International Telecommunication Union

FINANCIAL INCLUSION GLOBAL INITIATIVE (FIGI)

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(11/2017)

Security, Infrastructure and Trust Working Group

Discussion Paper: Unlicensed Digital Investment Schemes (UDIS)

Report of Trust Workstream

International Telecommunication Union

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

A new global program to advance research in digital finance and accelerate digital financial inclusion in developing countries, the Financial Inclusion Global Initiative (FIGI), was launched by the World Bank Group, the International Telecommunication Union (ITU) and the Committee on Payments and Market Infrastructures (CPMI), with support from the Bill & Melinda Gates Foundation.

The Security, Infrastructure and Trust Working Group is one of the three working groups which has been established under FIGI and is led by the ITU. The other two working groups are the Digital Identity and Electronic Payments Acceptance Working Groups and are led by the World Bank Group.

Unlicensed Digital Investment Schemes

Collaboration amongst telecommunications, financial sector regulators and criminal investigation authorities is needed to address flourishing criminal activity in the global financial eco-system

Trust Workstream

About this paper:

The paper was drafted by Jami Solli with substantial input including legal analysis from Assaf Klinger, Prof. Felicia Monye, Mercy Buku, Amol Kulkarni, Rashed Mohammed and Niyi Ajao..
Editorial, substantive guidance by Vijay Mauree. Special thanks to entire working group for its continued assistance.

Table of Contents

Executive Summary

Internet fraud in the form of unlicensed digital investment schemes (aka digital ponzis) is at an all time high. In fact, how high, and what the impact on financial exclusion is, nobody really knows because regulators have not been measuring the magnitude of the problem. Judging from past statistics in the pre-digital era, however, we know that this type of financial fraud can both severely harm individual consumers, as well as cause financial system risk, including causing civil unrest.

This paper seeks to better understand the impact of this specific type of fraud on both the consumer and financial exclusion through an analysis of UDIS and the legal/regulatory frameworks in which they thrive in India, Kenya and Nigeria. It also proposes new means to address a new form 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 on the UDIS challenge.

1. Introduction

UDIS are those schemes offered digitally via a domain name/URL, on social networks like Facebook, or via a text messaging services to promote and sell investment opportunities to consumers which are most often fraudulent. Schemes almost always pay returns to investors out of new capital *paid in* from an ever increasing supply of new investors, rather than from a legitimate, profit-generating activity. Schemes usually end, or collapse when there is insufficient new investment flows to sustain payments existing investors.

Examples of UDIS would include a recent Indian scheme in the Uttar Pradesh region in Noida, 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, and which had both a Facebook and URL presence (www.socialtrade.biz) would be included in the working group definition of an unlicensed, digital investment scheme. Ultimately, the scheme collapsed and it was 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.

Another example would be the ongoing MMM schemes, which are active on the internet with both a Facebook presence and some form of this www.countryname-MMM.net 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 and facebook pages.

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 (ie phishing).

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 effort to defraud others. Generally, fraudsters would also have to enlist a small army of ground level investors who then 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 $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 circle in the New York and Florida Jewish communities.

Today, with the facilitation of the internet, social networks and mobile phones, running a ponzi is much easier. Promotion of the schemes can be done from the comfort of one's home using social networks and sms to promote and mobile money to facilitate the transfer the funds in and out. Cryptocurrencies 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 without the need to sell door to door.[2] The internet and digital money also offer new technologies to package a ponzi so that few consumers truly understand what it's true nature is. For example, Initial Coin Offerings (ICOs) of cryptocurrencies have recently provided a new product offering for ponzi perpetrators to defraud unwitting investors.[3] Because it is difficult to analyze the underlying software code and thus business model, more often than not investors are not aware that it isn't a legitimate business.

And, a ponzi perpetrator[4] can also rely on his schemes to be promoted virally, selling in multiple countries simultaneously. If ever subjected to regulatory intervention or investigation in one state, a ponzi operator can simply target other jurisdictions[5]; he is limited only by his own language abilities, or the ability to collude with like minded criminals in the new jurisdictions.

Bank robbers almost always get caught, but ponzi operators rarely do.[6]

In the post internet world, there are three main reasons why financial & telecom sector regulators, consumer advocates and all financial inclusion stakeholders should take the problem of UDIS very seriously. This means allocating needed resources to address the problem, and utilizing existing technologies to monitor the internet and the dark web. To date, judging from the many flourishing UDIS, regulatory efforts have been grossly inadequate, and/or the volume of UDIS is increasing exponentially. In fact, it would not surprise the authors to discover that just like consumer products' manufacturers with multiple brands, that ponzi operators are also operating multiple fraudulent schemes simultaneously.

Concerted, global action against UDIS is now urgent because:

a) UDIS Can Harm the Financial System

The impact of an UDIS on an afflicted nation's economy can be dire and cause harm which lasts for a period of 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 even bring about the fall of a government.

For example, in the late 1990's, Albania was riddled with ponzi schemes and an estimated 50% of the nation's GDP was invested in fraudulent schemes. When the schemes collapsed, civil unrest occurred causing 2,000 deaths followed by a regime change.[7]

Caribbean nations, such as Jamaica and Grenada have also suffered from ponzi collapses whereby 12% and 25% of the nations' GDPs were invested.[8] During the peak of the microcredit industry in East Africa (2005-2007), ponzi schemes also flourished doing untold damage to financial inclusion.[9] Estimates suggest that around 15% of GDP of state of West Bengal was invested in ponzi schemes.[1]

As ponzi schemes migrated to the internet, schemes such as the *Ezubao* ponzi in China emerged. Ezubao purported to be earning profits from peer to peer lending, but it was in reality a ponzi scheme which inflicted massive damages in a relatively short period of time. From its inception in 2014 to discovery in 2016 only two years later, Ezubao stole over $9 billion USD [10]. By way of comparison, Bernie Madoff began his $65 billion ponzi scheme sometime in 1980's, only *turning himself in* following the market crash in 2008 which means he was *in business* for more than two decades.

b) The Harm to Consumers from UDIS May be Irreparable, Impacting Several Generations

The harm from UDIS to consumers can be life threatening, as well as have inter generational effects. Suicide risk increases exponentially when consumers lose money. During the years of 2008-2010 for example, coinciding with the *Great Recession*, suicides in North America and Europe were estimated to be at least 10,000 more than in previous years.[11]

In research done by this author, interviewing 65 victims of the *Caring for Orphans Widows and the Elderly (COWE)* ponzi scheme in Uganda, there were at least 11 victims who committed suicide by hanging, or drowning as a direct result of losing money to COWE fraudsters. One victim indicated that she went to the chemist to purchase poison in order to commit suicide, but did not have sufficient funds. At least one elderly male died in a related incident: falling and hitting his head on a rock while fleeing debt collectors.

Countless other victims experienced high blood pressure (and other stress related illnesses, including depression), divorces occurred, other victims fled the country to war torn Sudan and South Africa to avoid creditors, and still others were incarcerated by their creditors for failure to repay funds borrowed from commercial banks and SACCOs, which they used to invest in the COWE fraud. [12]

Many victims were also forced to pull their children out of school due to an inability to pay school fees.[13] One mother indicated that she sent two of her four children to live with their

[1] See https://www.worldwidejournals.com/global-journal-for-research-analysis-GJRA/file.php?val=April_2015_1429017303__72.pdfhttps://www.worldwidejournals.com/global-journal-for-research-analysis-GJRA/file.php?val=April_2015_1429017303__72.pdf

grandmother in another town, and the other two she sent to *find their own way* in Kampala, because neither she nor grandma could afford to feed them.

Once a fraudulent investment scheme collapses, consumers rarely get their funds back, and an individual's own economic recovery could take many years; if it ever occurs. We have yet to find research on the long term effects of ponzis on victims. And, because most ponzis are affinity frauds, victims entire families and social networks may have also been victimized, so when there is no help from the state, we can only presume that recovery may take many years.

COWE victims for example lost funds in 2007, and when interviewed some 8 years later most still have significant, related (and growing) debts with family members and friends similarly suffering.[14]

c) UDIS Can Cause Financial Exclusion

Financial exclusion can be inferred because once consumers have lost money to fraudulent, unlicensed investment schemes, they no longer have these funds to invest in legitimate, potentially profit generating activities. Further, consumers will probably have an increased distrust of the financial sector (and regulators which failed them), which they may pass on to their children and extended families.

Many an American who was an adult during the *Great Depression* then preferred putting his or her savings in a tin coffee container buried in the garden rather than saving with their local bank. The lack of interest paid by 'the garden bank' was made up for by the security that the money would still be there whenever the depositor required, and access was only a shovel away.

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[15]. Further, the shock waves resonated primarily through social networks.

In the age of internet, ponzi schemes are 1) easier to commit, 2) have greater impact, and they 3) resonate more profoundly through communities.

2. 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, nor to to their digital cousins, UDIS. The silence and failure to act is problematic given the significant negative impact of these frauds on consumers, markets and financial inclusion.

However, the failure to act is perhaps explained by the collective sentiment that 1) the buyer/consumer should beware or *know better*, but are greedy, or 2) there's not much that regulators and policymakers can do about the problem. Both of these sentiments are misguided because in effect little effort has been made to find new solutions, or to understand the motivations of consumers and therefore try more effectively to educate them.

Aside from the aforementioned IMF research on ponzis (2009); the Cornell University study on the impact of ponzis on investor trust (specific to the Madoff scheme), and the Emory University study on characteristics of the typical ponzi investor, there is not a plethora of research on point. There are even fewer studies on UDIS or on effective regulatory prevention efforts.

More research needs to be done on 1) best practices in ponzi prevention, including the use of new technologies to better monitor markets for these schemes, 2) how the use of well framed messaging can warn consumers and impact behavioral change, and 3) regarding the impact of UDIS on consumers and markets (in addition to erosion of consumer trust – what is the impact on financial exclusion in the medium and long terms?). In fact, the author has posed the question to multiple financial sector regulators in ponzi-afflicted developing economies during various ITU meetings, asking whether they are in fact collecting data related to ponzi schemes, or the impact on markets and consumers. The answer has never been yes.

With regard to consumer capability trainings or awareness raising, there are several examples of how the financial sector and securities regulators are trying to educate the public. However, again there has not been research to date on the efficacy of these consumer messaging initiatives.[16]

Malaysia, for example had an outreach campaign[17] 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 mean *licensed*, and engaging religious actors too to help inform the public. This is a very good idea, because fraudsters often use religious figures and gatherings to promote and sell their phony investment schemes. The Ugandan COWE scheme for example hired a preacher's wife to recruit investors. 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.

Outreach and consumer education efforts must be continuous however, but often warnings appear only once a particular ponzi has been identified, then the regulator will respond by posting a warning message to consumers on its website. This is too little; too late. How many consumers regularly check the central bank, or financial security regulators' webpages? Without further investigation, it is safe to say that relying on one forum for communicating with a diverse group of consumers, who may not have access to the internet, with varying literacy levels is woefully inadequate.

A more pro active method of educating the public of the dangers of ponzis was done several years back by the US Federal Trade Commission that published a *bait site* online. The web page offered a *too good to be true* investment offer and when consumers took the bait and entered their credit card details on the site to invest in the scheme, the webpage then flashed a warning message stating ***you almost lost all of your money*** and directed the consumer to an educational page explaining the dangers of unlicensed investment schemes and how to recognize the signs of same.

Another unique method of reaching consumers was reported by the Nigerian SEC to the International Organization of Securities Commission that the SEC was in the process of developing a weekly soap opera based on ponzi schemes to educate the public about the dangers.[18]

These are all good examples, but consistency may be just as important as the substance, and the efficacy of messaging should be measured as well.

3. Case studies by country (India, Kenya & Nigeria)

The three countries selected for further inquiry are countries where the working group has members with deep knowledge of the DFS market, and who provided input on the legal and regulatory frameworks, as well as agreed to conduct research on previously collapsed, or ongoing UDIS involvement in the country. The legal/regulatory reviews were informed by legal professionals from the country at issue.

All three countries have common law roots, but very distinct digital financial services (DFS) markets. Kenya for example boasts approximately 76% financial inclusion thanks in a large measure to the success and market domination of Safaricom's M-Pesa. Nigeria and India lag behind Kenya at 44% and 53% financial inclusion, respectively, but arguably Nigeria and India have greater geographic and language challenges to overcome.[19]

The other shared experience by 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 thanks to the internet and social networks.[20] The MMM UDIS operates via Facebook, Twitter and has numerous functioning web sites with a multitude of various domain names (using a chatbot to interact with consumers), including those URL that

contain the country names India, Kenya and Nigeria. None of the three countries shut down the MMM UDIS. In fact, the URL and Facebook pages affiliated with MMM remain operational in all three countries as of September 2017.

Because market monitoring, and apparently investigation and prosecution phases are challenging, this research sought to better understand the roles of the various regulators in Kenya, Nigeria and India 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:

i. Everyone's the Boss, but No one's in Charge (of UDIS)

In the three countries analyzed, we noted multiple regulators which 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.**[21]***

None of the three countries, however, seems to have **a lead authority** which coordinates the prevention/supervisory efforts amongst all the 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 are both trying to renounce legal responsibility for prevention of unlicensed investment schemes. It has been reported that SEBI has asked for a declaratory judgment from the Supreme Court that ponzi schemes do not fall within its jurisdiction. Similarly, RBI has made the claim that entities operating ponzis do not fall under its purview.[22]

If both SEBI and RBI are allowed to *opt out* of their codified regulatory duties vis-a-vis UDIS, that will leave TRAI holding the hot potato. However, to date, that agency has not yet appeared to engage on the issue of UDIS. 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.

Having too many responsible authorities can cause confusion for consumers, specifically about where to report potential UDIS, and it also increases the likelihood that individual authorities believe another authority should act, thus, none do.

Given the lackluster response to investigating and shutting down of the MMM scheme in all three countries, we presume both may be occurring.

ii. Low rates of prosecution for UDIS and rare reimbursements for the consumer

India seems to be more likely to prosecute (though the bar is set low for comparisons with Nigeria and Kenya), but there is no central database, nor one lead authority responsible for UDIS prevention. There is however a private consulting firm called Strategy India which keeps a running tab on unlicensed, unviable businesses inclusive of UDIS).[2]

The Ministry of Corporate Affairs in India investigated 185 such schemes in the past 3 years through the Serious Fraud Investigation Office, RBI was considering 486 cases of unauthorized collection of money, 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 case over the last three years. SEBI also passed interim orders to halt activities of 76 schemes and final orders against 65 entities for unlicensed investment activities.[23] And, what is the benefit of these investigations, or prosecutions for consumers who have been victimized by the scams if they are not reimbursed for lost funds?

Though, 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 or evidence of actual reimbursement paid to the victims.

This is the case in all three countries.

In Kenya and Nigeria, it is unknown whether data is being collected by regulators on unlicensed investment scheme prosecutions therein. We suspect the answer is no.

iii. Prevention by Outreach and Awareness Raising Efforts with Consumers is Limited and Ineffective

Kenya is the only country that reports that providers, as well as a government authority regularly conduct awareness raising 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 unknown.

[2] *See* https://www.strategyindia.com/blog/scam-alerts/

However, the use of multiple channels/voices to communicate with consumers does not seem to be happening. Further, it is necessary to engage the financial services providers in messaging campaigns. Financial institutions generally have 1) the legal obligation to track and report suspicious transactions and patterns of transactions, and 2) first hand information on potential UDIS operating on their platforms. In some countries, like Indonesia, financial institutions are obliged by law to participate in financial education programmes. Others may be inclined to do so because of corporate social responsibility ethos.

iv. Evolutions in unlicensed investment schemes since Charles Ponzi

The most evident is that UDIS operates now on the internet, using websites, and social networks like Facebook and Twitter for promotion and outreach. Investments are often solicited in Bitcoin. UDIS perpetrators are also flourishing on the dark web, as we will discuss in the next section.

Another interesting twist in the evolution of these digital schemes is present in the MMM scheme which calls itself a *global mutual aid fund,* and not an investment.[24] This appears to be an attempt to avoid the application of securities laws.

Also, as seen in Indian and American UDIS, there has been a borrowing of ideas from legitimate internet advertising, such as the 'pay for click' model. Both the Noida (India)[25] and Traffic Monsoon (USA)[26] schemes solicited funds from consumers who were promised 'jobs' which encompassed the investor/employee paying a fee and then clicking on company adverts or 'likes' on Facebook pages to promote an advertiser, that was purportedly paying for the employer for this service. The UDIS promoters, however had no underlying payment agreements with any external advertisers, and the pseudo companies were simply paying investors from investments of the next tier of investors/victims.

4. How the Dark Web Complicates the Ponzi Picture

Because cash and anti money-laundering regulations have made life more difficult criminals, they seek a less regulated space in which to conduct their 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 (because it is hidden from law enforcement), and it allows access to many potential victims. Of course, the deep web was constructed with noble intentions: freedom of expression and access to information in mind. The road to somewhere, however is paved with good intentions, but the dark web actually is an ideal environment for criminals.

The dark web's economy is not based on any fiat currency, it's based on crypto currencies (e.g. BitCoin). And, the rise of cryptocurrencies have also enabled criminal activities to flourish within the protection of the dark web. Certainly, this is not to state that the use of

crytopcurrencies always implies criminal activities are afoot. There are legitimate uses for cryptocurrencies.

However, just as fiat currency can be used to perpetrate frauds, so too can cryptocurrencies, however, cryptocurrency flows of funds are harder to trace.

In this segment, 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 3 focus countries do not acknowledge cryptocurrency as a valid 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 to formulate a plan to deal with this new and growing marketplace for financial fraud.

4.1 Inclusion

The dark web, or deep web is usually associated with hackers, and cybercriminals, who are very computer literate. And, connecting to it seems like a difficult task with a lot of prerequisites. Conversely, connecting to the dark web is easy and simple, and it's a mere two clicks away for anyone with internet access. The *main highway* to connect is the TOR[34] and a special web browser to surf it. Once installed, access to the dark web is granted. This access is also available on mobile platforms[35], 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 in reality simply secure storage on the internet (not necessarily in the dark web) to keep the transactional records which represent the balance. There are many services that offer free wallets, which are considered less secure, but good enough for the novice trader. More secure wallets are available for a fee paid in cryptocurrency making the inclusion process very easy. From scratch, a person can start trading cryptocurrency within thirty minutes. There are tutorials which guide the newcomer step by step to become a cryptocurrency trader [37].

Once connected with the cryptocurrency ecosystem, the user is exposed to many UDISs which advertise themselves within the dark web and in the public domain[36], even the infamous MMM scam has a bitcoin investment channel.

4.2 Monetization

Cryptocurrency in all of it's variations is not an official currency anywhere in the world (though we read that Zimbabwe is considering it)[3], thus making the task of converting it into fiat currency quite difficult. On the other hand, cryptocurrency is very easily converted into goods and services, some legitimate and many of which that are illegal. For example, according to a recent report nearly 100,000 merchants in Nigeria are accepting cryptocurrency payments [31]. And, as of 2015 more and more payment processors are accepting cryptocurrency [32]. As for the illegal side, on the darkweb there are dozens of marketplaces for drugs, stolen credit card numbers, guns and human trafficking, all which accept payment in cryptocurrency[33].

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 (eg in Zimbabwe, 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 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's easier to move cryptocurrency across borders, and because it's a virtual coin, trading abroad and moving the profits into the country have no restrictions and no taxes/fees associated with importing foreign currency;

3) Anonymity and security: cryptocurrency is considered secure, anonymous and untraceable. Which 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 cryptocurrency provide a fertile ground for developing UDISs, and the lack of regulation attracts criminal elements into this ecosystem. In fact, consulting firm, Strategy India estimates that there are over fifty ongoing cryptocurrency UDIS with more than $600 m USD invested in India at present.[4]

The fact that governments do not acknowledge cryptocurrency as an official currency and regulate its value or exchange, in hope to deter investors and traders is achieving the exact opposite result. The financial underworld is evolving and the black mark makers have moved

[3] http://www.tokenschedule.com/news/zimbabwean-bitcoin-price/

[4] https://the-ken.com/under-radar-regulation-crypto-conmen-spin-brazen-ponzi-schemes/

from cash to borderless virtual, untraceable and anonymous cryptocurrency. Simply ignoring the problem won't make it go away.

5. Does Payment Provider Liability for Facilitation of Financial Fraud Also Imply Social Network Liability?

It has been established from previous US Federal Trade Commission (FTC) legal actions that payment providers will be held liable for facilitating financial frauds on consumers. In 2010, for example, the FTC won a $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.

The federal court in Pennsylvania determined that the payment processors played a critical role in the schemes because they provided access to the banking system, and therefore the means to extract money from consumers' bank accounts.[27] Additionally, global payments provider Paypal has just been sued by a group of victims of the *Traffic Monsoon* ponzi scheme in the US, alleging Paypal should not have ever opened an account for the Traffic Monsoon CEO who had previous convictions for financial fraud. This is a lawsuit that Paypal will probably want to settle out of court.[28]

Is it logical to assume that 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, or if the company has previously been put on notice that crimes are being facilitated by the network (eg planning terrorist acts or the sale of guns/drugs), then, it would seem that there is a strong argument to be made in favor of legal liability for any company which facilitate 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 $100,000 worth of advertisements to Russian entities which allegedly sought to influence the 2016 US Elections.[29]

Are payments processors similarly liable for fraud facilitation in our focus countries, Kenya, Nigeria and India? And, would ISPs, social networks and messaging companies that facilitate UDIS be subject to liability? In Kenya, the first answer is decidedly 'yes,' payments processors have been found liable for facilitation of financial fraud per (cite case). The answer to the second question remains to be seen, but 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.[5] In India, however, it is not clear whether rules pursuant to the Information Technology Act of 2000, which proscribe obligations for internet intermediaries with respect

[5] https://www.apc.org/sites/default/files/Intermediary_Liability_in_Kenya.pdf

to data privacy, whether these same standards of care should apply to the transfer of funds. Payment processor and wallet issuers have indeed been victimized by frauds recently.[6]

6. New Technologies could be used to combat UDIS

Earlier this year, the background checking company *Trooly* was acquired by client Airbnb to help root out bad behavior in its online home renting business.[7] 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.

This same type of technology could be used to conduct due diligence on individuals who are promoting UDIS, or KYC by financial services providers for account opening purposes. For example, in the US Traffic Monsoon case previously mentioned, the promoter of that fraud, Charles Scoville had previously been banned by Paypal for previous financial frauds using Paypal.[8] Thus, if PapPal had done a scan of account closures for bad behavior, they no doubt would have noted that Mr. Scoville either should not have been given a new account, or his new account behavior should have been closely monitored.

Further, social networks which are facilitating UDIS have the ability to analyze big data and even the technology to manipulate human emotions and thus behavior. For example, Facebook *knows* when teenagers are feeling particularly depressed and even potentially suicidal, and can enhance their moods by sending 'likes' as well as positive content.[9]

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 vote in a certain manner, so too can public interest messaging be sent to consumers to warn of potential crimes which are thriving on social networks.
Additionally, when internet services providers, messaging services (eg WhatsApp, Facebook Messenger and Telegram) and social networks are made aware of existing UDIS, they should be obligated to shut down accounts perpetrating frauds.

Just as social networks shut down accounts for inappropriate content, they should be consistent in the application of rules and policies. For example, in a recent example actress Rose McGowan's Twitter account was shut down (albeit briefly) for her use of profanity when

[6] 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/
[7] http://fortune.com/2017/06/16/airbnb-trooly-background-checks/
[8] See the related case *Ezeude v. Paypal Inc. & Paypal Holdings* complaint available online at https://consumermediallc.files.wordpress.com/2017/05/paypal-ponzi-complaint.pdf
[9] https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens; https://www.theguardian.com/technology/2017/oct/05/smartphone-addiction-silicon-valley-dystopia

accusing Ben Affleck of lying about not having knowledge of Hollywood mogul Harvey Weinstein's propensity to sexually violate women.[10] If accounts are shut down for arguably (nominally) bad behavior, then the same standards should apply for crimes like UDIS. Interestingly, the infamous MMM UDIS is a frequent Twitter user.[11]

In fact, a cursory review of social network terms and conditions reveals that Facebook's own terms and conditions disallow the use of Facebook t*o do anything unlawful, misleading, malicious or discriminatory.*[12] Similarly, Instagram and Snapchat terms and conditions of use disallows any posting or behavior that is illegal.[13] Twitter, however, takes a slightly different approach; specifying that the user is responsible for all the content posted, but if Twitter believes it is exposed to liability, it has the right to shut down an account.[14]

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 advertizing 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.

7. Why do Victims Continually Fall for Such Obvious Frauds? And, Would Educational Messaging Make a Difference?

The essence of the Ponzi scheme is not statistical; it is psychological. It creates belief in that which is statistically impossible, and the degree of belief is so strong that anyone who points out the statistical impossibility of the scheme risks being cut off personally by the victim.

- Austrian economist Gary North

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 victim thought process to determine whether any warnings would have been effective. 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, understanding human behavior is essential to creating appropriate messaging

[10] https://www.theguardian.com/technology/2017/oct/12/rose-mcgowan-twitter-suspended-ben-affleck-harvey-weinstein
[11] https://twitter.com/mmmnigsupport?lang=en
[12] https://www.facebook.com/terms.php
[13] https://help.instagram.com/478745558852511; https://www.snap.com/en-US/terms/
[14] https://twitter.com/en/tos

and warnings, as well as designing financial education materials that lead to a discerning, and more financially capable population.

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 money: 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 consumers who believed the scheme to be a legitimate investment are those regulators must seek to better inform and protect.

And, 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 experience 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.

In fact, when this author conducted interviews 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 did disclose that they were a victimized by a ponzi scheme to a friend or trusted confidante, that victims were ridiculed and told *they deserved what they got.*

i. Additionally, in many instances police in the countries at issue (but not only) are unwilling or unable to assist the victims. In fact, it is not uncommon for the crime victims to be asked for bribes in order for the police to pursue an investigation. If a ponzi victim has lost his or her life savings and also borrowed money to invest in that same fraud, it is unlikely he or she will even have the funds required to pay the police, 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 counterveiled.

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; and 8% *admitted* to investing and losing money (on average $425 a piece). 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.[15]
Unfortunately, the Kenyan survey did not seek to understand consumers motivations for investing in the schemes or why specifically they trusted the promoters.

The authors of this publication are currently seeking to interview victims of various Kenyan ponzi schemes in the years 2005-7 in order to understand whether messaging from trusted sources could cause consumers *to distrust* UDIS. Thousands of the Kenyan victims from ponzis which collapsed a decade ago are currently represented by a noted Kenyan human rights lawyer and have an active class action against the Central Bank of Kenya; as well as other state actors alleging a failure to protect the public from financial fraud.[30] Further, it is alleged that ill gotten gains seized by the CBK vanished while under its control.

The authors have made contact with the victims' advocate and are attempting to survey a sampling of victims, but results will not be available in time to be integrated into this paper. The point is to better understand what type of messaging or information may have been effective to warn consumers to not invest in unlicensed investment schemes.

8. Recommendations

Regulators, including telecom, financial services and securities regulators; consumer protection agencies, internet registration and hosting companies, criminal investigators, social networks, internet messaging services and DFS stakeholders should collaborate to take global action to address the problem.

i. Increased monitoring of the internet and social media is needed to identify and prevent UDIS, but reliance on regulatory monitoring alone is insufficient.

    a. Incentives should be created for other private actors to identify these schemes. This can be done through the establishment of whistleblower compensation policies, including offering monetary rewards to whistleblowers and protection of their identities and families.

    b. For example, US federal legislation includes a whistleblower compensation scheme for (insider) information on securities fraud such as insider trading in the 1934 Securities Regulation Act, Sec. 21 A(e). Further, the US False Claims Act (FCA) also has a provision for discretionary compensation to the whistleblower (or relator) and payments can be up to 20% of the amount recovered by the US government for fraud perpetrated while doing business with the US government. The former has

[15] Available online at http://fsdkenya.org/publication/consumer-protection-diagnostic-study-kenya-2/

been used rarely in the SEC's history, but the latter has been used frequently and as a result has recovered billion of dollars annually for the US government.

ii. New technologies such as AI should be used to pro actively monitor social networks, instant messaging and communication services and the dark web for existence of UDIS.

iii. 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, like Whatsapp should also 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.

iv. Public private partnerships between financial institutions, social networks, instant messaging and communication services, domain name registrars and financial sector, securities and telecom regulators to share data on suspected UDIS should be encouraged through regular meetings. For example, ICANN could facilitate information sharing amongst registrars on known criminal organizations or activities associated with specific URL names. Facebook and Twitter can also monitor their name registrations reporting to the telecom regulators when known UDIS lists are available. Webpages and Social Networks having pre-identified key words should automatically be flagged for regulatory review.

v. Establish penalties for individuals and corporations which *knowingly* facilitate UDIS with the availability of punitive damages that can be allocated to victims' compensation funds. Knowing facilitation can be proven by the existence of illegitimate profits being earned through the individual or corporation's referral of investors to the scheme. We suggest that standards be set for platforms which host financial websites and content which solicit investments from the public.

vi. Countries should designate one government body with the primary responsibility for developing a proactive market monitoring, prevention strategies, investigation/prosecution and consumer education and outreach campaigns. The primary body can opt to outsource or coordinate these activities, but should bear the ultimate responsibility for UDIS. This body 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.

vii. The establishment of a global forum should be considered. This entity can aggregate and share data on the problem of UDIS globally, conducts research on prevention (eg AI methods to identify and combat schemes as well as appropriate messaging and other techniques which successfully advise consumers to beware of schemes); and advises national governments on how to improve monitoring of markets for UDIS and successfully

shut them down, and techniques to track and salvage as much of the existing proceeds as possible. This body will also have the mandate to engage in public interest advocacy to ensure consumer protection, trust and security of the internet are prioritized globally. It should also provide a platform for diverse national actors to convene and share experiences on effective practices to combat UDIS.

viii. Regulation of fiat to cryptocurrency conversions, by establishing a regulated and fair channel to monetize cryptocurrency, governments should track the source of profits, possibly tax them (within reason to keep this channel attractive) and to prevent criminal activity. An external actor would be less likely to be influenced by domestic politics which can often deter the prosecution of influential criminals.

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?