Ou (2015) described how regulatory requirements for the banking and financial industry in China fulfill the concepts and standards for prohibiting money laundering. Banking and financial institutions in China must follow strict national guidelines controlling how merchants may not only use Internet technologies but also use virtual addresses to complete each transaction. However, the regulating mechanisms for virtual currencies in China have not received any mentioned by researchers who have studied the impact of virtual addresses on merchants and consumers.

Despite the aforementioned research gap, some of the literature provides insights into the nature of mechanisms prohibiting tax evasion through money laundering practices. Considering the mining processes used to increase the value of virtual currencies, the legal and policy mechanisms that prohibit tax evasion have significance insofar as individuals who may have some connection to terrorist organizations utilize ICTs to detect whether regulatory agencies intend to audit the nature of business transactions completed when merchants use virtual addresses (Castri, 2013; Donahue et al., 2017; Koker, 2009, 2013). Accordingly, the legal and policy mechanisms that allow merchants to monitor the nature of high-value business transactions also influence whether banking and financial institutions adopt similar methodological frameworks to assess the empirical implications of overlooking activities that some public sector agencies legitimately define as constituting money laundering practices.

In relation, the legal research confirms how the fragmented state of regulations in the banking and financial industry demand closer attention by lawmakers and policy experts at the state, national, and international levels (Lo, 2016). Merchants or banking and financial institutions that experience some regulatory burdens must rely on divergent conceptualizations of terms defining money laundering between multiple transaction contexts. Depending on the payment methods accepted by merchants, the likelihood that some transactions bear any similarity to money laundering is largely contingent on whether the management sector has sufficient compliance mechanisms in place. At the same time, the types of customers merchants attract may reinforce the contingency of mechanisms adopted to prohibit the use of virtual addresses from inadvertently excusing money laundering practices.

Concerning the effective prevention of money laundering, the requirements for completing prudent business transactions are applicable to the inclusion of publicly traded firms on watch lists. For these requirements, the study by Armour, Mayer, and Polo (2017) presented information about the objectives of anti-money laundering practices as having implications for ensuring that merchants maintain high levels of confidence in market performance, enhance consumer safety, facilitate an increase in public awareness of financial systems, and reduce the probability that individuals will complete business transactions with some connections to criminal or terrorist organizations. While confidence in market performance refers to the ability of firms to increase profits based on their advertising potential, Armour et al. (2017) pointed out how the enhancements to consumer safety reinforce how each business transaction should protect the interests of key external stakeholders who control the level of investment in resources used for instituting effective policy mechanisms governing how merchants use virtual addresses to maintain core business operations.

In this context, the regulations that protect investors from the risk of fraud through money laundering should apply equally to consumers who rely on the quality of business relationships with merchants. On a country-by-country basis, as this study suggests, the regulations that apply directly to consumer and investor protections are significant for ensuring that merchant may stimulate economic development as ethically as possible. However, no sources to date provide a thorough investigation into the ethical implications of conforming to requirements for addressing the use of virtual addresses toward completing business transactions that involve money laundering. Despite that research gap, Rahman (2013) mentioned in an earlier study how the reporting of suspicious transactions that may resemble money laundering practices must refer to specific regulations or conditions that often incur fines for merchants that knowingly use virtual addresses to circumvent existing policies. However, the formal requirements for reporting suspicious business transactions present several challenges for ensuring that the outcomes for merchants and customers reflect an accurate application of risk-based methodologies.

Insofar as the regulations and policies instituted to prohibit money laundering apply differently at the state, national, and international levels, the requirements for reporting suspicious transactions lack sufficient mechanisms for establishing possible connections to criminal or terrorist organizations. However, as Jia et al. (2013) initially observed, the reporting requirements should involve on-site inspections that apply specifically to assessments of internal procedures that produce volumes of measurable data on an empirical basis. Although due diligence requirements have their use for ensuring that merchants may effectively enhance consumer safety, the task of verifying the identity of customers who frequently make large transactions with a merchant should incentivize regulators in the banking and financial industry to introduce special provisions for preventing any money laundering activities from having negative impacts on firm-level performance.

In a more qualitative fashion, researchers who employed a Bayesian approach for reporting suspicious financial activities noted how compliance requirements incentivize individuals who engage in money laundering activities to circumvent existing regulations by exploiting large loopholes. Khan, Larik, Rajput, and Haider (2013) noted in their earlier study that the Bayesian approach provides regulators in the banking and financial industry with opportunities to identify empirical patterns of suspicious behavior accurately. The Bayesian approach entails that regulators develop score computations and compile them into aggregate variables to locate evidence of suspicious transactions. However, researchers who employ the Bayesian approach should consider measuring the intervals at which individuals and merchants complete suspicious transactions by using virtual addresses.

Along these lines, Koker (2013) suggested implicitly that quantitative methodologies like the Bayesian approach may help banks identify the potential for risk as business operations expand. In these cases, designing a holistic methodology for measuring the risk incurred from money laundering entails that researchers must design an alternative approach that emphasizes the tendency for customers to abuse existing regulations. Particularly at the national level, the designs of holistic risk-based methodologies that include qualitative and quantitative measurements should provide both regulators and banks opportunities to close large gaps between definitions of risk management practices (Isa et al., 2015). Yet, insofar as FATF and FinCEN are responsible for overseeing how effectively merchants prevent money laundering, the process of designing a holistic risk-based methodology entails that researchers should also construct a working typology for identifying which countries are the most and least likely to have regulations providing support for money laundering activities.

More problematic with regard to the impact of virtual addresses is how the process of enacting consumer protection laws is mostly underdeveloped. Such a status reinforces the largely fragmented nature of anti-money laundering laws enacted at the state, national, and international levels (Kemal, 2014; Saperstein et al., 2015). Here, Luther (2014) remarked on how the requirements for enacting consumer protection laws situate individual impacted by money laundering as passive victims who lack sufficient information to take action on issues with direct impacts on their economic livelihood. The treatment of consumers as passive victims of money laundering indicates further that competition between banks in the global economy does not lend any credence to mitigating the problem.

Alternatively, consumers have the option of urging lawmakers and policy experts to design more effective regulations capable of preventing money laundering activities from negatively impacting economic well-being. Despite how banks may express a genuine interesting in enhancing consumer protections over maximizing profits, the task of designing a holistic risk-based methodology that encourages action should entail delivering economic incentives for minimizing patterns of systemic abuse as observed in suspicious transactions (Khan et al., 2013; Koker, 2013; Luther, 2014).

More recently, Helmy et al. (2016) commented on how due diligence requirements allow to understand better why some consumers frequently make high-end purchases. Despite how financial institutions who strongly support technological innovation may integrate detection techniques to monitor the transaction activities of some consumers, due diligence requirements occasionally produce false alarms suggesting that some individuals have ties to criminal or terrorist organizations that may use virtual addresses toward engaging in money laundering practices (Flores et al., 2013). Depending on the mechanisms that regulators in the banking and financial industry enact, financial institutions should obtain full information concerning which due diligence requirements control the degree of security in each completed transaction. Unfortunately, as noted by Rasul (2018), due diligence still does not receive sufficient attention in the research literature insomuch as financial institutions have legal and ethical incentives to prevent money laundering from having any adverse impacts on core business functions. Considering how certain high-risk business types encourage the use of virtual addresses and therefore hide the illicit motives for engaging in money laundering activities, the limitations to due diligence requirements present ongoing challenges pertaining to how financial institutions negotiate with lawmakers and policy experts.

2.3 Summary of the Literature Review

The problem of money laundering in financial institutions remains ambiguous insofar as its criminal and moral status entails the use of offshore banking systems to circumvent tax regulations (Morris-Cotterill, 2001). While several nations have lawmakers and policy experts who have proposed regulating business activities to mitigate money laundering, the literature reviewed here indicated that most empirical outcomes of anti-money laundering policy directives are insufficient in their scope (Mei, Ye & Gao, 2014; Me & Zhou, 2014; Pellegrina & Masciandaro, 2009). Notwithstanding the regulatory authority of FATF, FinCEN, and SEC, any proposals for instituting new regulations that govern money laundering practices illustrate further how the use of virtual addresses effectively facilitates the ease at which criminal and even terrorist organizations may hide under a cloak of anonymity to avoid detection (Bridy, 2016; Castri, 2013; Irwin et al., 2014; Koker, 2009, 2013). To the extent that clients of financial institutions make use of virtual addresses to engage in money laundering practices, the research literature review indicated that the use of virtual addresses to engage in money laundering practices reflects the inconsistency in enforcing policy directives across decentralized frameworks adopted by stakeholders who represent the public and private sectors.

Secondly, the preceding literature addressed de minimis and due diligence requirements for identifying a risk that clients will have any involvement in money laundering activities linked to terrorist organizations. The literature suggested primarily that the requirements for designing a holistic risk-based methodology to ameliorate the problem of money laundering should depend more on broad guidelines delegating responsibilities for identifying key patterns in problematic behaviors (Jakobi, 2015; Koker, 2009). The literature review also indicated that the development of new anti-money laundering regulations should close large research gaps pertaining to the increased popularity and general value of virtual currencies (Donahue et al., 2017; Saperstein et al., 2015; Wang & Ou, 2015). While de minimis requirements entail that FATF and FinCEN continue to play key roles in preventing money laundering, due diligence requirements mandate the reporting of suspicious transactions to the proper authorities (Böhme et al., 2015; Enweremadu, 2013; Flores et al., 2013). More pertinent to this discussion of how the holistic risk-based methodology proposed in this study should include due diligence requirements adopted by banking and financial institutions as tools for identifying unusual behavioral patterns in each transaction completed by clients.

Considering the methodology selected for this study, its quantitative nature has significance for explaining the empirical country-by-country impacts and dissemination of virtual addresses on money laundering behaviors. Applying an exploratory methodology aims to fulfill the purpose of closing research gaps and other inconsistencies in applications of policy frameworks adopted by the state, national, and international governing authorities. Given the quantitative nature of the data assessed in this study, the main research implications of applying an exploratory methodology illustrate how regulators in the banking and financial industry should identify multiple causes of money laundering practices facilitated by the use of virtual addresses.

3. METHODOLOGY

The research methodology selected for this study is quantitative in nature. Given that the data analyzed were granular and provided on a country-by-country basis, the quantitative nature of this study aims to close gaps regarding the measurements of money laundering practices. As noted by Gelb (2016), no standard method for measuring the impact of money laundering that involves merchants using virtual addresses to complete business transactions corresponds to how lawmakers and policy experts aim to regulate activities in the banking and financial industry. Nevertheless at least three methods identified in the research literature – gravity models, pricing aberrations, and rational monitoring – provide some indications as to the impact that virtual addresses may have on consumer safety when banking and financial institutions have sufficient policy mechanisms in place to manage risk holistically as well as prevent money laundering practices from implicating these institutions from having any direct involvement in terrorist activities. Considering how high-risk businesses, e. g. the exchange of virtual currencies like Bitcoin, have increased in popularity, the drivers of technological innovation confirm how no standard methods exist for measuring the impact of virtual addresses held by each merchant included in the entire sample.

3.1 Research Design

The research design constructed for this study is exploratory in nature insofar as the central purpose of answering the primary research question is to provide working solutions for existing problems. One important caveat to make about studies with an exploratory research design is that the problem assessed requires further clarification in future studies. In many ways, exploratory research designs provide the backdrop for conducting pilot studies explaining the potential effect of changes to regulatory frameworks on consumer safety. Considering how the virtual addresses identified in this study have specific country-by-country implications, the solutions proposed here aim to provide researchers and regulators in the banking and financial industry with objective models capable of testing the empirical strength of legal and ethical safeguards implemented to protect merchants and consumers from having any involvement in money laundering activities potentially facilitated by members of terrorist organizations. Accordingly, the exploratory nature of this study will allow researchers who conduct future investigations to deliver more conclusive results on a country-by-country basis. Although the sample of merchants included in this study presents legitimate concerns for discussing the use of virtual addresses to complete business transactions, the exploratory research design can provide future opportunities to close large research gaps concerning all possible legal and ethical implications for enhancing consumer safety through procedures like customer verification. More specific to this study, exploratory research designs provide researchers with multiple explanations of causes underlying the problem of virtual addresses and their impact on anti-money laundering regulations. Despite how exploratory studies may lack the rigor of most quantitative methodologies, the sample size provides substantial granular-level data that have strong implications for identifying which regulatory issues require attention at the state, national, and international levels. Many of the results produced in exploratory studies have extended significance for recommending improvements to decision-making processes that facilitate improvements in business relationships between merchants and customers. As such, the advantages of employing an exploratory research design to this study imply that any raw data generated from proprietary sources should entail third-party oversight insomuch as the personal information included in virtual and clean addresses is confidential Notwithstanding the criticisms that exploratory studies do not produce results generalizable to larger populations, the country-by-country data assessed in this study illustrate how even small differences in regulatory mechanisms are completely reflective of differences in regional and cultural norms. Rather, the purpose of employing an exploratory research design is to provide researchers with a detailed overview of which countries are the most likely to engage in money laundering practices. Considering the growing popularity of high-risk businesses, the purpose of employing an exploratory research design is to provide regulators in the banking and financial industry with strong recommendations for instituting structural reforms to ameliorate the problem.

3.2 Instrumentation

While this study was exploratory in nature, the instrumentation used was based on the investigative risk analyses (Chmiel & Prause, 2016), combining the collection of various indicators and a manual false positive clearing of the gained results by money laundering professionals of Web Shield Services GmbH[1]. In doing so, Web Shield evaluated a probability value between 0% and 100% if an address could be considered as virtual. This was applied to a total number of 53.461 addresses from over 150 global banks and financial service providers in the timeframe between January 1st, 2018 and June 3th, 2018[2] .

The addresses were gathered as part of an application process for credit card acceptance from online merchants and analyzed in context with the regulations regarding the determination of the principal place of business as established by the Visa Europe Member Letter VE65/16.

[1] Web Shield Services GmbH (www.webshield.com) is a provider for anti-money laundering online due diligence and monitoring services to the financial industry.

Given that the exact process of evaluating probability is considered a trade secret, the following discussion is merely a rough description of the crafting practice for determining the virtual presence. The following seven steps have been declassified and released for publication.

1. Country Risk: The probability score is based on a specific country or geographical risk issued by KnowYourCountry Limited[3]. Thereby the risk scoring reflects whether a jurisdiction is a conduit for offshore financial centers.

2. Number of Registered Entities: The probability score considered the number of registered entities at a specific address, whereas the details of the applied scale has not been shared.

#	High-Risk Area	#	High-Risk Area
1.	Accountant & Legal Services	23.	Massage Parlors
2.	Adult Entertainment	24.	Money Transfer Services
3.	Agricultural Companies	25.	Multi Level Marketing
4.	Alcohol / Liquor stores	26.	Nutraceuticals
5.	Art Dealers and Galeries	27.	Payday Loans
6.	Beauty Salons	28.	Payroll Services
7.	Binary / Forex Services	29.	Penny auctions
8.	Casinos	30.	Pharmacy
9.	Charity Business	31.	Precious Stones and Metals, Watches and Jewelry
10.	Chemicals	32.	Religious Organizations
11.	Collection Agencies	33.	Restaurants
12.	Construction	34.	Tanning Studios
13.	Credit Repair	35.	Tech Support
14.	Crypto Exchange	36.	Telemarketing
15.	Dating / Escort	37.	Timeshare
16.	Drug Dispensaries	38.	Tobacco
17.	Drugs	39.	Travel
18.	Estate Management	40.	Incorporation and Secretary Services
19.	Financial Services	41.	Vehicle Sales
20.	Import / Export	42.	Virtual or Remote Office Providers
21.	Insolvency Services	43.	Weapon Sales
22.	Mail Forwarding Services		

[2] Annex 1 contains the full list of analyzed countries. The strong European focus is due to the fact that Web Shield Services GmbH operates out of Germany and clients come primarily from the European area.
[3] KnowYourCountry Limited is a provider of on-line information of money laundering and sanction information on a country by country basis (www.knowyourcountry.com, 13.01.2019).

3. Identified or Advertised High-Risk Business: The probability score considered if any high-risk business areas are online advertised for the analyzed address. In total, the below 42 high-risk areas have been included into the research:

4. Identified Online Fraud Indicators: The probability score considered if any online fraud or scam warnings have been issued for the researched address, as virtual addresses are often used by fraudsters due to the alleged anonymity.

5. Identified Online Customer Complaints: The probability score considered if any online customer complaints have been identified for the researched address, as virtual offices are often used by deceptive online merchants and money balancing schemes.

6. Offshore Leak Databases: The probability score considered if the researched address has been identified in any leak database (such as the Panama or Paradise Papers).

7. Vicinity Analysis: The probability score considered if confirmed virtual addresses are in the vicinity of the address in question, because in some areas entire streets or even communities (Pal & Ojha, 2016) are affected by the phenomenon of virtual addresses.

In the final verification step the gathered results were reviewed for false / positives by any-money laundering professionals and Google Streetview was applied to cross-verify and estimate the accuracy of confirmed virtual addresses included in this study. Features in Google Maps and Google Earth, Google Street View offers Internet users with panoramic views of almost every physical street in the world. While Google Street View initially gained traction in large metropolitan areas, the application technology has expanded into rural areas and otherwise overlooked geographical territories. Thanks to the drivers of innovation underlying Google's business activities, the use of Google Street View to confirm the location of clean and virtual addresses was helpful toward employing an exploratory research design. Most of the photographic images provided to Internet users who access Google Street View are taken from moving automobiles.

In many unique ways, the instrumental value of Google Street View provides researchers in the banking and financial industry with valuable information for performing internal audits on transactions histories completed between merchants and customers who may have some involvement in terrorist organizations. Accordingly, researchers who employ an experimental design to study the impact of virtual addresses on anti-money laundering practices may complete time-and-motion logs documenting any extreme shifts in merchant and consumer behaviors over a specific period of time. However, the empirical validity and reliability of the study results should incentivize researchers to consider determining which solutions for solving the problem of money laundering are applicable in multiple business contexts.

Google Street View involves the use of immersive media technologies to provide digital snapshots of physical addresses located through user searches. Most pictures of physical addresses captured by cameras connected to Google Street View are pixelated and do not involve the use of a fish-eye lens to capture panoramic images. As with all mapping and location services, the position of recorded photographs that confirmed the virtual addresses of merchants included in this study must be accurate. Here, the use of Global Positioning System (GPS) technologies and navigation sensor data were integral for capturing accurate images of clean and virtual addresses that could have direct involvement in money laundering practices. Vehicles that contain data recording equipment were also useful in capturing the images of confirmed clean addresses of merchants accounted for in the country-by-country results. While it was not possible for any cameras equipped with Google Street View equipment to capture any images from the inside of clean addresses, the information assessed here is significant towards explaining how differences in national-level regulations facilitate the continuance of money laundering practices between merchants and consumers who may have some affiliation with terrorist organizations that use virtual currencies to achieve financial gains.

3.3. Validity and Reliability

In research studies that apply exploratory study designs, validity and reliability are significant for producing accurate results from the impact of variables measured. More specifically, validity has at least three different subtypes that reflect the degree of consistency contained in empirical results. Whereas internal validity indicates a high degree of consistency in results across variables, external validity refers to the capacity for the results of this study to have generalizable impacts on the results of future studies. Primarily because this study employs an exploratory research design, the procedures used to check for internal and external validity must reflect the accuracy of data collected by instruments such as Google Street View. Along these lines, content validity in exploratory research studies pertains to the appropriateness of applying instruments like Google Street View to confirm the existence of clean and virtual merchants on a country-by-country basis. Content validity also refers to the accuracy of results produced by researchers who collect and analyze data included in questionnaires and observation logs. Since no human subjects participated in the raw data gathering process, the use of observation logs must inform the degree of content validity across results provided on a country-by-country basis.

More specific to this study, reliability has significance insofar as the accuracy of results included in this study indicate predictive outcomes for researchers who conduct future empirical investigations included to close large research gaps. However, the reliability of results included in this study is not as important as their validity. While instruments like Google Street View are equally valid and reliable, the results that confirm the existence of clean and virtual merchant addresses must provide researchers of future studies with valid measures for assessing the real impact of anti-money laundering regulations. Similarly, the validity of results produced by applications of these instruments should contribute to knowledge and professional development in the banking and financial industry.

3.4 Ethical Considerations

The ethical considerations noted in this study pertain directly to the use of mapping and location services like Google Street View to confirm the clean and virtual addresses of merchants included on a country-by-country basis in this exploratory study. While this study does not involve any direct contact with human research participants, the sensitive nature of the data assessed in this study required special attention to privacy concerns. Here, the use of research, mapping and location services like Google Street View entailed that the principal investigator could use any personal information discovered throughout the entire investigative process.

Primarily because the clean and virtual addresses obtained in this study were confidential, ethical considerations pertaining directly to anonymity were important to consider. Insofar as the data collected and analyzed in this study were relevant on a country-by-country basis, each of the components highlighted has potential implications for identifying strong linkages between money laundering practices and terrorist activities. Similarly, each of the components highlighted in the datasets is relevant for identifying where regulators who oversee the banking and financial industry may work toward reducing policy deficits as deemed necessary.

As explained further in the next section, the money laundering risk of each country depends on the limited reach contained in regulations governing the banking and financial industry. Any initiatives developed and implemented to prevent money laundering and its potential links to terrorist activities should reflect the accuracy of results included in evaluations of program components instituted to enhance consumer safety. Similarly, the ethical implications of results produced in this study are unique in compelling researchers of future studies to draw from preliminary findings. In considering the wide policy gaps for the banking and financial industry are present at the state, national, and international levels, the task of designing effective policy mechanisms from smaller datasets necessitates closer attention to how policy initiatives achieve their intended goal.

4. RESULTS

The results of this study draw from the granular nature of the country-by-country data. While the data could have been categorized by geographical region, the purpose of compiling the results on a country-by-country basis indicates that researchers should not make blanket generalizations concerning how merchants may or may not engage in money laundering practices that have some linkages to the funding of terrorist activities. To protect the confidentiality of merchants who used virtual addresses, no names of merchants that have reported connections to money laundering and terrorist activities were mentioned in this study. The country-by-country data analyzed in this section indicate the number of confirmed clean addresses, the number and percentage of confirmed virtual addresses, the total number of merchants, and the average number of addresses per merchant. Accordingly, the results of this study have significance in illustrating how the fragmented scope of regulatory and policy frameworks for banking and financial institutions have serious implications for enhancing consumer safety.

While it was presumed that the United States has a high percentage of virtual addresses, the United Kingdom presented alarming results. From a total of 9,519 addresses for 8,517 merchants in the United Kingdom, this county had 1,482 (15.6%) confirmed virtual addresses and 1.06 addresses for each merchant. By comparison, the United States had only 439 confirmed addresses (6.4%) for 6,120 merchants having an average of 0.96 addresses per merchant. Of further note is how the United States had 6,402 confirmed clean addresses of 6,841 total addresses. Canada had nearly as many merchants with confirmed clean addresses. However, this country had only 51 (0.8%) confirmed virtual addresses out of 6,225 total addresses and 0.90 addresses per merchant. Germany ranked as having the fourth most number of confirmed clean addresses. However, Germany has fewer clean addresses than the United Kingdom, the United States, and Canada has. Germany had 4,123 confirmed clean addresses and 60 confirmed virtual addresses to indicate a higher percentage (1.4%) for the latter out 3,742 merchants that had a total of 0.91 addresses per merchant.

Interestingly, the Netherlands ranked fifth in its number of confirmed addresses. This EU country had 3,412 confirmed clean addresses and 83 virtual addresses. However, the percentage of confirmed virtual addresses in the Netherlands (2.4%) was higher than that for Germany and Canada despite how the number of addresses per merchant (0.92) per merchant was relatively similar across all four countries. Belgium and India ranked sixth and seventh in the number of clean addresses, yet both countries had only four confirmed virtual addresses. While Belgium had 2,949 confirmed clean addresses for 2,642 merchants, India had 2,936 confirmed clean addresses for 2,630 merchants. Both India and Belgium had 0.90 addresses for each merchant. Next, Denmark ranked eight in its number of confirmed clean addresses. This Scandinavian country had 2,834 confirmed clean addresses and only 14 (0.5%) confirmed virtual addresses. As with Belgium and India, Denmark had an average of 0.90 addresses for each merchant.

Cyprus, though ranking ninth, had 316 confirmed virtual addresses and only 1,003 clean addresses. Accordingly, almost one-fourth (24.0%) of the 1,319 addresses were virtual for the total number of 1,180 merchants that each had an average of 1.18 addresses. Although France has a lower number of confirmed clean addresses (n = 949), the number of confirmed virtual addresses (n = 38) represents only 3.9% percent of the 987 total addresses. France, more interestingly, had only 883 merchants included in the results while each merchant had, on average, 0.93 addresses. Sweden, unlike its Scandinavian counterpart in Denmark, had only eight confirmed virtual addresses and 869 confirmed clean addresses. These results indicate that the number of virtual addresses in Sweden account for only 0.9% percent of the 877 total addresses included in this survey. As highlighted in this Table 1, Sweden had 784 merchants included in this survey and 0.90 addresses per merchant.

More interestingly, the Russian Federation had only nine confirmed virtual addresses and 719 confirmed clean addresses indicating that only 1.2% of merchants may have reportedly engaged in money laundering practices. As noted in this survey, the Russian Federation had 651 merchants and an average of 0.91 addresses per merchant. Following the Russian Federation, the Eastern European country of Bulgaria had a total of 595 confirmed clean addresses. However, Bulgaria had 52 confirmed virtual addresses (8.0%) out of 647 addresses total. Bulgaria also had 578 merchants included in this survey and more addresses per merchant (n = 0.97) than most of the other countries mentioned so far with the exceptions of the United States and Cyprus. Moving into the Baltic States, Estonia had a total of 568 confirmed clean addresses yet had 60 (9.6%) confirmed virtual addresses, 561 merchants, and 0.99 addresses per merchant. Next in rank is Spain to the extent that this EU country had 563 confirmed clean addresses and only 16 (2.8%) confirmed virtual addresses. Spain had 518 total merchants included in this survey and had 0.92 addresses for each merchant.

Also, in the EU, Switzerland had 552 confirmed virtual addresses included in this survey and 26 (4.5%) confirmed virtual addresses. Switzerland also had a total of 517 merchants included in this survey and an average of 0.94 addresses per merchant. Moving eastward from the EU, the United Arab Emirates (UAE) had 505 confirmed clean addresses and only 32 (6.0%) confirmed virtual addresses. UAE had 480 merchants included in this survey, and each merchant had 0.95 addresses. Italy ranked shortly behind UAE in having 494 confirmed clean addresses and only 13 (2.6%) confirmed virtual addresses. Italy had a total of 453 merchants included in this survey and 0.92 addresses per merchant.

In the Baltic states, Latvia had a reported total of 464 confirmed clean addresses and only 6 (1.3%) confirmed virtual addresses included in this survey. Latvia had a total of 420 merchants included in this survey and 0.91 addresses per merchant. Similarly, Norway had 455 confirmed clean addresses and only 7 (1.5%) confirmed virtual addresses. Norway had 413 merchants included in this survey and, much like Latvia, had 0.91 addresses for each merchant. Austria had the next lowest number of

#	Country	Total Number of Addresses	Confirmed Clean Addresses	Confirmed Virtual Addresses	Percent	Number of Merchants	Addresses per Merchant
1	United Kingdom	9.519	8.037	1.482	15,6%	8517	1,06
2	USA	6.841	6.402	439	6,4%	6120	0,96
3	Canada	6.225	6.174	51	0,8%	5569	0,90
4	Germany	4.183	4.123	60	1,4%	3742	0,91
5	Netherlands	3.495	3.412	83	2,4%	3127	0,92
6	Belgium	2.953	2.949	4	0,1%	2642	0,90
7	India	2.940	2.936	4	0,1%	2630	0,90
8	Denmark	2.848	2.834	14	0,5%	2548	0,90
9	Cyprus	1.319	1.003	316	24,0%	1180	1,18
10	France	987	949	38	3,9%	883	0,93
11	Sweden	877	869	8	0,9%	784	0,90
12	Russian Federation	728	719	9	1,2%	651	0,91
13	Bulgaria	647	595	52	8,0%	578	0,97
14	Estonia	628	568	60	9,6%	561	0,99
15	Ireland	623	562	61	9,8%	557	0,99
16	Spain	579	563	16	2,8%	518	0,92
17	Switzerland	578	552	26	4,5%	517	0,94
18	Malta	542	435	107	19,7%	484	1,11
19	United Arab Emirates	537	505	32	6,0%	480	0,95
20	Italy	507	494	13	2,6%	453	0,92
21	Latvia	470	464	6	1,3%	420	0,91
22	Norway	462	455	7	1,5%	413	0,91
23	Austria	351	348	3	0,9%	314	0,90
24	Czech Republic	321	269	52	16,2%	287	1,07
25	China	284	275	9	3,2%	254	0,92
26	Lithuania	246	235	11	4,5%	220	0,94
27	Hongkong	243	203	40	16,5%	217	1,07
28	Poland	218	199	19	8,7%	195	0,98
29	Australia	195	175	20	10,3%	174	0,99
30	Ukraine	183	183	0	0,0%	163	0,89
31	Slovakia	147	131	16	10,9%	131	1,00
32	Luxembourg	134	121	13	9,7%	119	0,98
33	Slovenia	121	114	7	5,8%	108	0,95
34	Singapore	114	98	16	14,0%	102	1,04

#	Country	Total Number of Addresses	Confirmed Clean Addresses	Confirmed Virtual Addresses	Percent	Number of Merchants	Addresses per Merchant
35	Israel	113	108	5	4,4%	101	0,94
36	Finland	109	107	2	1,8%	97	0,91
37	Romania	105	100	5	4,8%	93	0,93
38	Hungary	89	83	6	6,7%	79	0,95
39	Portugal	86	86	0	0,0%	76	0,88
40	Gibraltar	83	50	33	39,8%	74	1,48
41	South Africa	80	71	9	11,3%	71	1,00
42	Saudi Arabia	76	74	2	2,6%	68	0,92
43	New Zealand	74	66	8	10,8%	66	1,00
44	Turkey	71	70	1	1,4%	63	0,90
45	Japan	63	63	0	0,0%	56	0,89
46	Egypt	63	62	1	1,6%	56	0,90
47	Philippines	60	59	1	1,7%	53	0,90
48	Isle of Man	59	45	14	23,7%	52	1,16
49	Greece	56	56	0	0,0%	50	0,89
50	Curaçao	53	21	32	60,4%	47	2,24
51	Lebanon	52	52	0	0,0%	46	0,88
52	Thailand	51	50	1	2,0%	45	0,90
53	Guernsey	50	35	15	30,0%	44	1,26
54	British Virgin Islands	45	25	20	44,4%	40	1,60
55	Belize	43	27	16	37,2%	38	1,41
56	Jordan	38	36	2	5,3%	34	0,94
57	Georgia	36	35	1	2,8%	32	0,91
58	Malaysia	35	32	3	8,6%	31	0,97
59	Mexico	34	33	1	2,9%	30	0,91
60	Panama	33	26	7	21,2%	29	1,12
61	Croatia	32	32	0	0,0%	28	0,88
62	Mauritius	32	24	8	25,0%	28	1,17
63	Seychelles	32	14	18	56,3%	28	2,00
64	Saint Vincent and the Grenadines	26	13	13	50,0%	23	1,77
65	Brazil	23	22	1	4,3%	20	0,91
66	Iceland	23	19	4	17,4%	20	1,05
67	Indonesia	23	23	0	0,0%	20	0,87
68	Jersey	23	22	1	4,3%	20	0,91

#	Country	Total Number of Addresses	Confirmed Clean Addresses	Confirmed Virtual Addresses	Percent	Number of Merchants	Addresses per Merchant
69	Costa Rica	21	20	1	4,8%	18	0,90
70	Republic of Korea	20	20	0	0,0%	17	0,85
71	Argentina	18	18	0	0,0%	16	0,89
72	Republic of Moldova	18	18	0	0,0%	16	0,89
73	Belarus	17	17	0	0,0%	15	0,88
74	Montenegro	15	14	1	6,7%	13	0,93
75	Serbia	15	14	1	6,7%	13	0,93
76	Kazakhstan	14	14	0	0,0%	12	0,86
77	Andorra	13	13	0	0,0%	11	0,85
78	Azerbaijan	13	13	0	0,0%	11	0,85
79	Bahamas	13	7	6	46,2%	11	1,57
80	Liechtenstein	13	9	4	30,8%	11	1,22
81	Anguilla	13	9	4	30,8%	11	1,22
82	Nigeria	12	12	0	0,0%	10	0,83
83	Qatar	12	12	0	0,0%	10	0,83
84	Taiwan, Province of China	11	11	0	0,0%	9	0,82
85	Vanuatu	11	3	8	72,7%	9	3,00
86	Colombia	10	9	1	10,0%	8	0,89
87	Ghana	10	10	0	0,0%	8	0,80
88	Viet Nam	10	9	1	10,0%	8	0,89
89	Monaco	9	9	0	0,0%	8	0,89
90	Saint Kitts and Nevis	9	5	4	44,4%	8	1,60
91	US Virgin Islands	9	9	0	0,0%	8	0,89
92	Bahrain	8	4	4	50,0%	7	1,75
93	Bermuda	8	4	4	50,0%	7	1,75
94	Cayman Islands	8	2	6	75,0%	7	3,50
95	Chile	8	8	0	0,0%	7	0,88
96	Armenia	7	7	0	0,0%	6	0,86
97	Kenya	7	5	0	28,6%	6	1,20
98	Kuwait	7	6	1	14,3%	6	1,00
99	Pakistan	7	7	0	0,0%	6	0,86
100	Peru	7	6	1	14,3%	6	1,00
101	Uzbekistan	7	7	0	0,0%	6	0,86
102	Dominica	6	3	3	50,0%	5	1,67
103	Dominican Republic	6	6	0	0,0%	5	0,83

#	Country	Total Number of Addresses	Confirmed Clean Addresses	Confirmed Virtual Addresses	Percent	Number of Merchants	Addresses per Merchant
104	Puerto Rico	6	6	0	0,0%	5	0,83
105	Barbados	5	4	1	20,0%	4	1,00
106	Sri Lanka	5	5	0	0,0%	4	0,80
107	Iran	5	5	0	0,0%	4	0,80
108	Marshall Islands	5	4	1	20,0%	4	1,00
109	Tunisia	5	5	0	0,0%	4	0,80
110	Bangladesh	4	4	0	0,0%	3	0,75
111	Cuba	4	4	0	0,0%	3	0,75
112	Faeroe Islands	4	4	0	0,0%	3	0,75
113	Martinique	4	4	0	0,0%	3	0,75
114	Nicaragua	4	4	0	0,0%	3	0,75
115	San Marino	4	4	0	0,0%	3	0,75
116	Samoa	4	2	2	50,0%	3	1,50
117	Antigua and Barbuda	3	2	1	33,3%	2	1,00
118	Brunei Darussalam	3	3	0	0,0%	2	0,67
119	Jamaica	3	2	1	33,3%	2	1,00
120	Kyrgyzstan	3	3	0	0,0%	2	0,67
121	Morocco	3	3	0	0,0%	2	0,67
122	Oman	3	3	0	0,0%	2	0,67
123	Namibia	3	2	1	33,3%	2	1,00
124	Afghanistan	2	1	1	50,0%	1	1,00
125	Algeria	2	2	0	0,0%	1	0,50
126	Bolivia	2	2	0	0,0%	1	0,50
127	Bosnia Herzegovina	2	2	0	0,0%	1	0,50
128	Myanmar	2	2	0	0,0%	1	0,50
129	Cambodia	2	2	0	0,0%	1	0,50
130	Ecuador	2	2	0	0,0%	1	0,50
131	El Salvador	2	2	0	0,0%	1	0,50
132	French Guiana	2	2	0	0,0%	1	0,50
133	Greenland	2	2	0	0,0%	1	0,50
134	Guadeloupe	2	2	0	0,0%	1	0,50
135	Guinea	2	2	2	100,0%	1	0,50
136	Iraq	2	2	0	0,0%	1	0,50
137	Cote d'Ivoire	2	2	0	0,0%	1	0,50

#	Country	Total Number of Addresses	Confirmed Clean Addresses	Confirmed Virtual Addresses	Percent	Number of Merchants	Addresses per Merchant
138	Democratic Peoples Republic of Korea	2	2	0	0,0%	1	0,50
139	Libya	2	2	0	0,0%	1	0,50
140	Macao	2	2	0	0,0%	1	0,50
141	Madagascar	2	2	0	0,0%	1	0,50
142	Rwanda	2	1	1	50,0%	1	1,00
143	Saint Lucia	2	1	1	50,0%	1	1,00
144	Sierra Leone	2	2	0	0,0%	1	0,50
145	Trinidad and Tobago	2	2	0	0,0%	1	0,50
146	United Republic of Tanzania	2	2	0	0,0%	1	0,50
147	Uruguay	2	2	0	0,0%	1	0,50
148	Venezuela	2	2	0	0,0%	1	0,50
149	Albania	1	1	0	0,0%	1	1,00
150	Bhutan	1	1	0	0,0%	1	1,00
151	Cameroon	1	1	0	0,0%	1	1,00
152	Benin	1	1	0	0,0%	1	1,00
153	South Georgia and the South Sandwich Islands	1	1	0	0,0%	1	1,00
154	French Polynesia	1	1	0	0,0%	1	1,00
155	Palestine	1	1	0	0,0%	1	1,00
156	Guatemala	1	1	0	0,0%	1	1,00
157	Mongolia	1	1	0	0,0%	1	1,00
158	Nepal	1	1	0	0,0%	1	1,00
159	New Caledonia	1	1	0	0,0%	1	1,00
160	Niger	1	1	1	100,0%	1	1,00
161	Paraguay	1	1	0	0,0%	1	1,00
162	Sao Tome and Principe	1	1	0	0,0%	1	1,00
163	Senegal	1	1	0	0,0%	1	1,00
164	Somalia	1	1	0	0,0%	1	1,00
165	Swaziland	1	1	0	0,0%	1	1,00
166	Togo	1	1	0	0,0%	1	1,00
167	Turkmenistan	1	1	0	0,0%	1	1,00
168	Uganda	1	1	0	0,0%	1	1,00
169	The Former Yugoslav Republic of Macedonia	1	1	0	0,0%	1	1,00
170	Burkina Faso	1	1	0	0,0%	1	1,00
171	Zambia	1	1	0	0,0%	1	1,00
	Total	53.461	50.075	3.389	6,34%		

confirmed clean addresses (n = 348). However, Austria had only three (0.9%) confirmed virtual addresses included in this survey. Austria had a total of 413 merchants included in this survey and, much like the aforementioned countries, had 0.91 addresses for each merchant. Next, Malta had a reported total of 435 confirmed clean addresses, yet had an astonishingly high number of confirmed virtual addresses (n = 107). Out of 542 merchant addresses, 19.7% of them were virtual. Interestingly, Malta had 1.11 addresses for each merchant and had 484 total merchants included in this survey.

Next, China had a reported total of 275 confirmed clean addresses. Yet, China had only nine (3.2%) confirmed virtual addresses. China had 254 merchants included in this survey and had 0.92 addresses for each merchant. Closer to the EU, the Czech Republic had a reported total of 269 confirmed clean addresses yet had 52 (16.2%) confirmed virtual addresses. The Czech Republic had 287 merchants included this survey and had 1.07 addresses for each merchant. Next, Lithuania had 235 had a reported total of 235 confirmed clean addresses and had only 11 (4.5%) confirmed virtual addresses. Lithuania had 220 merchants included in this survey and had 0.94 addresses for each merchant.

Interestingly, just south of China, the Republic of Hong Kong had a reported total of 203 confirmed clean addresses and 40 (16.5%) confirmed virtual addresses. The Republic of Hong Kong had 217 merchants included in this survey and, like the Czech Republic, had 1.07 addresses for each merchant. Next, and closer to the EU, Poland had 199 confirmed clean addresses included in this survey and had 19 (8.7%) confirmed virtual addresses. Poland also had 217 merchants included in this survey and had 1.07 addresses for each merchant. However, Ukraine had 183 confirmed clean addresses included in this survey. More surprising is how Ukraine had zero confirmed virtual addresses. For each of the 163 merchants based in Ukraine, the country had 0.89 addresses for each merchant. Closer to the Czech Republic, Slovakia had 131 confirmed clean addresses included in this survey. Slovakia also had 16 (10.9%) confirmed virtual addresses. Out of 131 total Slovakian merchants included in this survey, there was one address for each merchant.

In the EU, Luxembourg had a total of 121 confirmed clean addresses included in this survey yet had 13 (9.7%) confirmed virtual addresses. Out of 119 total Luxembourgish merchants included in this survey, there were 0.98 addresses for each merchant. Next, Slovenia had a total of 114 confirmed clean addresses included in this survey. Slovenia had only seven (5.8%) confirmed virtual addresses. However, Slovenia had 108 merchants included in this survey and had 0.95 addresses for each merchant. Israel had relatively similar figures to the extent that this country had a total of 108 confirmed clean addresses included in this survey and had only 5 (4.4%) confirmed virtual addresses. Israel also had a total of 101 merchants included in this survey and had 0.94 addresses for each merchant. Similar in ranking to Israel, the Scandinavian country of Finland had 107 confirmed clean addresses included this survey. However, Finland had only two (1.8%) confirmed virtual addresses. Out of 97 total merchants included survey, each had an average of 0.91 addresses.

Romania, as well, had a similar ranking in having 100 confirmed clean addresses and only five (4.8%) confirmed virtual addresses. Out of 93 Romanian merchants included in this survey, the Eastern European country had 0.93 addresses for each merchant. Also in Eastern Europe, Hungary had a total of 83 confirmed clean addresses and six (6.7%) confirmed virtual addresses included in this survey. Out of 79 total Hungarian merchants included in this survey, the Eastern European country had 0.95 merchants for each address. Portugal had a ranking similar to that of Hungary insofar as this Western European country had 86 confirmed clean addresses included in this survey. Like Ukraine, however, Portugal had zero confirmed virtual addresses. Portugal had 76 total merchants included in this survey and had 0.88 addresses for each merchant.

In the Middle East, Saudi Arabia had 74 confirmed clean addresses and only two (2.6%) confirmed virtual addresses. The 68 Saudi Arabian merchants included in this study had 0.92 addresses for each merchant. South Africa was next in having 71 confirmed clean addresses. However, South Africa had nine (11.3%) confirmed virtual addresses. South Africa had 71 total merchants included in this study and had one address for each merchant. Next, Turkey had 70 confirmed clean addresses yet had only one (1.4%) confirmed the virtual address. Turkey had 63 total merchants included in this study and had 0.90 addresses for each merchant.

Moving eastward, New Zealand had 66 confirmed clean addresses. However, New Zealand had eight (10.8%) confirmed virtual addresses. This country had 66 total merchants included in this study and had one address for each merchant. Next, Japan had 63 confirmed clean addresses and had no confirmed virtual addresses. Out of 56 total Japanese merchants included in this study, there were 0.89 addresses for each merchant. Moving westward, Egypt had 62 confirmed clean addresses and only one (1.6%) confirmed virtual address included in this study. Out of the 56 total Egyptian merchants included in this study, each had an average of 0.90 addresses. Similarly, the Philippines had 59 confirmed clean addresses and only one (1.7%) confirmed the virtual address. The Philippines had 53 total merchants included in this study and had 0.90 addresses per merchant. Returning to Eastern European and the Mediterranean region, Greece had 56 confirmed clean addresses and had no confirmed virtual addresses included in this study. Out of the 50 Greek merchants included in this study, each has 0.89 addresses. Near Greece, Lebanon had 52 confirmed clean addresses and had no confirmed virtual addresses included in this study. For each of the 46 Lebanese merchants included in this study, there were 0.88 addresses. Moving to the Far East, Thailand had 50 confirmed clean addresses and had only one (2.0%) confirmed the virtual address. Out of the 45 Thailand-based merchants included in this study, each had an average of 0.90 addresses.

By stark contrast to Thailand, the island nation of Gibraltar had 50 confirmed clean addresses. Yet, Gibraltar had an astonishing 33 (39.8%) confirmed virtual addresses included in this study. For all 74 merchants in Gibraltar that were included in this study, there was an average of 1.48 addresses for each merchant. In the Middle East, Jordan had 36 confirmed clean addresses and had only two (5.3%) confirmed virtual addresses included in this study. Out of the 34 Jordanian merchants included in this study, each had an average of 0.94 addresses. Both the British island of Guernsey and the former Soviet republic of Georgia each had 35 confirmed clean addresses included in this study. However, Guernsey had 15 (30.0%) confirmed virtual addresses while Georgia had only one (2.8%) confirmed virtual address included in this study. Out of the 44 merchants in Guernsey that were included in this study, each had an average of 1.26 addresses. Out of the 32 total merchants based in Georgia that were included in this study, each had an average of 0.91 addresses.

Subsequently, Mexico had 33 confirmed clean addresses and had only one virtual address included in this study. Out of the 30 Mexico-based merchants included in this study, each had an average of 0.91 addresses. Malaysia and Croatia each had 32 confirmed clean addresses included in this study. However, Malaysia had three (8.6%) confirmed virtual addresses while Croatia had no confirmed virtual addresses. Out of the 31 Malaysian merchants included in this study, each had an average of 0.97 addresses. Out of the 28 total Croatian merchants included in this study, each had an average of 0.88 addresses. Moving to Central America, the countries of Belize and Panama respectively had 27 and 26 confirmed clean addresses. However, Panama had seven (21.2%) confirmed virtual addresses identified in this study. Out of the 29 Panamanian merchants included in this study, each had an average of 1.12 addresses. More astonishingly, Belize had 16 (37.2%) confirmed virtual addresses identified for this study. Out of the 38 Belizean merchants included in this study, each had an average of 1.41 addresses.

In the Caribbean, the British Virgin Islands had 25 confirmed clean addresses. However, this island nation had 20 (44.4%) confirmed virtual addresses. Out of the 40 merchants based in the British Virgin Islands that were included in this study, each had an average of 1.60 addresses. Next, the island nation of Mauritius had 24 confirmed clean addresses yet had eight (25.0%) confirmed virtual addresses included in this survey. Out of the 28 merchants based in Mauritius that were included in this study, each had an average of 1.17 addresses.

Indonesia had 23 confirmed clean addresses and zero confirmed virtual addresses included in this survey. For each of the 20 Indonesian merchants included in this study, each had an average of 0.87 addresses. Next, Brazil had 22 confirmed clean addresses and only one (4.3%) confirmed virtual address included in this study. Out of the 20 Brazilian merchants included in this study, each had an average of 0.91 addresses. Similarly, the island of Jersey had precisely the same number of confirmed clean and virtual addresses included in this study. Both Jersey and Brazil each had 20 merchants included in this study, and each merchant had an average of 0.91 addresses. The island of Curacao had 21 confirmed clean addresses included in this survey. However, this island country had an astonishing 32 (60.4%) confirmed virtual addresses. Out of the 47 merchants based in Curacao that were included in this study, each had an average of 2.24 addresses. Moving down the country-by-country ranking Costa Rica and South Korea each had 20 confirmed clean addresses. However, Costa Rica had one (4.8%) confirmed virtual address while South Korea had zero confirmed virtual addresses. For each of the 18 Costa Rican merchants included in this survey, each had an average of 0.90 addresses. For each of the South 18 South Korean merchants included in this survey, each had an average of 0.85 addresses.

Interestingly enough, Iceland had a total of 19 confirmed clean addresses included in this study. Iceland, however, had four (17.4%) confirmed virtual addresses. Out of the 20 Icelandic merchants included in this survey, each had an average of 1.05 addresses. Both Argentina and the Republic of Moldova each had 18 confirmed clean addresses and zero confirmed virtual addresses included in this survey. Argentina and Moldova also had 16 merchants included in this survey. Both countries had an average of 0.89 addresses for each merchant. The former Soviet republic of Belarus had 17 confirmed clean addresses and zero confirmed virtual addresses included in this study. Out of the 15 Belarusian merchants included in this study, each had an average of 0.88 addresses.

Four countries included in this survey – Seychelles, Montenegro, Serbia, and Kazakhstan – each had 14 confirmed clean addresses. However, Seychelles had 18 (56.3%) confirmed virtual addresses while the Eastern European countries of Montenegro and Serbia had only one (6.7%) confirmed virtual address. Kazakhstan had zero confirmed virtual addresses included in this study. Out of the 28 merchants based in Seychelles, each had an average of two addresses. Both Montenegro and Serbia each had 18 merchants included in this survey. Both countries had an average of 0.93 addresses. Out of the 12 merchants Kazakh merchants included in this survey, each had an average of 0.86 addresses.

Moving down the country-by-country list, Andorra and Azerbaijan each had 13 confirmed clean addresses and zero confirmed virtual addresses included in this survey. Both Andorra and Azerbaijan had 11 merchants included in this survey. Each merchant in either country had an average of 0.85 addresses. However, Saint Vincent and the Grenadines had 13 confirmed clean addresses and 13 (50.0%) confirmed virtual addresses included in this survey. Out of the 23 merchants based in Saint Vincent and the Grenadines included in this survey, each had an average of 1.77 addresses. Much less dramatically, Nigeria and Qatar each had 12 confirmed clean addresses and zero confirmed virtual addresses included in this survey. Both Nigeria and Qatar had 10 merchants. Each merchant in either country had an average of 0.89 addresses. Next, Taiwan had 11 confirmed clean addresses and zero confirmed virtual addresses included in this survey. Out of the nine Taiwanese merchants included in this survey, each had an average of 0.82 addresses.

Ghana had ten confirmed clean addresses included in this survey. However, Ghana had no confirmed virtual addresses. Out of the eight merchants included in this survey, each had an average of 0.80 addresses. Next, six countries included in the survey – Liechtenstein, Anguilla, Colombia, Vietnam, Monaco, and the US Virgin Islands – each had nine confirmed clean addresses. However, Liechtenstein and Anguilla each had four (30.8%) confirmed virtual addresses included in this study. For each of the 11 merchants from Liechtenstein and Anguilla included in this survey, each had an average of 1.22 addresses. Colombia and Vietnam each had one (10.0%) confirmed virtual address included in this survey. Out of the eight merchants based in Colombia and Vietnam that were included in this survey, each had an average of 0.80 addresses. Lastly, Monaco and the US Virgin Islands had zero confirmed virtual addresses included in this survey. Out of eight merchants based in Monaco and the US Virgin Islands that were included in this survey, each had an average of 0.89 addresses.

Chile had eight confirmed clean addresses and zero confirmed virtual addresses included in this survey. Of the seven Chilean merchants included in this survey, each had an average of 0.88 addresses. Four countries included in this survey – Bahamas, Armenia, Pakistan, and Uzbekistan – each had seven confirmed clean addresses.

However, Bahamas had six (46.2%) confirmed clean addresses while Armenia, Pakistan, and Uzbekistan had no virtual addresses. For each of the 11 merchants based in the Bahamas, each had an average of 1.57 addresses. For the six merchants based in Armenia, Pakistan, and Uzbekistan that were included in this survey, each had an average of 0.86 addresses.

Three countries included in this survey – Kuwait, Peru, Dominican Republic – and one US territory (Puerto Rico) each had six confirmed clean addresses. Puerto Rico had zero confirmed virtual addresses and had an average of 0.83 addresses for each Puerto Rican merchant included in this survey. The Dominican Republic also had zero confirmed virtual addresses included in this survey and also had an average of 0.83 addresses for each of the five merchants identified. Kuwait and Peru each had one (14.3%) confirmed virtual address. Both countries each had six merchants that had an average of one address.

Ten countries included in this survey – Bahrain, Bermuda, Barbados, Marshall Islands, Bangladesh, Cuba, Faeroe Islands, Martinique, Nicaragua, and San Marino – each had four confirmed clean addresses. However, Bahrain and Bermuda each had four (50.0%) confirmed virtual addresses included in this survey. For each of the seven merchants based in Bahrain and Bermuda that were included in this survey, each had an average of 1.75 addresses. Barbados and Marshall Islands each had one (25.0%) confirmed virtual addresses. Both countries had four merchants included in this survey, and each merchant had an average of one address. The remaining six countries that had four confirmed clean addresses – Bangladesh, Cuba, Faeroe Islands, Martinique, Nicaragua, and San Marino – had zero confirmed virtual addresses included in this survey. All six of these countries had three merchants included in this study. Each merchant based in these six countries had an average of 0.75 addresses.

Six countries included in this survey – Vanuatu, Dominica, Brunei Darussalam, Kyrgyzstan, Morocco, and Oman – each had three confirmed clean addresses. However, Vanuatu had an alarming eight (72.7%) confirmed virtual addresses included in this survey. Of the nine merchants based in Vanuatu that were included in this survey, each had an average of three addresses. Dominica had three (50.0%) confirmed virtual addresses included in this study. Of the five merchants based in Dominica that were included in this study, each had an average of 1.67 addresses. The remaining four countries of Brunei Darussalam, Kyrgyzstan, Morocco, and Oman each had zero confirmed virtual addresses included in this study. Each of these four countries had two merchants. Each merchant based in any of these four countries had an average of 0.67 addresses.

Twenty (n=20) countries had two confirmed clean addresses included in this study. Out of these 20 countries, 16 had zero confirmed virtual addresses. These 16 countries included Algeria, Bolivia, Bosnia Herzegovina, Myanmar, Cambodia, Ecuador, El Salvador, French Guiana, Greenland, Guadeloupe, Iraq, Cote d'Ivoire, the Democratic Peoples' Republic of Korea, Libya, Macao, and Madagascar. The Cayman Islands had two confirmed clean addresses. However, this Caribbean nation had six (75.0%) confirmed virtual addresses included in this study. Out of the seven Cayman Islands-based merchants included in this study, each had an average of 3.50 addresses. Samoa also had two confirmed clean addresses. However, this Pacific island nation had the same number (50.0%) of confirmed virtual addresses include in this study. The three Samoan merchants included in this study each had an average of 1.50 addresses. The African country of Namibia, along with the Caribbean islands of Jamaica and Antigua and Barbuda, had two confirmed clean addresses. Each of these three countries had one (33.3%) confirmed virtual address included in this study. For the two merchants based in Antigua and Barbuda that were included in this study, each had an average of one address. The same situation was the case for Jamaica and Namibia.

In this study, 26 countries had one confirmed clean address. Out of these countries, four of them – Niger, Saint Lucia, Rwanda, and Afghanistan – also had one (50.0%) confirmed virtual address. The 22 countries with one confirmed clean address and had no confirmed virtual addresses were Albania, Bhutan, Cameroon, Benin, South Georgia and the South Sandwich Islands, French Polynesia, Palestine, Guatemala, Mongolia, Nepal, New Caledonia, Paraguay, Sao Tome and Principe, Senegal, Somalia, Swaziland, Togo, Turkmenistan, Uganda, the Former Yugoslav Republic of Macedonia, Burkina Faso, and Zambia.

5. INTERPRETATION OF THE RESULTS

The country-by-country results detailed in this study illustrate that the use of virtual addresses is a global phenomenon but some jurisdictions seem to either lack the appropriate policy enforcement mechanisms designed to mitigate the risks to consumer safety incurred by money laundering practices or somehow inadvertently support or encourage the spread. Especially in context of the application for a credit card acceptance it seems that merchants rely heavily on virtual addresses to complete business transactions.

Armour et al. (2017) discussed how the risk of money laundering by clients of merchants or banking and financial institutions represents deliberate misconduct in failing to comply with legal and ethical obligations outlining the contractual nature of each business transaction. Any harm caused to customers when merchants do not disclose information contained in physical or virtual addresses is often caused by a lack of knowledge pertaining to which regulations governing business activities in the banking and financial industry have the strongest impacts on preventing members of terrorist or criminal organizations from engaging in money laundering practices. However, the opportunities to develop a holistic risk-based methodology to ameliorate the problem of money laundering entails that researchers who conduct future exploratory investigations should strive toward filling in smaller gaps concerning the role of third-party party entities. Considering the independent nature of third-party entities, their role in ensuring that merchants and customers are not prone to money laundering activities committed in part by offshore banking is significant for enacting stronger policy mechanisms governing anti-money laundering regulations at the state, national, and international levels.

Secondly, the country-by-country results detailed in this study point to how critics of corrupt governments may play a valuable role in contributing information toward preventing money laundering from having too many adverse effects on the quality of business relationships between merchants and consumers. One high-profile case in Nigeria in 1999 illustrates precisely how political campaigns to end money laundering often entail the use of innovative techniques to repatriate funds invested by consumers and held in virtual addresses. Here, Enweremadu (2013) observed how the attempt of President Olusegun Obasanjo to recover approximately US$2 billion in assets indicated that the extent of money laundering practices that result from offshore banking erect several obstacles to instituting effective policy mechanisms at the local, state, and national levels. Notwithstanding the lack of transparency in existing regulations governing business activities in the banking and financial industry, the tendency for merchants and customers alleged to have participated in money laundering activities to adopt an uncooperative attitude indicates how more researchers should define which strategies foster more cooperative attitudes as enforced by regulators, lawmakers, policy experts, and third-party entities.

Thirdly, the country-by-country results indicate that some industries are not supportive of regulations enacted to deter merchants and customers from engaging in money laundering practices. While a substantial number of researchers have recommended that merchants strengthen business relationships with customers through the enforcement of “know your customer” policy requirements, businesses in the telecommunication industry may not necessarily support recommendations for restricting the use of innovative technologies by individuals who have alleged links to terrorist organizations (Suárez, 2016, p. 950). Accordingly, the requirements that companies in the telecommunications industry restrict access to innovative technologies do not enhance consumer safety protections codified into some legal frameworks. While more merchants and customers have access to and can make use of virtual addresses, that provides alternative methods for recording business transactions, the methodologies used to ameliorate the problem of money laundering should provide researchers with sufficient reasons to define concepts and variables more precisely in future investigations.

The evolution of online business such as the exchange of virtual currencies like Bitcoin has further implication for improving the accuracy of results included in future studies. Light (2019) described how the popularity of virtual currencies that increased by 40 times (!) within the past two years should present merchants, customers, regulators, lawmakers, and policy experts with legitimate causes for alarm if innovative technologies must remain the primary tools that permit completion of most business transactions. The previous work of Mullan (2014) initially reinforced that regulating agencies like FATF and FinCEN enforce that financial service providers must comply with existing policy frameworks governing the nature of each business transaction. To the extent that FATF and FinCEN aim to prevent money laundering through the strategic collection of physical and virtual information from merchants, the establishment of anti-money laundering programs should inform the scope of future research investigations that aim to produce results with higher levels of empirical reliability and validity (Mei et al., 2014; Mei & Zhou, 2015). Consequently, researchers who conduct future studies may produce more valid empirical results by designing a risk-based holistic methodology capable of tracing the origins of funds involved in suspicious transactions identified by third-party entities or evaluating the reason why specific jurisdictions encourage the genesis and spread of virtual addresses.

Seabrooke and Wigan (2017) discussed how the published work on anti-money laundering policies recommends the development of novel or experimental methodologies that allow regulators in the banking and financial industry to identify which countries are the most cooperative. Insomuch as money laundering practices involve the deliberate attempt to conceal income sources, offshore banking practices must, therefore, receive more attention in future research studies. In this context, the process of designing and employing a risk-based holistic methodology should provide solutions that supplement what researchers have recommended in previous studies. Especially considering how some money laundering activities may indicate connections to consumers affiliated with terrorist organizations, the development of strong policy mechanisms entails that regulators in the banking and financial industry are responsible for improving consumer safety by monitoring the types of data that enter into the physical layers of technological infrastructures. Since terrorist organizations have access to innovative technologies, the tendency to use a virtual address to hide the real ultimate beneficiary of a suspicious transactions should provide researchers who conduct future studies with a sufficient reason for refining the scope of recommendations for improving business relationships between financial institutions and consumers.

More interestingly, the phenomenological paradigm proposed by Vervaele (2013) may inform how researchers conduct future investigations into the impact of virtual addresses on anti-money laundering regulations enacted at the state, national, and international levels. This particular paradigm allows researchers to evaluate the lived experiences of individuals who knowingly engage in money laundering practices and fully understand their criminological repercussions. Especially after the 2008-2009 global financial crisis led to proposals for regulating the business activities of major banking and financial institutions supported by Wall Street investors, the phenomenological paradigm lends illustrates how financial institutions involved in money laundering have the option of cooperating with proposed regulations but choose to evade the auspices of governing authorities responsible for enforcing criminal sanctions. Insomuch as FATF and FinCEN perform regularly scheduled evaluations of merchants that allegedly participate in money laundering activities, the phenomenological paradigm entails that any links to terrorist activities should also involve researchers accounting for all possible human rights implications of using virtual addresses to complete business transactions.

However, the results evidently reinforced the inconsistencies embedded in regulations governing the business activities of financial institutions. Considering the number and percentage of virtual addresses that most countries included in this survey had, the regulatory inconsistencies indicates how some lawmakers and policy experts have yet to develop an effective taxonomy concerning which rules govern physical and virtual presences and how that should impact the overall money laundering risk for financial institutions.

6. CONCLUSION

To conclude, the results appear to raise questions of accountability concerning whether regulators in the banking and financial industry should introduce legislative or policy mechanisms that reduce administrative burdens. Jakobi (2015) explained how accounting for regulatory inconsistencies should reflect the interplay between stakeholders in the public and private sectors who insist that governments should adopt various levels of policymaking strategies to ameliorate the problem of money laundering. By implication, researchers interested in designing and employing a holistic risk-based methodology should include measures accounting for legal discrepancies present at the state, national, and international levels. Furthermore, the results of this study indicated that regulators in the banking and financial industry who proposed anti-money laundering regulations should focus their attention on the relationship between virtual addresses and attempts to substitute private or public sector debt, as the use of a virtual address can be a first red flag for shell company or nominee structures and seems to be complimentary to any applied sanction list screenings. Although, as Palan and Nesvetailova (2013) noted, policy frameworks regulating the banking and financial industry that govern offshore or shadow banking present hurdles in accounting for improving consumer safety, proposals for enacting anti-money laundering regulations should accurately reflect the political and economic environments that present an appropriate contextual backdrop. Especially since the 2008-2009 global financial crisis left multiple aftershocks, small and large, the opportunities to design a holistic risk-based methodology and apply it toward implementing effective policy mechanisms should draw from the need to prevent money laundering practices as originating in the public and private sectors. However, the recommendations for conducting future research should compel lawmakers and policymakers to expand their methodological scope to institute broader yet more effective anti-money laundering regulations that also mitigate terrorist activities.

REFERENCES

Abboushi, S. (2017). Global virtual currency – Brief overview. Journal of Applied Business & Economics, 19(6), 10-18. Retrieved from http://www.m.www.na-businesspress.com/JABE/AbboushiS_19_6_.pdf

Armour, J., Mayer, C., & Polo, A. (2017). Regulatory sanctions and reputational damage in financial markets. *Journal of Financial and Quantitative Analysis, 52*(4), 1429-1448. doi: 10.1017/S0022109017000461

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. *Journal of Economic Perspectives, 29*(2), 213-238. doi: 10.1257/jep.29.2.213

Bridy, A. (2016). Internet payment blockades. *Florida Law Review, 67*(5), 1523-1568. Retrieved from https://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=1285&context=flr

Budik, J., & Schlossberger, O. (2015). Processes and technologies for identifying illegal financial operations. *International Journal in Economics and Business Administration, 3*(2), 22-31. Retrieved from https://www.ersj.eu/repec/ers/pijeba/15_2_p2.pdf

Chmiel, C. (2010). Investigative Risk Analysis. *Online-Investigation im Due Diligence-Prozess von Acquirer-Banken* (pp. 52-97). Norderstedt, Germany: BOD. doi: 9-783839-189030

Castri, S. (2013, February). *Mobile money: Enabling regulatory solutions.* London, UK: GSM Association. Retrieved from http://presite.gsma.com/mobilefordevelopment/wp-content/uploads/2013/02/MMU-Enabling-Regulatory-Solutions-di-Castri-2013.pdf

Donahue, J., Paturi, A., & Mukkamala, S. (2017). *Visualization techniques for efficient malware detection* (White Paper). Albuquerque, NM: RiskSense. Retrieved from https://risksense.com/wp-content/uploads/2018/05/Visualization-Techniques-for-Efficient-Malware-Detection.pdf

Enweremadu, D. U. (2013). Nigeria's quest to recover looted assets The Abacha affair. *Africa Spectrum, 48*(2), 51-70. Retrieved from https://journals.sub.uni-hamburg.de-/giga/afsp/article/download/648/646

Filippi, P. (2014). Bitcoin: A regulatory nightmare to a libertarian dream. *Internet Policy Review, 3*(2), 43-54. Retrieved from https://hal.archives-ouvertes.fr/hal-01026112/document

Flores, D. A., Angelopoulou, O., & Self, R. J. (2013). An anti-money laundering methodology: Financial regulations, information security and digital forensics working together. *Journal of Internet Services and Information Security, 3*(1/2), 101-114. Retrieved from http://isyou.info/jisis/vol3/no12/jisis-2013-vol3-no12-07.pdf

Gelb, A. (2016, February). *Balancing financial integrity with financial inclusion: The risk-based approach to "know your customer"* (CGD Policy Paper 074). Washington, DC: Center for Global Development. Retrieved from http://www.cgdev.org/sites/default/files/CGD-Policy-Paper-Gelb-KYC-Financial-Inclusion.pdf

Harasic, V. (2015). It's not just about the money: A comparative analysis of the regulatory status of Bitcoin under various domestic securities laws. *American University Business Law Review, 3*(3), 487-517. Retrieved from http://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1047&context=aublr

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. Retrieved from http://www.jatit.org/volumes-/Vol85No3/18Vol85No3.pdf

Hendrickson, J. R., Hogan, T. L., & Luther, W. J. (2016). The political economy of Bitcoin. *Economic Inquiry, 54*(2), 925-939. doi: 10.1111/ecin.12291

Henriques, I., & Sadorsky, P. (2018). Can Bitcoin replace gold in an investment portfolio? *Journal of Risk and Financial Management, 11*, 48-66. doi: 10.3390/jrfm11030048

Herlin-Karnell, E., & Ryder, N. (2017). The robustness of EU financial crimes legislation: A critical review of the EU and UK anti-fraud and money laundering scheme. *European Business Law Review, 27*(4), 427-446. Retrieved from http://eprints.uwe.ac.uk/28919/3/The%20Robustness%20of%20EU%20Financial%20Crimes%20Legislation-%20A%20Critical%20Review%20of%20the%20EU%20and%20UK%20Anti-Fraud%20and%20Money%20Laundering%20Scheme.pdf

Horst, C., Erdal, M. B., Carling, J., & Afeef, K. (2014). Private money, public scrutiny? Contrasting perspectives on remittances. *Global Networks, 14*(4), 514-532. doi: 10.1111/glob.12048

Irwin, A. S. M., Slay, J., & Choo, K.-K. R., & Lui, L. (2014). Money laundering and terrorism financing in virtual environments: A feasibility study. *Journal of Money Laundering Control, 17*(1), 50-75. doi: 10.1108/JMLC-06-2013-0019

Isa, Y. M., Sanusu, Z. M., Haniff, M. N., & Barnes, P. A. (2015). Money laundering risk: From the bankers' and regulators perspectives. *Procedia Economics and Finance, 28*, 7-13. doi: 10.1016/S2212-5671(15)01075-8

Jakobi, A. P. (2015). Non-state actors and global crime governance: Explaining the variance of public-private interaction. *The British Journal of Politics and International Relations, 18*(1), 72-89. doi: 10.1111/1467-856X.12064

Jayasree, V., & Balan, R. V. S. (2017). Money laundering regulatory risk evaluation using Bitmap Index-based decision tree. *Journal of the Association of Arab Universities for Basic and Applied Sciences*, 23(1), 96-102. doi: 10.1016/j.jaubas.2016.03.001

Jia, K., Zhao, X., & Zhang, L. (2013). Assessing money laundering risk of financial institutions with AHP: Supervisory perspective. *Journal of Financial Risk Management, 2*(1), 29-31. doi: 10.4236/jfrm.2013.21004

Kemal, M. U. (2014). Anti-money laundering regulations and its effectiveness. *Journal of Money Laundering Control, 17*(4), 416-427. doi: 10.1108/JMLC-06-2013-0022

Khan, N. S., Larik, A. S., Rajput, A., & Haider, S. (2013). A Bayesian approach for suspicious financial activity reporting. *International Journal of Computers and Applications, 35*(4), 181-187. doi: 10.2316/Journal.202.2013.4.202-3864

Koker, L. (2009). Identifying and managing low money laundering risk: Perspectives on FATF's risk-based guidance. *Journal of Financial Crime, 16*(4), 334-352. doi: 10.1108/13590790910993

Koker, L. (2013). The 2012 revised FATF recommendations: Assessing and mitigating mobile money integrity risks within the new standards framework. *Washington Journal of Law, Technology & Arts, 8*(3), 165-196. Retrieved from https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2639462_code1959968.pdf?abstractid=2639462&mirid=1&type=2

Lal, R., & Sachdev, I. (2015). *Mobile money services – Design and development for financial inclusion* (Working Paper 15-083). Cambridge, MA: Harvard Business School. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.697.5349&rep=rep1&type=pdf

Levi, M. (2015). Money for crime and money from crime: Financing crime and laundering crime proceeds. *European Journal on Criminal Policy and Research, 21*(2), 275-297. doi: 10.1007/s10610-015-9267-7

Light, K. (2019). Cryptocurrencies: Can they live together with national currencies and what impact do they have on national and global economies. In J. Kelso (Ed.), *Learning to live together: Promoting social harmony* (pp. 213-223). Cham, Switzerland: Springer. doi: 10.1007/978-3-319-90659-1_23

Lo, B. (2016). Fatal fragments: The effect of money transmission regulation on payments innovation. *Yale Journal of Law & Technology, 18*, 111-147. Retrieved from https://www.yjolt.org/sites/default/files/lo_18yjolt111_jz2_0.pdf

Luther, W. J. (2016). Regulating Bitcoin: On what grounds? In H. Peirce & B. Klutsey (Eds.), *Reframing financial regulation: Enhancing stability and protecting consumers* (pp. 391-415). Arlington, VA: Mercatus Center at George Mason University.

Mann, H. K., & Chhabra, G. S. (2016). Volatile memory forensics: A legal perspective. International *Journal of Computer Applications, 155*(3), 11-15. Retrieved from https://pdfs.semanticscholar.org/f140/f3bdb657f4dcfbfd4bf0183524bfa925a872.pdf

Masciandaro, D. (2005). False and reluctant friends? National money laundering regulation, international compliance and non-cooperative countries. *European Journal of Law and Economics, 20*, 17-30. doi: 10.1007/s10657-005-1012-2

Mei, D., Ye, Y., & Gao, Z. (2014). Literature review of international anti-money laundering research: A scientometrical perspective. *Open Journal of Social Sciences*, 2, 111-120. doi: 10.4236/jss.2014.212016

Mei, D., & Zhou, L. (2015). Anti-money laundering game between banking institutions and employees in the progressing CNY internationalization. *Modern Economy*, 6, 490-497. doi: 10.4236/me.2015.64048.

Mirjanich, N. (2014). Digital money: Bitcoin's financial and tax future despite regulatory uncertainty. *DePaul Law Review*, 64(1), 217-248. Retrieved from http://via.library.depaul.edu/cgi/viewcontent.cgi?article=1492&context=law-review

Morris-Cotterill, N. (2001). Money laundering. *Foreign Policy*, 124, 16-20, 22. doi: 10.2307/3183186

Mullan, P. C. (2014). *The digital currency challenge: Shaping online payment systems through US financial regulations.* New York, NY: Palgrave Macmillan.

Pagliari, S. (2012). A wall around Europe? The European regulatory response to the global financial crisis and the turn in transatlantic relations. *Journal of European Integration, 35*(4), 391-408. doi: 10.1080/07036337.2012.689830

Pal, A., & Ojha, H. (2016). How a British town became a hub for online porn and poker. *Reuters Investigates.* Retrieved from https://www.reuters.com/investigates/special-report/britain-consett-companies/

Palan, R., & Nesvetailova, A. (2013). *The governance of the black holes of the world economy: Shadow banking and offshore finance* (CITYPERC Working Paper Series No. 2013/03). London, UK: City University London. Retrieved from https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2216795_code1989161.pdf?abstractid=2216795&mirid=1&type=2

Pellegrina, L. D., & Masciandaro, D. (2009). The risk-based approach in the new European anti-money laundering legislation: A law and economics view. *Review of Law & Economics, 5*(2), 931-952. doi: 10.2202/1555-5879.1422

Pieters, G., & Vivanco, S. (2016). Financial regulations and price inconsistencies across Bitcoin markets. *Information Economics and Policy*, 39, 1-14. doi: 10.1016/j.infoecopol.2017.02.002

Rahman, A. A. (2013). The impact of reporting suspicious transactions regime on banks: Malaysian experience. *Journal of Money Laundering Control, 16*(2), 159-170. doi: 10.1108/13685201311318502

Rasul, H. (2018). Does bitcoin need regulation? An analysis of Bitcoin's decentralized nature as a security and regulatory concern for governments. *Political Analysis, 19*, 9-28. Retrieved from http://scholarship.shu.edu/cgi/viewcontent.cgi?article=1045&context=pa

Saperstein, L., Sant, G., & Ng, M. (2015). The failure of anti-money laundering regulation: Where is the cost-benefit analysis? *Notre Dame Law Review Online, 91*(1), 1-10. Retrieved from http://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=1015&context=ndlr_online

Seabrooke, L., & Wigan, D. (2017). The governance of global wealth chains. *Review of International Political Economy*, 24(1), 1-29. doi: 10.1080/09692290.2016.1268189

Suárez, S. L. (2016). Poor people's money: The politics of mobile money in Mexico and Kenya. *Telecommunications Policy, 40*(10-11), 945-955. doi: 10.1016/j.telpol.2016.03.001

Vervaele, J. (2013). Economic crimes and money laundering: A new paradigm for the criminal justice system? In B. Unger & D. van der Linde (Eds.), *Research handbook on money laundering* (pp. 379-397). Northampton, MA: Edward Elgar Publishing.

Wang, Y., & Ou, Y. (2015). Anti-money laundering regulation of China's mobile payment and settlement industry. *Open Journal of Social Sciences, 3,* 276-281. Doi: 10.4236/jss.2015.311033

Zoppei, V. (2015). Money laundering: A new perspective in assessing the effectiveness of the AML regime. *The European Review of Organized Crime, 2*(1), 130-148. Retrieved from http://www.academia.edu/download/37867251/7_Verena_Zoppei_pp130-148.pdf

COUNTRIES & NUMBER OF ADDRESSES

Country	Total Number of Addresses
United Kingdom	9.519
USA	6.841
Canada	6.225
Germany	4.183
Netherlands	3.495
Belgium	2.953
India	2.940
Denmark	2.848
Cyprus	1.319
France	987
Sweden	877
Russian Federation	728
Bulgaria	647
Estonia	628
Ireland	623
Spain	579
Switzerland	578
Malta	542
United Arab Emirates	537
Italy	507
Latvia	470
Norway	462
Austria	351
Czech Republic	321
China	284
Lithuania	246
Hongkong	243
Poland	218
Australia	195
Ukraine	183

Country	Total Number of Addresses
Slovakia	147
Luxembourg	134
Slovenia	121
Singapore	114
Israel	113
Finland	109
Romania	105
Hungary	89
Portugal	86
Gibraltar	83
South Africa	80
Saudi Arabia	76
New Zealand	74
Turkey	71
Japan	63
Egypt	63
Philippines	60
Isle of Man	59
Greece	56
Curaçao	53
Lebanon	52
Thailand	51
Guernsey	50
British Virgin Islands	45
Belize	43
Jordan	38
Georgia	36
Malaysia	35
Mexico	34
Panama	33
Croatia	32
Mauritius	32
Seychelles	32
Saint Vincent and the Grenadines	26
Brazil	23
Iceland	23

Country	Total Number of Addresses
Indonesia	23
Jersey	23
Costa Rica	21
Republic of Korea	20
Argentina	18
Republic of Moldova	18
Belarus	17
Montenegro	15
Serbia	15
Kazakhstan	14
Andorra	13
Azerbaijan	13
Bahamas	13
Liechtenstein	13
Anguilla	13
Nigeria	12
Qatar	12
Taiwan, Province of China	11
Vanuatu	11
Colombia	10
Ghana	10
Viet Nam	10
Monaco	9
Saint Kitts and Nevis	9
US Virgin Islands	9
Bahrain	8
Bermuda	8
Cayman Islands	8
Chile	8
Armenia	7
Kenya	7
Kuwait	7
Pakistan	7
Peru	7
Uzbekistan	7

Country	Total Number of Addresses
Dominica	6
Dominican Republic	6
Puerto Rico	6
Barbados	5
Sri Lanka	5
Iran	5
Marshall Islands	5
Tunisia	5
Bangladesh	4
Cuba	4
Faeroe Islands	4
Martinique	4
Nicaragua	4
San Marino	4
Samoa	4
Antigua and Barbuda	3
Brunei Darussalam	3
Jamaica	3
Kyrgyzstan	3
Morocco	3
Oman	3
Namibia	3
Afghanistan	2
Algeria	2
Bolivia	2
Bosnia Herzegovina	2
Myanmar	2
Cambodia	2
Ecuador	2
El Salvador	2
French Guiana	2
Greenland	2
Guadeloupe	2
Guinea	2
Iraq	2
Cote d'Ivoire	2
Democratic Peoples Republic of Korea	2
Libya	2
Macao	2
Madagascar	2
Rwanda	2
Saint Lucia	2
Sierra Leone	2
Trinidad and Tobago	2
United Republic of Tanzania	2
Uruguay	2
Venezuela	2
Albania	1
Bhutan	1
Cameroon	1
Benin	1
South Georgia and the South Sandwich Islands	1
French Polynesia	1
Palestine	1
Guatemala	1
Mongolia	1
Nepal	1
New Caledonia	1
Niger	1
Paraguay	1
Sao Tome and Principe	1
Senegal	1
Somalia	1
Swaziland	1
Togo	1
Turkmenistan	1
Uganda	1
The Former Yugoslav Republic of Macedonia	1
Burkina Faso	1
Zambia	1
Total	53.461

LEARN MORE ABOUT WEB SHIELD

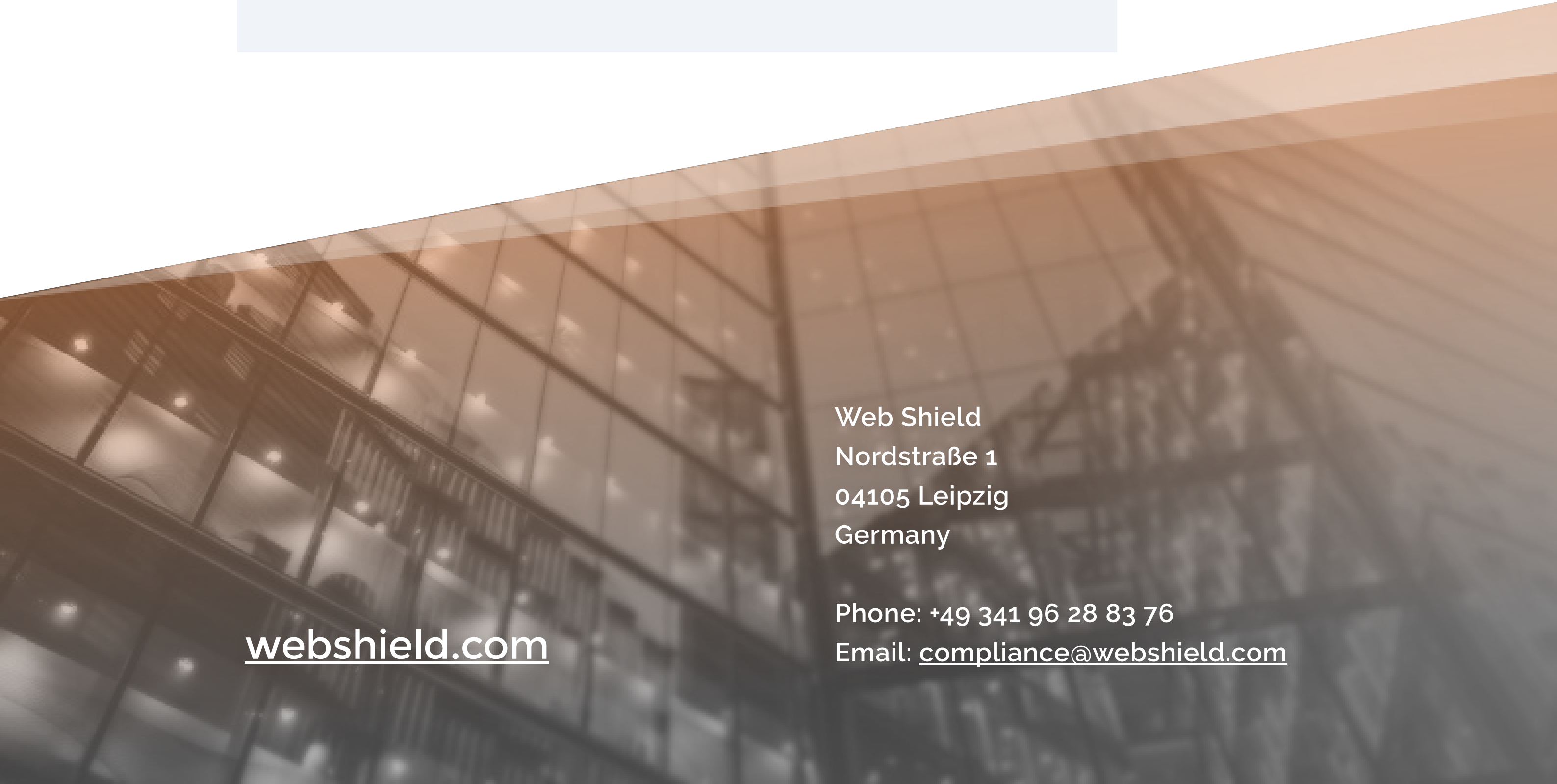
Web Shield is a RegTech company and global leader in real-time on-boarding and risk-based monitoring solutions.

As the trusted partner of international players in the field of merchant acquiring and payment processing, we assist our clients by enabling exceptionally fast on-boarding and monitoring in a dynamic regulatory landscape.

With the Web Shield Academy, we operate an educational program for underwriters that is unique in the industry and since 2017, we organise RiskConnect, the annual Networking Conference for anti-fraud, compliance and risk professionals.

EXPLORE OUR PORTFOLIO

Web Shield builds exceptional underwriting and monitoring solutions.
https://webshield.com/



webshield.com

Web Shield
Nordstraße 1
04105 Leipzig
Germany

Phone: +49 341 96 28 83 76
Email: compliance@webshield.com