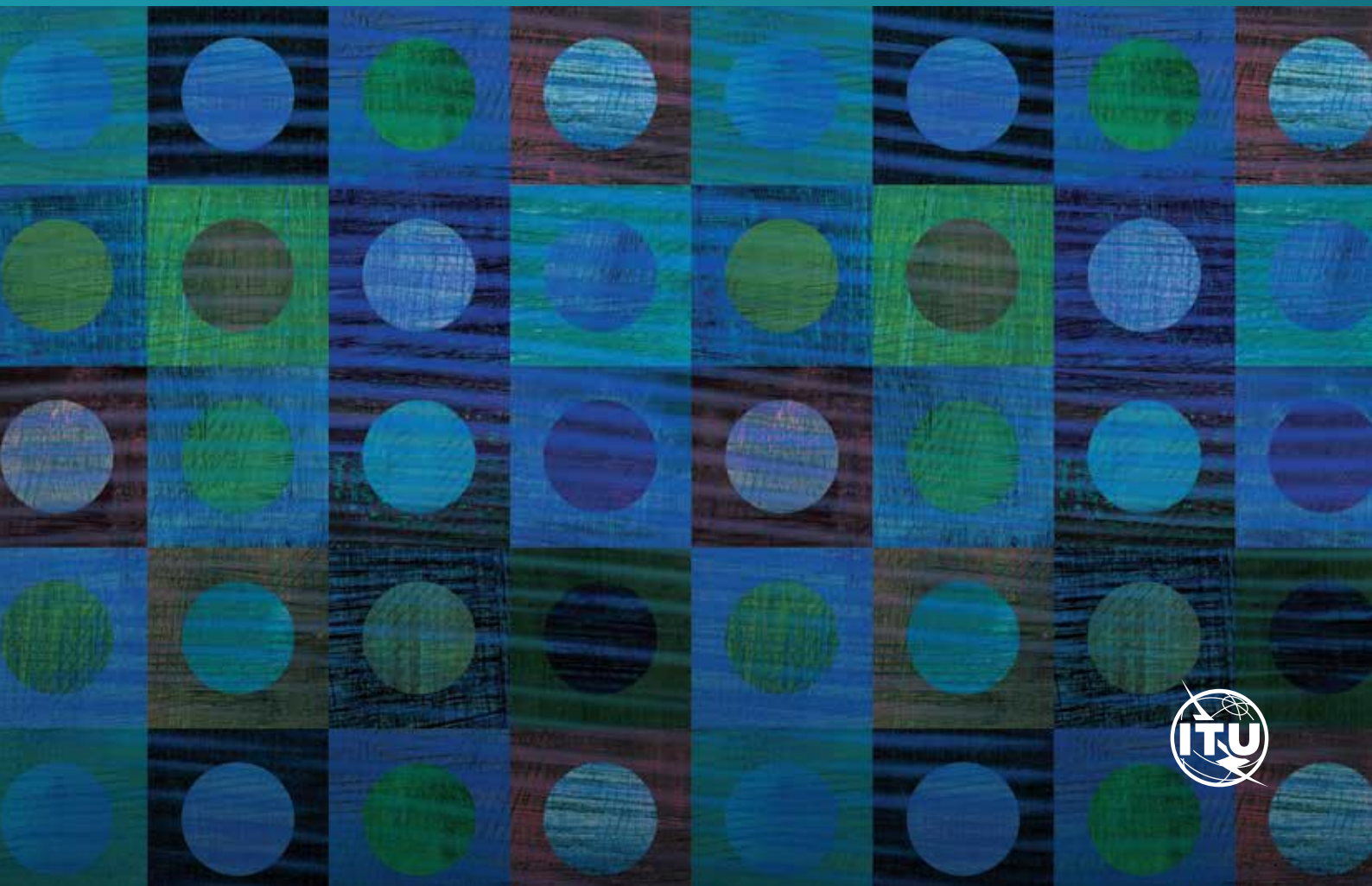
FIGI

FINANCIAL INCLUSION
GLOBAL INITIATIVE

SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP

Unlicensed Digital Investment Schemes (UDIS)

REPORT OF TRUST WORKSTREAM



SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP

Unlicensed Digital Investment Schemes

Flourishing criminal activity in the global financial ecosystem calls for collaboration amongst telecommunications, financial sector regulators and criminal investigation authorities.

DISCLAIMER

The Financial Inclusion Global Initiative (FIGI) is a three-year program implemented in partnership by the World Bank Group (WBG), the Committee on Payments and Market Infrastructures (CPMI), and the International Telecommunication Union (ITU) funded by the Bill & Melinda Gates Foundation (BMGF) to support and accelerate the implementation of country-led reform actions to meet national financial inclusion targets, and ultimately the global 'Universal Financial Access 2020' goal. FIGI funds national implementations in three countries—China, Egypt and Mexico; supports working groups to tackle three sets of outstanding challenges for reaching universal financial access: (1) the Electronic Payment Acceptance Working Group (led by the WBG), (2) The Digital ID for Financial Services Working Group (led by the WBG), and (3) The Security, Infrastructure and Trust Working Group (led by the ITU); and hosts three annual symposia to gather national authorities, the private sector, and the engaged public on relevant topics and to share emerging insights from the working groups and country programs.

This report is a product of the FIGI Security, Infrastructure and Trust Working Group, led by the International Telecommunication Union.

The findings, interpretations, and conclusions expressed in this work do not necessarily reflect the views of the Financial Inclusion Global Initiative partners including the Committee on Payments and Market Infrastructures, the Bill & Melinda Gates Foundation, the International Telecommunication Union, or the World Bank (including its Board of Executive Directors or the governments they represent). The mention of specific companies or of certain manufacturers' products does not imply that they are endorsed or recommended by ITU in preference to others of a similar nature that are not mentioned. Errors and omissions excepted, the names of proprietary products are distinguished by initial capital letters. The FIGI partners do not guarantee the accuracy of the data included in this work. The boundaries, colours, denominations, and other information shown on any map in this work do not imply any judgment on the part of the FIGI partners concerning the legal status of any country, territory, city or area or of its authorities or the endorsement or acceptance of such boundaries.

Acknowledgements

This paper was written by Jami Solli with substantial input and research from the following persons: Assaf Klinger (Vaulto), Niyi Ajao (Nigeria Interbank Settlement System), T.O. Fatukun (Central Bank of Nigeria), Md. Rashed Mohammed (Bangladesh Financial Intelligence Unit), Amol Kulkarni (CUTS International, India), Mercy Buku (CGAP), Felicia Monye (Consumer Awareness Organisation, Nigeria) and Prof Louis de Koker (La Trobe University, Australia). Substantive editorial guidance was provided by Vijay Mauree and Charlyne Restivo of the Telecommunication Standardization Bureau of the ITU.

The author would like to thank the Security, Infrastructure and Trust Working Group for its continued assistance. The opinions expressed in this report are those of the author and do not necessarily reflect the views of the International Telecommunication Union or its membership.

Contents

Executive Summary

Internet fraud in the form of unlicensed digital investment schemes (aka digital Ponzis) is at an all-time high. Yet, the impact on financial exclusion is unknown, because few regulators have been measuring the magnitude of the problem. Judging from past Ponzi statistics in the pre-digital era, however, we know that this type of financial fraud can severely harm individual consumers and their families and cause financial system risk, which may induce civil unrest.

This paper aims at providing a better understanding of the impact of this specific type of fraud on both the consumer and financial exclusion through an analysis of unlicensed digital investment schemes and the legal/regulatory frameworks in which they thrive in India, Kenya and Nigeria. It also proposes new means to address a digital mutation of a very old problem, and makes concrete recommendations regarding the use of new technologies and new partnerships, including the involvement of the telecommunications regulator to take up the unlicensed digital investment schemes challenge.

Abbreviations and acronyms

AML	Anti-Money Laundering
DFS	Digital Financial Services
GDP	Gross Domestic Product
ICO	Initial Coin Offerings
IMF	International Monetary Fund
ISP	Internet service provider
MMM	Mavrodi Mondial Money
RBI	Reserve Bank of India
SACCO	Savings and Credit Cooperatives
SEBI	Securities and Exchange Board of India
SMS	Short Messaging Service
TRAI	Telecom Regulatory Authority of India
UDIS	Unlicensed Digital Investment Schemes
URL	Uniform Resource Locator

Unlicensed Digital Investment Schemes (UDIS)

1 BACKGROUND

UDIS are fraudulent schemes which are promoted digitally via a domain name/URL, on social networks or text messaging services. These schemes promote and sell investment opportunities to consumers which are not licensed by the appropriate regulator. They pay returns to investors from the new capital that is *paid in* by new investors, rather than from a legitimate, profit-generating business or activity. These schemes usually end, or collapse when there is insufficient new capital paid in to sustain pay outs to existing investors.

The paper will not consider unlicensed investment schemes where there is no digital element to the fraud, nor where the solicitation is an attempt to elicit consumer's private financial data online (e.g. phishing) nor will it consider social engineering frauds such as solicitations for funds from fraudsters pretending to be a love interest in order to extort money from unsuspecting, and lonely consumers.

This is not to diminish the very real harm these types of scams, but the authors believe that the collective harm caused by UDIS is much greater, with the potential to adversely affect the health of the financial system.

UDIS Examples:

An example of an ongoing, international UDIS is the Mavrodi Mondial Money, or MMM schemes, which remain active on the Internet with both a Facebook presence, and some form of www.countryname-MMM.net as an URL.

MMM purports to be *a community of ordinary people helping each other.* Consumers are encouraged to send money, including via bitcoin, and are promised monetary support at some time in the future from the common fund. Thirty-percent returns are promised on the website, on Facebook pages, via Twitter and even closed MMM groups have been identified on Whatsapp. Further, MMM offers and online school to learn how to promote a MMM scheme.

Another example of an UDIS applying a new twist to promote its fraudulent investment offer is the recent scheme in the Uttar Pradesh region in Noida, India, which called for consumers to invest money in a scheme that allowed consumers to purportedly earn money by clicking 'like' on Facebook for various companies, which had supposedly paid the promoter for 'pay for click' advertising.

The Noida scheme had both a Facebook and URL presence (www.socialtrade.biz) and ultimately, it too collapsed. It was later revealed that consumers were being misled and any return on investment was offered solely because of later investments by new consumers who were similarly duped, and not paid by actual companies which had purchased marketing services from the promoter. This type of UDIS illustrates that criminals try to mask their activities as valid marketing practices or a new business/investment model (e.g. initial coin offerings which will be discussed later in the paper). And, thus the Noida scheme too would be included in the

working group's definition of an unlicensed, digital investment scheme.

2 ICTS AND UDIS

Prior to the existence of the world wide web, social networks, or digital financial services, the perpetrators of financial frauds, such as Ponzi and pyramid schemes were charismatic salesmen, exerting a lot of time and effort to defraud victims. Generally, fraudsters would also enlist an inner circle of first line investors, who simultaneously acted as a secondary sales force. Promotion of the phony investment product to one's close circle of friends, family and business associates was done the old fashioned way: in person and on the telephone.

In this manner, Bernie Madoff was able to accumulate an estimated USD 65 billion dollars in his Ponzi scheme due to his charismatic, trustworthy demeanor which allowed him to mobilize *feeder funds* from amongst global money managers to the uber wealthy, including members of European royal families.[1] Like many affinity fraudsters, Madoff also preyed within his own social circles; including within the Jewish communities in New York and Florid.

Today, with the advent of the Internet, social networks and mobile phones, running a Ponzi scheme has become much easier. Promotion of the schemes can be done from the comfort of one's home, or from anywhere using social networks and SMS to promote the scheme and mobile money to facilitate the transfer the funds in and out. Crypto currencies are also available to launder the proceeds so today's Ponzi operator can reach a much greater volume of victims with arguably much less effort, and hide the ill gotten gains easier.

The Internet and digital money also offer new technologies in which to disguise a Ponzi so that few consumers truly understand its underlying, fraudulent nature. For example, Initial Coin Offerings (ICOs) of crypto currencies have recently provided a new product offering for Ponzi perpetrators to use to defraud unwitting investors. It is difficult to analyze the underlying software code at issue in an ICO, and thus determine whether it is a valid business or a Ponzi. More often than not potential investors lack the capacity to analyze whether there is indeed a legitimate business model.

This is not to say that all ICOs are Ponzis, but merely to point out that fraudsters utilize complicated technologies to disguise the true nature of their offering. For example, the scheme devised by Charles Ponzi known as the original Ponzi master, involved the purported arbitrage of international postal reply coupons.[2] The average person was not familiar with postal reply coupons, and thus did not question the charismatic salesman's purported superior knowledge.

With digital means, a Ponzi perpetrator can promote schemes virally, setting schemes in motion simultaneously in multiple jurisdictions. If they are ever subject to regulatory intervention or investigation in one jurisdiction, the Ponzi operator can simply target other jurisdictions; they are limited only by their own linguistic abilities, or the ability to collude with likeminded criminals in the new jurisdictions. For example, the above mentioned MMM scheme was hatched in 1989 by Sergei Mavrodi and has now spread to many countries with the advent of the Internet and Facebook. The author would suggest that *bank robbers almost always get caught, but Ponzi operators rarely do.*

3 IMPACT OF UDIS

In the post Internet world, there are three main reasons why financial and telecom sector regulators, criminal investigators, consumer advocates and all financial inclusion stakeholders should take the problem of UDIS very seriously:

i. UDIS can harm the financial system

ii. The harm to consumers from UDIS may be irreparable, impacting several generations

iii. UDIS can cause financial exclusion

A significant allocation of resources may be needed to address the UDIS problem, including utilizing existing technologies to monitor the Internet and the dark web. Financial institutions can also look for suspicious transfer patterns and report as per existing anti-money laundering (AML) requirements. Financial fraud is after all a predicate offense to money laundering.

To date, judging from the many flourishing UDIS, supervision and monitoring efforts have either been inadequate or antiquated. As a result, the volume of UDIS continues to increase exponentially.

3.1 UDIS can harm the financial system

The impact of UDIS on a national economy can be devastating, causing harm which lasts for years. The history of unlicensed investment schemes, which previously operated within a single country's boundaries serves to illustrate that impact can cause systemic risk, and undermine the political stability of a country

For example, in the late 1990's, Albania was riddled with Ponzi schemes and an estimated 50% of the nation's GDP (Gross Domestic Product) was invested in fraudulent schemes. The collapse of the schemes were subsequently followed by civil unrest causing approximately 2,000 deaths and a change of regime according to the IMF[3] (International Monetary Fund). Caribbean nations, such as Jamaica and Grenada, are known to have suffered from Ponzi collapses whereby 12% and 25% of the nations' GDPs were invested, according to the IMF.[4] During the peak of the microcredit industry in East Africa (2005–2007), Ponzi schemes flourished there causing untold damage to financial inclusion according to the media.[5] For example, the COWE and Dutch International Schemes which collapsed in Uganda in 2007 causing an estimated USD 7 million in losses

to consumers (see box 1 for further details). In neighboring Kenya, more than 26,000 consumers lost money to hundreds of Ponzi schemes operating in the same period. It has been estimated that some USD 300 million USD were lost in Kenyan Ponzi schemes within this period. In India, estimates from a 2014 BBC article suggest that around USD 160 billion USD have been lost in Ponzi schemes (though, no source was provided for their data).[6]

As Ponzi schemes have migrated to the Internet, new schemes such as Ezubao in China emerged. *Ezubao* purported to be earning profits from peer to peer lending, whereas it turned out to be a Ponzi scheme, which inflicted massive damages in a relatively short period. From its inception in 2014, to its discovery in 2016 only two years later, Ezubao inflicted a USD 9 billion USD to the Chinese economy. An economy of China's size may be able to withstand a loss of 9 billion USD by consumers, but a loss of this scale in a smaller economy would very likely result in significant civil unrest.

3.2 Consumers from UDIS may be irreparable, impacting several generations

The harm from UDIS to consumers can be life threatening, impacting more than one generation in the same family. The sudden loss of large amounts of money may cause utmost emotional distress, which may even lead to suicide in the worst cases. During the years of 2008–2010 for example, coinciding with the recession triggered by the subprime crisis, suicides in North America and Europe were estimated to have caused 10,000 deaths more than in previous years.[7]

Also, it has been observed that once a fraudulent investment scheme collapses, consumers rarely get their funds back. Their recovery from such losses could take many years; if it ever happens. The authors have not found sufficient research on the long term effects of Ponzi schemes on victims. Most Ponzi schemes are linked to affinity frauds promoted by people enjoying close affinity with the victims' entire families and social networks being affected. In situation where State support is unavailable, and and extended families are unable to assist, we can only presume that recovery from losses to a Ponzi may take many years. See the COWE example below.

3.3 UDIS can cause financial exclusion

Financial exclusion can be inferred once consumers have lost money to fraudulent, unlicensed investment schemes: they no longer have these funds to invest in legitimate, profit generating activities, nor in asset building. Furthermore, these consumers may also experience distrust towards the financial sector and the regulators, which have failed to protect them. This distrust may be passed on to their children, and extended families.

In fact, researchers at Cornell University described the *trust shock* that rippled through the US economy following Bernie Madoff's fraud which lead to other investors collectively withdrawing $363 billion from investment accounts.[8] It was found that the shock waves resonated primarily through social networks.

In the age of Internet, Ponzi schemes are first and foremost easier to commit, secondly have greater impact, and thirdly resonate more profoundly through communities.

BOX 1

UGANDA: CARING FOR ORPHANS WIDOWS AND THE ELDERLY (COWE)

A study interviewed 65 victims of the *Caring for Orphans Widows and the Elderly (COWE)* Ponzi scheme which collapsed in Uganda in 2007, with an estimated USD 7 million USD in losses to consumers. It was found that the COWE fraudsters had contributed to 11 suicides. Some suicides attempts were only prevented by the victim's lack of financial resources (e.g. to purchase poison). Some died attempting to flee debt collectors. Countless other victims experienced high blood pressure and other stress-related illnesses, including depression. Divorces rates rose, other victims fled the country to war-torn Sudan and South Africa to avoid creditors, and others were incarcerated by their creditors for failure to repay funds borrowed from commercial banks, microfinance institutions and savings and credit cooperatives (SACCOs) which they used to invest in the COWE and Dutch International schemes. Families were torn apart, and many victims were also forced to pull their children out of school, due to an inability to pay school fees. 65 victims of the COWE scheme were interviewed in person in 2014 and another 150 victims of the same scheme were surveyed with the assistance of the COWE Victims Association in Kbale, Uganda. A case summary was prepared by Simmons and Simmons law firm of London.

More than 8 years after the COWE Ponzi scheme collapses, interviews with COWE victims showed that many of these victims were still battling significant growing debts. It was also found that many of the victim's friends and family members had accumulated similar debts.[1]

4 A SURVEY OF EXISTING RESEARCH/ INITIATIVES ON UNLICENSED INVESTMENT SCHEMES

To date, the global financial inclusion stakeholders have not dedicated much attention in terms of research, nor concerted action to unlicensed investment schemes let alone to UDIS. This lack of research and related failure to act is problematic given the significant negative impact of these frauds on consumers, markets and financial inclusion.

Failure to act may also be related to the perception that first, the buyer/consumer should beware of the dangers of Ponzi schemes, or *should know better* than invest in such schemes. It may also relate to regulators and policymakers feeling powerless to address the issue. The author believes that both of these sentiments are misguided. In fact, little effort has been made to find new, technology based solutions, nor to understand the behavioral motivations of consumers for finding these schemes credible or worth the risk of investing. Are consumers emotions driving the investment decision-making process or do we have low financial literacy levels to blame, or both? And if emotions are driving the process, can they be countered by similar emotional appeals to avoid making a bad investment decision? If so, how could these warnings be effectively crafted, and who should deliver the message? For example, would it be effective to use the same public figures; like actors, sports stars and religious leaders to warn consumers; as those used to pitch investments schemes? We can only speculate regarding the answers to the above, because this type of research has not been done.

Aside from the aforementioned IMF research on Ponzis (2009); the Cornell University study on the impact of Ponzis on investor trust which are specific to the Madoff scheme, and an Emory University study on characteristics of the typical Ponzi investor, there is very little existing research on the matter. There are even fewer studies on UDIS, or on effective regulatory prevention efforts.

The authors propose that much more research is needed. Firstly, research is required on the best practices in Ponzi prevention, including the use of new artificial intelligence technologies to better monitor markets to identify these schemes. Secondly, research should enquire how the use of well framed messaging from influential sources can warn consumers and impact behavioral change. There is also need for research to study the impact of UDIS on consumers and markets, in addition to the erosion of consumer trust. Lastly, we should explore what is the impact on financial exclusion in the medium and long terms on consumers and markets.

With regard to consumer capability trainings or awareness raising, there are a few examples of how the financial sector and securities regulators are trying to educate the public. However, again there has not been an evaluation as to the efficacy of these consumer messaging initiatives.[9]

Malaysia, for example had an outreach campaign to warn consumers and which informed where specifically to check the registration status of an investment; also telling consumers that the words *Sharia compliant* does not necessarily mean *licensed,* and engaging religious actors too to help inform the public.[10] This is a very good idea, because fraudsters often use religious figures and gatherings to promote and sell their phony investment schemes. The aforementioned Ugandan COWE scheme, for example hired a preacher's wife to recruit investors. She signed up the entire 700+ member congregation and after the Ponzi collapsed had to move out of the community. Indian Ponzi schemes have often used cricket stars and Bollywood actors (who were perhaps unaware of the illegitimacy of the offer) to promote investments which later turned out to be fraudulent. A Bangladeshi Ponzi called Destiny which stole an estimated USD 75 million was chaired and promoted by an ex-Army general.

Outreach and consumer education efforts must be continuous, but often warnings appear only upon the collapse of a particular ponzi, at which time, the regulator will respond by posting a warning message to consumers on its website. This is too little; and too late to be useful to the masses who have already lost money. And, even its deterrent impact on other consumers likely to invest in other similar schemes is also likely to be low, simply because they have been told that the collapsed Ponzi was a fraud, but may not be able to identify other future Ponzi schemes as such. Further, relying solely on one channel of communication where there is a diverse group of consumers with varying literacy levels and who may or may not have internet access is insufficient to protect consumers.

The Working Group did identify one effective method of educating the public of the dangers of Ponzi schemes which was a *bait site* online published by the US Federal Trade Commission. The web page offered a *too good to be true* investment offer leading consumers who took the bait to enter their credit card details on the site to invest in the scheme; at which point the webpage then flashed a warning message stating "you almost lost all of your money" and then directed the consumer to an educational page explaining the dangers of unlicensed investment schemes and how to recognize the signs of a potential financial fraud.

Another unique method of reaching consumers was reported by the Nigerian security exchange commission to the International Organization of Securities Commission that it is in the process of developing a weekly soap opera in Nigeria based on Ponzi schemes to educate the public about the dangers of Ponzi schemes.

These are all good examples, but consistency may be just as important as the content, and the efficacy of messaging should be measured as well so as to not waste funds on ineffective messaging.

5 CASE STUDIES BY COUNTRY (INDIA, KENYA & NIGERIA)

The countries selected for further study were countries where the working group has members with deep knowledge of the DFS market, who were also able to provide input on the legal and regulatory frameworks, and provide background on past and ongoing UDIS involvement in the country. The legal/regulatory reviews were also conducted by legal professionals from the country at issue.

A fourth country, Bangladesh, was also used as a point of comparison as the working group, which benefitted greatly from insights of a Financial Intelligence Unit Director at the Bank of Bangladesh who is also an AML expert.

All three countries have common law roots, but very distinct digital financial services (DFS) markets. Kenya, for example boasts approximately 82% financial inclusion thanks in a large measure to the success of Safaricom's M-Pesa.[11] Nigeria lags behind Kenya at 40% financial inclusion, respectively, but arguably Nigeria has greater geographic, and language challenges to overcome.[12]

The other shared characteristic of the focus countries is the victimization by at least one large scale, unlicensed digital investment scheme. In fact, all three countries have been victimized by *Mavrodi Mondial Moneybox* or MMM, a scheme which originated in Russia in the 1990's and which has expanded globally due to the Internet and social networks. The MMM UDIS operates via Facebook, Twitter, WhatsApp and Snapchat and has numerous functioning web sites with a multitude of domain names (several using a chatbot to interact with consumers), including those URL that contain the country names India, Kenya and Nigeria. None of the three countries studied shut down the MMM UDIS. In fact, the URL and Facebook pages affiliated with MMM remain operational in all three countries as of March 2018. *See case note 1* for more details on the MMM scheme in Nigeria.

Because market monitoring, and apparently investigation and prosecution phases are challenging, this research sought to better understand the roles of the various regulators in India, Kenya, and Nigeria and to better understand why they are failing to act, as per statutory mandates.

During the research, country contacts responded to ten questions in order to better understand the legal and regulatory frameworks related to UDIS, what should happen to prevent/deter these schemes, and what improvements can be made in the future. (The full list of questions is attached as Annex A).

Our key findings are as follows:

a) Everyone is the boss, but no one is really in charge (of UDIS).

b) There are low rates of prosecution for UDIS and rare reimbursements for the consumer when funds are lost.

CASE 1

NIGERIA: THE IMPACT OF ONE UNLICENSED INVESTMENT SCHEMES ON THE ECONOMY CAN BE SIGNIFICANT

In an attempt to better understand how fraudulent unlicensed digital investment schemes impact the Nigerian economy, the Nigeria Inter Bank Settlement System, PLC (NIBSS), the central switch for the country's financial sector undertook an analysis of interbank transactions from commercial banks.

Transactions were analyzed from June 2016 to December 13, 2016 for linkages with the Mavrodi Mundial Moneybox (MMM) Ponzi scheme in Nigeria. Because the scheme directed customers to put identifying information on the transfer order, NIBSS was able to discern that during the six month period that 28.7 billion in Nigerian Naira was transferred between banks related to the MMM fraud, or USD 77.8 million. This amount transacted in this one fraud in six months exceeded the Nigerian Ministry of Education's annual budget by 61%.

Further, the data analyzed was only from interbank transfers. Thus, intra bank transfers related to the MMM Ponzi are estimated to be at least twice the interbank transfer volume.

NIBSS conducted its analysis just following the MMM's second crash.[13] At the time, consumers who had invested funds, yet who had not received any payout lost over 11.9 billion Naira or USD 32.8 million.

At the time of drafting of its report, NIBSS also noted that it found evidence of at least 89 other ongoing unlicensed digital investment schemes in the country.

NIBSS has subsequently noted that the Central Bank Nigeria has been running awareness raising campaigns on TV to inform consumers of the dangers of these schemes, however it would seem that campaigns alone are insufficient. And, given that NIBSS own data analysis was possible because consumers used keywords on their transfer orders, it would seem that artificial intelligence could be similarly used to monitor the Internet and social media for indicators of similar fraudulent activity and to set indicators for financial institutions to flag suspicious transactions which would bely an underlying Ponzi scheme is afoot.

CASE 2

KENYA: REPORT OF THE PYRAMID SCHEME TASK FORCE

In response to public outcry during the period around Kenyan elections in 2007 which saw rising levels of frauds by unlicensed investment schemes, the Ministry of Cooperative Affairs in Kenya established a task force charged with assessing the scope of problem in the country. The task force also sought to give the crime victims a voice and to make recommendations regarding how to best respond to the problem.

In June 2009, the taskforce presented a report to the Ministry which indicated that 148,784 investors had lost over 8 billion Kenyan shillings (USD 78.8 million) in recent years.[14] The report identified some 270 fraudulent schemes, and even documented land purchases by the accused criminals with the ill-gotten gains from the fraudulent investment schemes. The report noted that the deleterious effects on victims were many, including suicides, depression, hypertension and diabetes to name only the health consequences.

The report recommended that criminal prosecutions proceed against the named perpetrators.

It is unclear whether the State ever initiated criminal prosecutions related to the enumerated scams, however, it is unlikely given that the crime victims themselves subsequently organized an advocacy organization called the National Pyramid Schemes Victims Initiative (NPSVI). The NPSVI itself filed a class action on behalf of its 40,000 members alleging negligence on the part of the Attorney General's Office and the Central Bank Kenya causing them to collectively lose 5.7 billion Kenyan shillings. NPSVI initially filed its class action on behalf of victims in early 2015 and has continually been met with delays and postponements in the case with its next court hearing scheduled for 6 November 2019.[15] It is unlikely that this legal action will provide the victims with redress any time soon.

The task force's key recommendations are that more awareness campaigns are necessary for the public; it proposes the formation of a permanent agency tasked with eradicating pyramid/Ponzi schemes.

5.1 Everyone is the boss, but no one is really in charge of UDIS.

In the three countries analyzed, we noted multiple regulators actually have the legal authority to take preventative action, including seizure of accounts if necessary. In Nigeria, for example, there are a total of *five* main government actors which perform functions that impact digital and financial services and that can therefore investigate, intervene and shut down unlicensed digital investment schemes; including the Nigerian Communications Commission (telecom regulator), National Information Technology Development Agency (regulator for information technology practices), the Central Bank, the Securities and Exchange Commission and the Economic and Financial Crimes Commission.[16]

None of the three countries, however, seems to have a lead authority or coordinating body charged with UDIS prevention/supervisory efforts amongst existing regulatory bodies and/or police. In fact, in India, where there are three regulators with the authority to prevent UDIS: the Securities and Exchange Board of India (SEBI), the Reserve Bank of India (RBI) and the Telecom Regulatory Authority of India (TRAI): the first of the two regulators, SEBI and RBI both seek to renounce legal responsibility for prevention of unlicensed investment schemes. It has been reported that SEBI has asked the Supreme Court for a declaratory judgment stating that Ponzi schemes do not fall within its jurisdiction. Similarly, RBI has made the claim that entities operating Ponzis do not fall under its mandate.[17]

If both SEBI and RBI are allowed to *opt out* of their regulatory mandates vis-a-vis UDIS, then that will leave only TRAI (and the police) left to act. Similarly, in Kenya and Nigeria the telecommunications regulator has the statutory authority to act to shut down UDIS, but appears to not be monitoring internet content for UDIS. For instance, as of the drafting of this paper, the MMM-Country Name websites are all still live.[18]

5.2 Low rates of prosecution for UDIS and rare reimbursements for the consumer

Too many responsible authorities can also cause confusion for consumers, leaving them unsure of where to report potential UDIS. Low rates of prosecution for UDIS and rare reimbursements for the consumer are already the norm.

Of the three countries compared, India appears most prolific in its prosecutions, but as with all three focus countries there is no central database (to date), nor one lead authority responsible for UDIS prevention.[19] A private consulting firm named Strategy India, does however keep a running tab on unlicensed, potentially fraudulent businesses inclusive of UDIS.[20]

The Ministry of Corporate Affairs in India investigated 185 such schemes in the past 3 years through the

Serious Fraud Investigation Office, the Reserve Bank of India was considering 486 cases of unauthorized deposit collection, and the Central Bureau of Investigation had registered 115 cases for such scams from January of 2014 to June of 2017. And, the Directorate of Enforcement had investigated 36 cases in the last three years. Also, the Securities and Exchange Board of India, which regulates collective investment schemes issued final orders against 65 entities for carrying out investment activities without a certificate of registration in the three years leading up to February of 2017.[21]

SEBI also passed interim orders to halt activities of 76 schemes and final orders against 65 entities for unlicensed investment activities. And, what result did these investigations, or prosecutions deliver for the consumers affected by the scams and not reimbursed for their losses?

While, there have been reimbursements of victims *ordered* by tribunals, and reported in the media as being *underway* (for example for Indian chit fund frauds), we can find no forthcoming articles, nor evidence of actual reimbursement paid to the victims.

See also, box 2 on Kenya where the proceeds of a large Ponzi were actually frozen by Central Bank Kenya but victims remain uncompensated more than a decade later, but the money is apparently gone.

This is a challenge in all the countries reviewed.

6 OUTREACH AND AWARENESS RAISING EFFORTS WITH CONSUMERS

Prevention through outreach and awareness raising efforts with consumers is limited and ineffective. Kenya is the only country reporting that financial services providers, as well as a government authority regularly conduct awareness raising campaigns. It is unclear whether telecoms are similarly conducting anti-fraud campaigns.

In India, regulators have also engaged civil society to communicate with consumers. The frequency of the messaging, framing of the content and efficacy of the campaigns is heretofore unknown.

Further, usage of multiple channels/voices by regulators to communicate with consumers does not seem to be happening. Furthermore, it is necessary to engage the financial services providers, including telecoms in messaging campaigns. Financial institutions generally have 1) the legal obligation to track and report suspicious transactions and patterns of transactions, as well as 2) access to data on potential UDIS operating on their platforms.

To date, technology has helped criminals, but it could also be a tool for regulators for combatting UDIS.

Technology can likewise be used to monitor the web for the existence of these schemes using natural language searches. Yet, no regulator reported regularly monitoring the Internet or social media for these schemes.

In Bangladesh, for example, the Financial Intelligence Unit of the Bank of Bangladesh indicated that they do check the internet for the existence of UDIS, but report that more resources are needed and that the use of artificial intelligence to scan the web for UDIS using key words could indeed be helpful.

See Box 2 for more on a recent Ponzi prosecution in Bangladesh.

BOX 2

BANGLADESH: USING ANTI MONEY LAUNDERING LEGISLATION TO SEIZE PONZI SCHEME PROCEEDS

The Destiny Group was a multi-level marketing pyramid scheme, which operated for 12 years in Bangladesh. At its peak, it claimed to have 4.5 million distributors of its products, and to be engaged in an array of industries from organic fertilizer production and renewable energy to having a cooperative society. Destiny promoters also claimed to have subsidized rice farmers and to have a thriving corporate social responsibility program.[22]

In reality, Destiny was making money off the constant recruits lured in by charismatic promoters; its high profile promoters hailed from Parliament, Dhaka University and included an ex-army general.[23]

It is unclear what specific events lead to Destiny's demise, but per the Bangladesh Bank's report for the Anti-Corruption Commission (ACC), Destiny illegally laundered some 5,000 Crore depositing funds in some 722 bank accounts in the names of 30 related companies.

The ACC was able to seize a small amount of the Destiny crime proceeds due to modifications in the country's anti money laundering legislation of 2015, which allow for emergency seizures.[24] Prior to this modification, relevant authorities had to wait for a final court sentence to act, which allowed for funds to disappear.

Though laudable, these efforts come after the fraud was operational for over a decade and the millions of Bangladeshis who lost their hard-earned taka have not yet received compensation.

7 THE DARK WEB COMPLICATES THE PONZI PICTURE

Because anti money-laundering regulations have made life more difficult for criminals, they seek a less regulated space in which to conduct criminal activities. The dark web or deep web offers fraudsters a petri dish for growth and financial gain. It also offers anonymity, little likelihood of being caught by law enforcement, and it allows access to many potential victims. Of course, the deep web was constructed with noble intentions: such as freedom of expression and access to information in mind; nonetheless, the dark web is actually an ideal environment for criminals too.

The dark web's economy is not based on any fiat currency, it is instead based on crypto currencies (e.g. BitCoin). In this regard, the rise of cryptocurrencies has also enabled criminal activities to flourish within the protection of the dark web. However, the use of cryptocurrencies does not always imply that criminal activities are afoot. Certainly, there are legitimate uses for cryptocurrencies (e.g. an investment, unit of exchange, or store of value).

In this section, we will address two primary questions:

a) Inclusion: does the DFS user community have, or can it easily gain access to the dark web in order to participate in these unlicensed investment schemes?

b) Monetization: How do DFS users who own cryptocurrency earned from Ponzis convert the funds to actual fiat currency, because the three focus countries do not acknowledge cryptocurrency as a legal currency?

This paper will most likely raise more questions than it answers. Our purpose is simply to highlight that this financial activity is happening under the cover of the dark web, and formulate a plan to better understand and deal with this dynamic and growing marketplace for financial fraud.

7.1 Inclusion

The dark web is usually associated with hackers, and cybercriminals, who are very computer literate. While connecting to it may seem like a difficult task with many prerequisites, it is in fact a mere two clicks away for anyone with Internet access. The *main highway* to connect is the Tor,[25] which requires a special web browser to surf it. Once installed, access to the dark web is granted. This access is also available on mobile platforms such as on Google store,[26] which means that the prerequisites for connecting are just a smartphone, or a computer and a data connection.

With access made easy, inclusion into the world of cryptocurrency requires one additional item—a wallet. Since cryptocurrency is a virtual coin, a virtual wallet for cryptocurrency is also required. A cryptocurrency wallet is described as a secure storage on the internet (not necessarily in the dark web), which records transactions and reflects the balance on account. Although considered less secure, many services offer free wallets, which are good enough for the novice trader. More secure wallets are available for a fee paid in cryptocurrency making the inclusion process very easy. Starting from ground zero, a person can start trading cryptocurrency within thirty minutes. Tutorials to become a cryptocurrency trader are available online guiding newcomers step-by-step.

Once connected with the cryptocurrency ecosystem, the user is exposed to a plethora of UDISs which advertise themselves within the dark web and in the public domain, even the infamous MMM scam has a bitcoin investment channel.

7.2 Monetization

7.2.1 Darkweb and crypto currency

Cryptocurrency in all of its variations is not an official currency anywhere in the world although Zimbabwe is considering it,[27] thus making the task of converting it into fiat currency quite difficult. On the other hand, cryptocurrency can very easily converted into goods and services, some legitimate, but many of which are illegal. Cryptocurrency in all of its variations is not an official currency anywhere in the world although Zimbabwe is considering it , thus making the task of converting it into fiat currency quite difficult. On the other hand, cryptocurrency can very easily converted into goods and services, some legitimate, but many of which are illegal.

As of 2015, more and more payment processors are accepting cryptocurrency.[28] As for the illegal side, the dark web offers dozens of marketplaces for drugs, stolen credit card numbers, guns and human trafficking, all of which accept payment in cryptocurrency.[29]

In effect, cryptocurrencies are booming in developing countries, due to three main reasons:

1) It offers protection from fiat currency fluctuations and rising inflation, in most developing countries (e.g. in Zimbabwe, where Bitcoin has become very popular). Our focus countries are no exception: inflation rates are high and the exchange rates of the official currency are not stable, thus it is believed that using cryptocurrency and exchanging for goods and services protects the user from government induced inflation and from the central bank's monetary strategy;

2) It is proven easier to move cryptocurrency across borders because its virtual nature. Trading abroad and moving the profits into the country have no restrictions, nor are there taxes/fees associated with importing foreign currency.

3) Anonymity and security: cryptocurrency isconsidered secure, anonymous and untraceable. This makes it a very lucrative venture for traders who wish to conduct illegal activity such as crime and tax evasion because trading in cryptocurrency is not regulated.

In conclusion, the dark web and crypto currency provide a fertile ground for developing UDISs, and the lack of regulation attracts criminal elements into this ecosystem. In fact, the consulting firm, Strategy India estimates that there are over fifty ongoing crypto currency related UDIS with more than USD 600 million invested in India at present.[30] See Box 3 for recent happenings in India.

The fact that governments do not acknowledge crypto currency as an official currency and regulate its value or exchange, in the hopes of deterring investors and traders may not be achieving the desired result. The financial underworld is evolving and the black market makers have moved from cash to borderless virtual, untraceable and anonymous cryptocurrency.

7.2.2 Social Network and other internet intermediaries liability

Could social networks and other internet intermediaries be liable for *Aiding and Abetting Financial Fraud?* Previous US Federal Trade Commission (FTC) legal actions have established that payment providers will be held liable for facilitating financial frauds on consumers. In 2010, for example, the FTC won a USD 3.6 million judgment against a payments processor and its subsidiary that were profiting from processing unauthorized debits on behalf of Internet based scams and deceptive telemarketers.

And, various US banks have been recently sued by US Attorney Generals and the Ponzi victims for failing to report suspicious transactions and lack of robust money laundering detection protocols in place. For example, US Attorney General Anne Tompkins, from North Carolina, brought legal action against CommunityOne Bank for allowing a USD 40 million Ponzi scheme to be operational out of one bank account. However, CommunityOne never filed a single suspicious transaction report, ignoring hundreds of suspicious transactions.

The US Attorney Tompkins stated that "Banks asleep at the switch need to wake up. The Banking Secrecy Act applies to more than just drug and terrorist financing." As part of a settlement with the State, CommunityOne was required to pay USD 400,000 in restitution to victims and prohibited from expansion in the state.[31]

If banks and payment processors can be held liable for aiding and abetting Ponzi schemes, it is logical to assume that internet service providers (ISPs), social networks and messaging services may one day be deemed liable for facilitation of unlicensed digital investment schemes.

If a 'but for' test is applied for liability, or if the company has previously been put on notice that crimes are being facilitated by the client or user (e.g. planning terrorist acts or the sale of guns/drugs), then, it would seem that there is a strong argument in favor of legal liability for any company which facilitates, and is profiting from UDIS, albeit indirectly.

For example, Facebook and Twitter are now subject of Congressional inquiries, as well as the investigation by Special Counsel Robert Mueller on their involvement in any manipulation of US Presidential elections in 2016. Facebook profited through the selling of USD 100,000 worth of advertisements to Russian entities which allegedly sought to influence the 2016 US Elections.[32] Are payments processors similarly liable for

BOX 3

INDIAN REGULATORS SEND MIXED SIGNALS ON CRYPTO CURRENCIES

In February of 2018, the Indian finance minister pronounced crypto currencies to *not* be legal tender in India.

Similarly, in April of this year, the Reserve Bank of India (RBI) published a statement that it will no longer provide services to any person or business dealing in crypto currencies, indicating in its 'Statement on Development and Regulatory Policies,' that ***virtual currencies raise concern of consumer protection, market integrity and money laundering among others.***

India has had its fair share of high profile ICO and crypto currency related UDIS. Most recently, a noted crypto currency expert, author and promoter of Bitcoin in India, Amit Bhardwaj was arrested in Delhi for reportedly running a 300 billion Indian Rupee UDIS called GainBitcoin which stole from approximately 8,000 victims. The GainBitcoin debacle comes only six months after the OneCoin UDIS was uncovered by Indian authorities and multiple arrests were made of 23 promoters in the midst of their informational session with potential new investors/victims. It is alleged that 75 Crore Rupees were stolen by OneCoin which was a multi-jurisdictional UDIS.

However, the Indian Government's pronouncement would seem that it is now impossible for crypto currencies and account holders to use commercial banks. This policy does not make sense (from a consumer protection standpoint at least) when one considers that the RBI's 'Statement on Development and Regulatory Policies,' which indicates that it will be conducting a feasibility study related to the development of its own state-backed crypto currency.

fraud facilitation in the focus countries, Kenya, Nigeria and India? And, would ISPs, social networks and messaging companies that facilitate UDIS be subject to liability?

These questions remain unanswered because we have not found any related case law in the three jurisdictions. However, legislation and pending legislation on consumer protection, data privacy and communications issues seem to lean in the direction of a finding of liability for Internet intermediaries which facilitate fraud or the spread of false, or harmful information.[33]

In India, for example, the Information Technology Act of 2000, prescribes obligations for Internet intermediaries with respect to data privacy, but it is unclear whether these same standards of care should apply to the transfer of funds. Payment processors and wallet issuers have indeed been victimized by frauds recently.[34]

8 NEW TECHNOLOGIES COULD BE USED TO COMBAT UDIS

Recently, the background checking company Trooly was acquired by client Airbnb to help root out bad behavior in its online home renting business.[35] Trooly and like technology can be used to detect past bad conduct by individuals, and thus assess the risk of future likelihood to engage in risky or criminal behavior.

It is suggested that similar type of technology be used to conduct due diligence on individuals who are promoting UDIS, or as a know your customer (KYC) measure by financial services providers for account opening purposes.For example, US Traffic Monsoon fraudster Charles Scoville had previously been banned by Paypal in the past for conduct which had violated the company's terms of use. Thus, if PayPal had done a scan of account closures for bad behavior, they could have prevented Mr. Scoville from being given a new account, or could take necessary measures to more closely monitor his account and transactions.

Furthermore, social networks which are facilitating UDIS have the ability to analyze big data and even the technology to manipulate human emotions, and thus behavior. This same technology could be engineered to send messaging to potential investors who are discussing potential investments to beware of potentially fraudulent offers. Just as advertising content is sent to consumers whose psychometric states are deemed receptive in order to entice us to spend money, or to vote in a certain manner, so too can public interest messaging be sent to consumers to warn of potential frauds which are thriving on social networks.

Additionally, when Internet services providers, messaging services (e.g. WhatsApp, Facebook Messenger and Telegram) and social networks are made aware of existing UDIS, they should be obligated to shut down accounts perpetrating frauds. This too is an important role for the telecommunications regulator, and it implies close collaboration and information sharing amongst regulators, criminal investigators and the private sector.

In fact, a cursory review of social network terms and conditions reveals that Facebook's own terms and conditions disallow the use of Facebook "to do anything unlawful, misleading, malicious or discriminatory."[36] And, recently, Facebook has announced a new advertising policy (also valid for affiliate services like Messenger and Instagram) which states that "ads must not promote financial products and services that are frequently associated with misleading or deceptive promotional practices, such as binary options, initial coin offerings or cryptocurrencies."[37]

In the event that social networks, instant messaging services and ISPs are reluctant to scan for criminals that run fraudulent UDISs, external intelligence gathering can and should be used to crawl the internet to find online accounts advertising such UDIS's. This type of intelligence is called Open Source Intelligence, and there are several companies in existence that provide products and services for such intelligence gathering. This technology is directed at finding criminal and terrorist organizations but can certainly be redirected to find fraudulent UDISs.

9 WHY DO VICTIMS CONTINUALLY FALL FOR SUCH OBVIOUS FRAUDS?

There are many theories about what causes humans to suspend rationality, causing them to fail to do any due diligence on potential investments, but there have not been concrete studies which explore the Ponzi victim behavior to determine whether *any* warnings would have been effective to dissuade them. A behavioral economic approach which researches and develops and the new educational methods and regulatory/educational policies is certainly needed to combat UDIS.

It has also been argued by some that the lack of appropriate investment vehicles for consumers in the formal economy may be contributing to their investing in these informal schemes. Thus, this too may be an interesting area of research for legitimate financial services providers.

There are of course victims who were not entirely innocent, meaning that they may have invested knowing that the scheme was a Ponzi and they hoped to cash out in time to make a profit: that is before the scheme collapsed and they may even have recruited others to join for that purpose. Those individuals are not the focus of this paper, but rather, we are concerned with consumers who believed the scheme to be a legitimate investment. Those are the individuals that regulators must seek to better inform and protect.

Conducting research regarding how to better protect these consumers requires interviewing those victims of unlicensed investment schemes to better understand whether and why they blindly trusted the scheme perpetrators. However, these victims are often embarrassed and unwilling to talk about a traumatic experi-

ence which may still be adversely influencing their quality of life. Further, society can be cruel to victims, thus it is no surprise that they seek anonymity.

As illustrated in Box 1, interviews were conducted with several hundred victims of the *Caring for Orphans, Widows and the Elderly* (COWE) Ponzi scheme in Uganda in 2014, many of the COWE victims indicated that when they disclosed that had been victimized by a Ponzi scheme to a friend or trusted confidante, they were subsequently ridiculed and told *they deserved what they got.*

Additionally, in many instances authorities in the countries at issue might be unable to assist the victims. In fact, it is not uncommon for the crime victims to be asked for bribes in order for authorities to pursue an investigation. If Ponzi victims have lost their life savings and also borrowed money to invest in that same fraud, it is unlikely they will even have the funds required to pay the police, or a lawyer, nor should they have to.

Another reason why consumers are persuaded to invest is that the promoters use public personalities and celebrities to endorse their *brands* similar to how legitimate businesses sell products and services. Therefore, more research needs to be done to determine how this messaging can be regulated perhaps through advertising registration for financial products and/or counter veiled.

An interesting consumer diagnostic commissioned by *Financial Sector Deepening Kenya* surveyed Kenyan respondents nationwide and found that 44% of the respondents had been approached to invest in an unlicensed investment scheme. Eight percent *admitted* to investing and losing money (each person loosing on average USD 425). Extrapolating from their survey data, the report concluded that 1 million Kenyans lost money to such frauds for a total of 31 billion Kenyan shillings lost.[38]

Unfortunately, the Kenyan survey did not seek to understand consumers' motivations for investing in the schemes nor why specifically they trusted the promoters.

10 RECOMMENDATIONS FOR ADDRESSING UDIS AT NATIONAL AND INTERNATIONAL LEVEL

a) National level

i. Countries should designate one government body with the primary responsibility for UDIS; including developing a national strategy for combatting UDIS; which includes proactive market monitoring, prevention strategies, investigation/prosecution and consumer education and outreach campaigns. The primary implementing body can opt to outsource and/or coordinate these activities, but should bear the ultimate responsibility for UDIS.

ii. The designated authority should produce regular reports available to the public on the volume of UDIS, the impact on markets and consumers, and the actions taken by government to prevent/interrupt these schemes, seize assets/accounts and act to compensate victims. This entity should operate at the national and sub national levels.

iii. A protocol for information sharing on UDIS should be developed between the public and private sector such that financial services providers, social networks, instant messaging, domain name registrars can convene regularly to share data on suspected UDIS with the appropriate government lead agency.

iv. Financial sector regulators should consider classifying UDIS as a predicate offense to money laundering, thus enabling national anti-money laundering authorities to address the issue and to collaborate fully with other institutions to investigate and prosecute UDIS.

v. Increased monitoring of the Internet and social media is needed to identify and prevent UDIS, but reliance on regulatory monitoring alone is insufficient. Appropriate incentives should be devised by regulators, such the establishment of whistleblower compensation policies, including offering monetary rewards to whistleblowers and protection of their identities and families. Incentives can be offered to financial services employees and DFS agents who spot suspicious transactions, which turn out to be UDIS.

vi. There should be multiple channels established for the public to submit complaints and information regulators about suspected UDIS, including online, free hotlines and SMS. The use of social networks and messaging services should be used to connect with consumers, in addition to offering walk in services and accepting email and standard mail. Regular reports should be generated on these tips/complaints and what investigative or enforcement action followed which should be made public.

vii. Regulators should consider the establishment of a victims' compensation scheme to provide redress for the most vulnerable victims of UDIS.

viii. Regulators should establish penalties for individuals and corporations which knowingly facilitate UDIS with the availability of punitive damages that can be allocated to victims' compensation funds.

ix. Regulators should use new technologies such as artificial intelligence (AI) to proactively monitor social networks, instant messaging and communication services and the dark web for existence of UDIS.

b) International level

i. To enable the establishment of a global entity, or a dedicated department within an existing intergovernmental organization, such as the ITU, or any other international body at the conjuncture of the financial,

investment and telecommunication sector, to address the growing UDIS problem.

a) Terms of references for such an entity are to be drafted by regulators and quasi-regulatory bodies interested in taking an active and formative role in such a body. The initial suggested activities of such a body are as follows:

b) Aggregate and share data on the problem of UDIS globally (including the establishment of an international UDIS watch list).

c) Conduct research on prevention, including consumer education and financial literacy.

d) Conduct awareness raising for national regulators, governments, law and policy makers on the scope of the problem.

e) Advise on how to improve monitoring of markets for UDIS and best practices in terms of closure and prosecution, techniques to track and salvage as much of the related assets as possible.

ii. This entity would also have the mandate to bring financial services and telecom regulators together to share information about such schemes and create an international platform for knowledge sharing.

iii. This entity could also engage in public interest advocacy to protect consumers, and obtain redress for victims of UDIS. Such work could be done in concert with national consumer protection bodies as well as with civil society.

iv. A membership structure for such an entity is proposed which aggregates both national financial and telecommunications regulatory bodies as members, and could be funded by one or more of the following mechanisms:

a) Payment of membership fees by States;

b) Private foundation donations.

c) Contributions from financial institutions' corporate social responsibility (CSR) funds.

v. Contributions from national asset seizures from convicted UDIS criminals, as a result of the new entity's assistance or involvement, or a combination of the above.

ANNEX A

Questionnaire

1) Which regulators have the legal authority to investigate, intervene and shut down unlicensed investment schemes in the country?
2) What are the limitations of their mandate(s)?
3) What activities are consistently taken to monitor markets?
4) Is there a procedure to make government aware of an existing UDIS suspected to be a fraud?
5) What is government protocol when it is made aware of an existing UDIS?
6) Is any information being aggregated on these unlicensed schemes annually?
7) How does a typical fraudulent scheme behave?
8) Are DFS providers setting parameters to flag suspicious flows of funds which could be linked to UDIS? Does the law require this?
9) Are consumer awareness campaigns conducted?
10) Do you believe this problem needs new solutions and if so, what could help in monitoring or prevention?

Endnotes

1. *The Wizard of Lies,* Henriques, Diana, St. Martin's Press, 2011.
2. https://en.wikipedia.org/wiki/International_reply_coupon
3. Jarvis, Christopher, *The Rise and Fall of Albania's Ponzi Schemes,* IMF Working Paper, 99/98.
4. Carvajal, Ana, Monroe, H., Pattillo, C., Wynter, B., Ponzi Schemes in the Caribbean, IMF Working Paper, WP/9/95 .
5. See https://www.theguardian.com/global-development-professionals-network/2016/jan/13/ugandan-victims-still-fighting-for-compensation-years-late-cowe; See http://www.businessdailyafrica.com/26000-pyramid-scheme-victims-sue-for-lost-cash/-/539546/2647582/-/tbbjb1z/-/index.html
5. See https://www.bbc.com/news/business-29916178
6. See https://www.reuters.com/article/us-china-fraud/leader-of-chinas-9-billion-ezubao-online-scam-gets-life-26-jailed-idUSKCN1BN0J6
7. Reeves, Aaron, McKee, M., Stuckler, D., *Economic Suicides in the Great Recession in Europe and North America,* The British Journal of Psychiatry, June 12, 2014.
8. Gurun, U. Stoffman, N. Younder, S., *Trust Busting: the Effect of Fraud on Economic Behavior,* Cornell University, 12 July 2017.
9. According to the International Organization of Securities Commission, regulators' communication with consumers is limited to anecdotal evidence of impact. Final Report, IOSCO, May 2015 https://www.iosco.org/library/pubdocs/pdf/IOSCOPD485.pdf
10. http://ifie.org/ifieasia/SCMalaysia_Fraud_Preso_only_branded[1].pdf
11. World Bank, Global Findex Database, 2017, https://globalfindex.worldbank.org/sites/globalfindex/files/countrybook/Kenya.pdf
12. World Bank, Global Findex Database,2017 https://globalfindex.worldbank.org/sites/globalfindex/files/countrybook/Nigeria.pdf
13. MMM has subsequently restarted and its URL, Facebook page, Twitter and Instagram accounts are still live as of 21 February 2018.
14. Report of the Taskforce on Pyramid Schemes, Ministry of Co-Operative Development and Marketing https://www.slideshare.net/guestd260ae/report-of-the-taskforce-on-pyramid-schemes
15. Per the NPSVI's post of September 6, 2019 at https://www.facebook.com/NPSVI/
16. Ajao, Niyi, ITU Survey responses, September 2017
17. Kulkarni, Amol, ITU Survey Responses, September 2017
18. And, https://mmm-india.net/ remains live as of 12 September 2019.
19. In a Lok Sabha unstarred Question No. 2113, Answered 28th July, 2017 (SHRAVANA 6, 1939 (SAKA), the Minister of State for Finance announced that the Serious Fraud Investigation Office is preparing a comprehensive digital database of shell companies and their associates.
20. *Strategy India Blog,* https://www.strategyindia.com/blog/scam-alerts/
21. Kulkarni, Amol, Survey Responses, September 2017, citing data extracted from Government of India, Ministry of Finance Department of Financial Services, Unstarred Question No. 3880, March 24, 2017/CHAITRA 3, 1939 (SAKA).
22. From http://destiny-2000.com website still live as of 5 March 2018. The Company motto was 'Together we Build Our Dream.'
23. *Destiny Groups Formidable Trap of Deceiving People,* Neazy, Sheikh Nahid, The Independent, 11 March, 2016, available online at http://www.theindependentbd.com/home/printnews/36788
24. See https://www.bb.org.bd/aboutus/regulationguideline/lawsnacts.php
25. Tor is a free software for enabling anonymous communication. For more information : https://en.wikipedia.org/wiki/Tor_(anonymity_network)
26. Google store, https://play.google.com/store/apps/details?id=info.guardianproject.orfox&hl=en
27. http://www.tokenschedule.com/news/zimbabwean-bitcoin-price/
28. https://bitcoinist.com/voguepay-co-founder-bitcoin-will-enable-online-commerce-nigeria/
29. Markets for counterfeit money, counterfeit passports, fake US ID, and illicit drugs can be found on the TOR network ".onion".
30. https://the-ken.com/under-radar-regulation-crypto-con-men-spin-brazen-Ponzi-schemes/
31. Meyerowitz, Steven, Bank to Pay $400,000 to Victims of Ponzi Scheme it Failed to Detect and Report, 4-28-2011, LexisNexis.com
32. https://www.nytimes.com/2017/09/21/technology/facebook-russian-ads.html?mcubz=0
33. Munya, Grace Githaiga and Victor Kapiyo, 'Intermediary Liability in Kenya,' Kenya ICT Action Network, 2012.
34. https://timesofindia.indiatimes.com/city/Noida/rs-5-5-crore-frozen-in-Ponzi-case/articleshow/57135701.cms and https:/www.mdianama.com/2017/09/223-mobikwik-money-missing/
35. Fortune, http://fortune.com/2017/06/16/airbnb-trooly-background-checks/
36. https://www.facebook.com/terms.php
37. https://www.facebook.com/business/news/new-ads-policy-improving-integrity-and-security-of-financial-product-and-services-ads
38. Available online at http://fsdkenya.org/publication/consumer-protection-diagnostic-study-kenya-2/

International Telecommunication Union
Place des Nations, CH-1211
Geneva 20, Switzerland