Journal of Contemporary Management
Volume 15: Special Edition: Fourth Industrial Revolution presented by UKZN

How can Artificial Intelligence reduce fraud in the inclusive cover niche: A case of developing African countries

BZ CHUMMUN
University of KwaZulu-Natal (UKZN)
chummunb@ukzn.ac.za

ABSTRACT

The article seeks to investigate the relationship between artificial intelligence and fraudulent claims in the inclusive insurance sector in developing countries. Although low-income cover has been classified as an important tool to combat poverty, fraudulent claims continue to escalate and is more a serious threat to the low-income cover market sustainability as fraudsters seem to be a step ahead of the game. Through a review of literature that has flagged to be scarce, the author advances the hypothesis that artificial intelligence is more likely to be successful where the increased use of online purchases of inclusive cover(micro-insurance), high cost of identifying claims fraud, lack of data and resources experienced by the providers of inclusive cover amongst others, are available. The study's drive is predicated on the argument that although with the advances of computing techniques and technology, artificial intelligence systems can be employed to reduce the frequency and severity of fraudulent claims. Despite some identified challenges, the findings reveal that leveraging use of artificial intelligent systems in the low-income cover market could promote the effective sustainability of the inclusive cover niche market as it is an uncertain profit business by nature of its low premium income and high transaction cost compared to the regular insurance market. Finally, the author points to some possible ways for combatting fraudulent claims occurrences through the effective use of artificial intelligence systems in the midst of Industry 4.0.

Key phrases

Artificial intelligence; fraudulent claims; fraudulent-combatting measures; inclusive insurance and low-income households

1. INTRODUCTION

The Fourth Industrial revolution has given rise to a more globalised, interconnected world that ever before (World Economic Forum 2016:8). The digitisation and the internet of things (IOT) have been transformational for business, with assets and infrastructure shifting from the physical to the intangible including the business of insurance (Schwab 2016). The insurance industry stands on the precipice of change, with waves of innovation and disruption unlocking new algorithmic opportunities created by AI and machine learning across all areas of the business including pricing, underwriting, claims and more importantly the detection of fraud. The surge in the use of digital technologies has driven us forward into an age of unprecedented connectivity. Data is now a globally traded currency being one of the most valuable assets and also uses data analytics to extract valuable information(trends and patterns) in inclusive insurance business (ISACA 2011:5). The outcome of data analytics is also known as the science of analysing raw data (Rouse 2008:1). The outcome of data analytics can be used in many operations such as detecting of fraud, enhance efficiency in operations of businesses, identify risks and influence decision making in an organisation. Data analytics has also given rise to AI in the wake of this unprecedented change facing digitisation, the inclusive insurance sector is faced with disruptions and challenges although the low-income cover or micro-insurance has received a lot of attention especially since the last decade from policymakers and other stakeholders as an important drive to mitigate poverty in developing countries (World Bank 2012).

However, for inclusive insurance to succeed in its battle against poverty issues, both the providers of the low-income cover and the low-income households should benefit the former one should be commercially successful and the latter one should be covered in cases of vulnerability (Dahlman, Lasagabaster & Larsen 2016; Biener & Eling 2012). Achieving these two conflicting aims are not easy as the costs associated with micro-insurance should be minimised as the nature of the cover is often related to low premium and high cost of transactions. Fraud committed on a general basis increases the costs of providing insurance to any policyholder. According to a study made by Thompson and Reuters in 2017, the costs related to fraud is more than $1.5 billion a year (Jenner 2017). Cohen, Mccord and Sebstad (2005) mentioned that the feasibility of low-income cover depends highly on control systems that detect and prevent fraud, amongst other costs. According to the International Association of Insurance Supervisors, an act of insurance fraud has been related to an

omission that intended to gain a manipulated benefit for the fraudster or any other related parties (Yusuf & Babalola 2009).

Claims fraud can take into account both a fabrication of losses and a superficial claim of loss amounts (Tennyson 2008). Moreover, fraud can be derived from premeditation or opportunism. Premeditation refers to a scenario where someone seeks cover with the initial intention of committing fraud, on the other hand with opportunism, committing an act of fraudulent act is not necessary the main purpose of subscribing to an insurance policy, but fraudulent act is committed once an opportunity or a case presents itself (Tennyson 2008). The insurance industry invests heavily in identifying and preventing fraud, given the cost to insurers and the honest policyholders who find their premiums increased due to this illegal act. One of the growing areas for counter-fraud investment with the advances of digitalisation in the midst of industry 4.0 nowadays has been the concept of ***artificial intelligence (AI)*** which has started to flow in the insurance industry. However, since research in the field of micro-insurance and combating fraud in this low-income cover segment using AI has been very limited and preliminary, hinder its full running of operations. The development of AI in counter-acting fraud in the inclusive niche segment can only be managed once the types of fraud relating to this specific low-income cover market have been identified and researched but the question arises: can Artificial intelligence really prevent insurance fraud in the low-income sector with all the disruptions happening at present? A point of departure, however, is to determine the different possible kinds of fraud pertaining to the inclusive cover market by scientific measurement thereof.

2. OBJECTIVES

The main aim of this study is to investigate how AI can reduce fraudulent claims in the inclusive insurance sector. Thus, the secondary objectives are thus to:

- Determine the different types of fraud related to inclusive insurance and their consequences;
- Investigate whether fraud happening in the micro-insurance field is more significant compared to regular insurance;
- Identify approaches used to detect fraud in the inclusive insurance using Artificial Intelligence and

- Provide recommendations on to how those fraudulent acts can be mitigated or prevented using Artificial Intelligence in the inclusive cover niche market in the midst of Industry 4.0.

3. DEVELOPMENT OF THE STUDY

3.1 Literature review

3.1.1 A snapshot of different types of fraud related to inclusive insurance and consequences of claim fraud

Inclusive insurance also referred to as micro-insurance relates to "the protection of low-income people against specific perils in exchange for regular premium payments proportionate to the likelihood and cost of the risk involved" (International Association of Insurance Supervisors 2007:9). According to a study made by ILO in 2017, there is evidence of the growing impact of inclusive cover. The number of risks covered by micro-insurance has more than doubled since 200*9.* Micro-insurance covers an estimated 500 million risks worldwide as at present compared to 135 million in 2009 (ILO 2017). Although the low-income cover has increased exponentially, billions of low-income persons remain excluded from quality insurance services. However, inclusion access has been important to provide a safety net against susceptibility to financially excluded households or "emerging" customers being equipped with inclusive cover (Tom & Selvam 2010; Ernst & Young 2014b). The "emerging consumer" at present will be pivotal to a growing market niche in the near future. According to a study made by Ernst & Young in 2014, it is expected that the low-income households will grow exponentially by approximately more than two billion people if given access to inclusive cover in developing economies in the next couple of decade (Ernst & Young 2014b). The increased number of low income included people will be imperative to provide economic welfare and inclusion globally. Thus, inclusive cover has an important contribution in giving financial access to low-income people. The West African countries (Kenya, South Africa, Ghana and Tanzania) and India are the main ones where low-income people are mainly subscribed to and enjoying the benefits of inclusive insurance (Ernst & Young 2014b). However, low-income emerging consumers over the years have seemed to have trust issues in relation to insurance offerings therefore appropriate fraud controls to promote trust is of essence and should be addressed (Ernst & Young 2014b).

Before discussing different types of controls, it is imperative to understand the different types of fraud that are related to micro-insurance. Fraud in insurance can be defined *as "an act or omission intended to gain a dishonest advantage for the fraudster or other related parties"* (IAIS, 2007, Yusuf & Babalola 2009). In the inclusive niche market, insurance fraud can be made by the policyholders during claims investigation or while processing the policy. According to the Money Laundering and Proceeds of Crime Act (2013) chapter 9:24 and international standards of Zimbabwe, insurance fraud is a serious predicate offence. A predicate offence is "an illegal offence, which has the potential to provide funds for money laundering and financing of terrorism". Furthermore, fraud can be committed by any intermediary/broker/agent or any third party as well as by insurance provider employees (IAIS 2007). It may take the form of "padding" that is an increase in the amount of claim; wrong representation of information on an insurance application; claiming death event that has never happened. A relatively more "enabling" supervisory and regulatory framework that regulates the provision of inclusive cover can also lead to occurrence of fraud (IAIS 2007).

3.1.2 Fraud committed by policyholders in agricultural insurance

According to a study made by Glauber (2012), most of the world's low-income households rely on agricultural insurance for a living. According to Barnett and Mahul (2007) agricultural insurance can be defined as crop and livestock insurance to help rural communities and farmers in coping with risks. Some of the cover is offered by insurance companies to low-income farmers on a commercial and non-subsidised basis, but most agricultural cover is offered to subsidise low-income farmers by government to promote financial support and encourage socio-economic development (Mahul & Stutley 2010). Low-income farmers are vulnerable to the financial consequences of climate related events. For this reason, crop insurance allows poor farmers that rely on agricultural activities to earn a living have the opportunity to transfer the climatic risks to insurers (Barnett & Mahul 2007). According to a study made by Glauber (2012), there is a high demand for agricultural insurance as scarcity of food is more prevalent in developing countries than developed ones and climate change is more unpredictable. Agricultural insurance can mitigate the consequences of crops or livestock loss, thereby preventing the rural people from depriving themselves from food in these respective segments. However, there can be higher risks related cover for low-income farmers. As a result of increase in demand, fraud in crop insurance is more likely to occur

(Spink & Moyer 2011). According to a study made by Lloyds (2009), fraud can be high in these areas leading to difficulties in validating the insurance claims. Food fraud has been common throughout history for as long as food has had some economic value (Spink & Moyer 2011). This malpractice has become a common issue in the developing countries where unregulated practices are more likely to be prevalent (Wheatley & Spink 2013).

3.1.3 Fraud committed by intermediaries (Agents/ Brokers)

According to Wharton (2013), people collecting insurance money or premiums on behalf of low-income policyholders in inclusive insurance businesses may be fraudsters against insurers and or policyholders. In the sense the fraudsters can pocket money paid to them rather than submit it to insurance providers. In addition, records could be falsified Mccord, Wiedmaier-Pfister and Chatterjee (2008).

3.1.4 Frauds committed by third party

A common micro-insurance product where third party fraud exists is credit life insurance; if the insured passed away, the life policy is deemed to cover the outstanding balance of the loan amount and include some funeral benefits allocated to the policyholder. However, a common third party micro-insurance fraud can involve conniving with the “funeral societies” (IAIS 2007). For instance, the provider of micro-insurance may not honour its promises to pay for the burial expenses. According to Boyer (2000), the “agent” sometimes may not have submitted the premium income to micro-insurance provider. According to IAIS (2007), validating the terms and conditions of the micro-insurance policy can be difficult by the provider. To mitigate similar types of fraud, a group of people could manage their own funds, thereby counteracting occurrence of fraud by group members (Boyer 2000). Such kind of groups are common in Ghana, where the collection of funds is done by a selected member of the group who is responsible to act as a mediator between the micro-insurance provider and the members of the group (Giesbert, Steiner & Bendig 2011). Another type of third party fraud involves cases where fabricated policies are issued and signed by fraudsters who pretend to be authorised providers of micro-insurance (IAIS 2007). These fraudsters tend to collect premiums but do not honour in validating any valid claims by paying the insured benefits (IAIS 2007).

3.1.5 Fraud committed by insurance providers against insureds

Frauds committed by insurance providers against insureds are popular through mis-understanding, mis-offering due to lack of product knowledge, terms and conditions misunderstanding and illiteracy (Guarnaschelli, Cassar & Dalal 2012; IAIS 2007).

Further, a more stringent supervisory framework is needed to regulate the provision of inclusive insurance products to prevent fraudulent occurrence (IAIS 2007). At times when fraud instances are high also known as “high risk”, the cover related claims can be difficult to validate (Lloyd's 2009). Also, a lenient supervisory framework to regulate the inclusive insurance in developing countries might lead to an opportunity where fraud might be rampant (National Treasury of South Africa 2011).

The negative effect of fraud in the inclusive insurance segment can affect policyholders, micro-insurance providers, the industry as a whole and development and welfare in various ways. The negative effects of fraud in micro-insurance are mainly related to the high cost of cover to low-income people as premiums are charged according to their respective previous claims experience. Further, the low-income insurance pool is depleted therefore is more likely to affect insurers business success. Resultantly the insurance industry’s profitability and welfare are affected accordingly which leads to lack of viability of the whole industry. It also prevents people to invest in the area of insurance. Consequently, insurers will refuse to provide the fraudster with cover next time he/she applies for cover. The providers may also take legal action against the fraudster, which may be expensive for the incumbent in terms of legal representation and costs. The fraudster may also be denied the right to be refunded all premiums paid. Detecting fraud reduces the ability of low-income earners to transfer risk to micro-insurance providers. Counteracting insurance claim fraud can thus assist in overcoming the above-mentioned challenges involved in providing insurance to the low-income households. The next question arises as to why the occurrence of fraud related claims is more common in micro-insurance than regular insurance.

3.1.6 The likelihood of fraud in inclusive cover compared to regular insurance

Although literature flags very limited research into the issue of fraud in the inclusive niche market, the problem of fraud poses a more serious threat in the micro-insurance field than regular one(IAIS 2007). When the providers target the low-income segments to offer

inclusive insurance products, increased risk of fraud is likely to occur due to the higher transaction costs of identifying fraud relative to the size of the policy, lack of resources and data experienced by providers and unregulated or lenient regulatory environment.

According to Tennyson (1997), subscribers of micro-insurance who have generally perceived to pay higher insurance premiums than what was expected have been more likely to be more accepting of fraudulent behaviour to their respective policy than those who did not. Further Tennyson (2008) also added that a negative attitude towards micro-insurance can lead to low-income people in committing fraud. As the nature of micro-insurance is mainly related to low-income people, it is likely that the insurance premiums being paid form an important portion of their monthly income compared to higher remunerated individuals (Churchill 2012). According to Churchill (2012) negative attitude towards micro-insurance is mainly caused by lack of insurance education. Low-income people tend to have little knowledge and education about micro-insurance. Although concerted efforts have been used to financially educate the low-income people about the benefits and value of a micro-insurance policy in assisting them in case of vulnerability and preventing them further into poverty line, results also showed that it has been difficult to convince them to subscribe to a policy when there might be no benefit to be received in return on their respective policy in case of no future risk happening or vulnerability. Negative perception can also be caused by insisting that low-income earners should subscribe to compulsory cover who believed that a cover is not a necessity. Subsequently, they were found to be more prone in committing fraud in order to justify paying for the insurance premiums (Tennyson 2007).

Combating fraud has been seen particularly more challenging in micro-insurance field and would require claim prevention measures that are more thorough. Mitigating fraud in micro-insurance is particularly difficult because it is relatively costly to counter check valid claims and denying paying claims can result into a lack of trust from the low-income cover niche market. Although many measures such as the use of index policies where pay-outs are based on rainfall instead of customers in agricultural insurance or partnering with reputable regulators and organisations to remove dishonest claimants have been in place over the years, there is the need to move to more appropriate measures in mitigating fraud now that Industry 4.0 has started to flow. The next section reveals how more profound type of fraud mitigating measures can be applied in the inclusive cover field using technology.

3.1.7 The role of Artificial Intelligence in combating fraud-related claims in the midst of Industry 4.0

In the midst of the Fourth Industrial Revolution, the insurance industry like in many other sectors is driven by technology and digitisation. Building on the growing popularity of FinTech (financial technology), we now have InsurTech (insurance technology), the newest term used to describe the blending of insurance and technology (World Economic Forum 2016). Over the past decade where inclusive insurance has been evolving at a rapid pace in developing countries, copious volumes of data, lack of resources to counter verify fraudulent claims have overtaken human capabilities. With the focus on front-end customer interactions taking centre stage, it is no secret that the back offices of most insurance companies follow underlying processes that are often repetitive and monotonous. A considerable amount of resources in terms of money and time is invested in manual tasks that serve as the link to connect various departments and business units. In the wake of immense digitisation, **streamlining business processes and the reduction of fraud** to enhance efficiency and enable better customer experiences have been a prime focus for the insurance industry through technology.

The emerging technology trend so called, Artificial Intelligence (AI) has never gained popularity until Industry 4.0 has started to flow (Schwab 2016). AI has started to play a pivotal role in automated fraud detection for micro-insurers to better enhance fraud prevention measures. "AI relates to the science of making machines do things that would require intelligence if done by men" concluded the father of AI Mr. Marvin Minky (Minsky 2016). One of its main functions was to counteract the issue of fraud in inclusive insurance, an area where fraud is rampant due to lack of resources. Before fraud combating measures using AI are recommended in this study, it is important to highlight the mechanism of fraud in the low-income cover business In the midst of industry 4.0, where digitisation is increasingly being used in the financial services sector, mobile money lying at the core of financial services where inclusive insurance has not been set free from cybercriminals and fraudsters attempts. The rise in the transfer from the conventional way to mobile micro-insurance transfer of premiums has probed into vulnerabilities (Symantec 2016). These have been untested applications that tend to expose financial/personal information to fraudsters. These exposures can easily lead to issues such breaches and frauds for the industry.

One of the biggest breaches is related to the risk of fraud. The use of unstructured supplementary service data (USSD) being a communication technology for transactions has been used for mobile financial services firms such as mobile banking/payment and insurance. The interception of mobile micro-insurance data by fraudsters can happen while it is being transferred. The encrypted mobile data on servers in developing countries compared to the unencrypted mobile data while transferred on servers makes it lenient to breach in developing countries while performing mobile money transactions to pay their micro-insurance policies online (Macharia 2011). Another noted identified weakness by Kenya Safaricom M-PESA a major provider of mobile money in Sub Sahara Africa is related to when low-income households have registered their information and a two-mode authentication is needed to match the user phone number and the account where their money lies. Fraudsters have constantly been on the lookout to breach this process. One of the reasons cited by the Kenya Bankers Association (KBA) Chief Executive has been that fraudsters and hackers are closely connected with employees working on the system giving rise to identity theft (phishing) (Olaka 2017). The fraudsters and cybercriminals are quick to connect with micro-insurance employees online to forge identity asking to change customers' personal details, and contact phone numbers (Olaka 2017). As employees perceives to be dealing with the main account users, the change of details can easily probe the middle man in the attack(fraudster) to move money across using the new phone details.

Over the years mobile banking/payment/remittances and insurance has been the centre of attraction of cyber criminals and fraudsters. (Martini & Choo 2013). Malware experts have invaded mobile tools and the number of communication network attacks has increased in this regard such as preventing mobile money activities to proceed on a mobile device, moving funds on a mobile money platform of which mobile micro-insurance is also part of (McAfee 2013). Alternatively, the application could illegally track all the purchases and movement of funds made by the target user, potentially giving the adversary information about the users' strategies and physical location. Mobile malware can attack any data such as account details recorded on mobile tools (McAfee 2013)

Although cyberattacks are not directly fraud-related in the low-income insurance sector (Arachchilage & Love 2014), according to Agostinho & Cherry (2016), claims fraud has been classified as a major attack in the field of micro-insurance. Most of these fraudulent acts

happen because of limited resources and expensive process to trace fraud-related claims by micro-insurance providers (Agostinho & Cherry 2016).

4. RECOMMENDATIONS

To generate the combating fraud process and detection, AI must be fed with lots of data. Within the Fourth Industrial Revolution, big data that relates to large amount of dataset explores the opportunities for small policies in the micro-insurance space and provides new information that can be utilised to counteract this disruption. Further it allows providers to counteract information while processing claims and avoid fraud in micro-insurance field (Kumbla 2016).

Advances in AI and machine learning are making it possible to leverage new and unstructured sets of data. With fewer available data sources such as credit histories, online usage, and even national ID systems, developing markets need to be ever more creative in identifying and leveraging unique datasets. New types of data, such as mobile phone usage and social media are already being used to extend credit offerings to previously excluded consumers. However, significant potential risks such as fraud also exists across the micro-insurance value chain, where AI could help improve risk modelling, pricing, collection frequencies, customer acquisition, distribution and detect fraud ultimately.

AI is catching up slowly but steadily in insurance applications and industry perception about its value is changing as and when technology such as InsurTech and Fintech are revolutionising the low-income cover business in the wake of Industry 4.0. For an insurer to derive the greatest value from AI software and functionality, it is important to understand its functions in insurance processes and claims fraud prevention as well as ignore unrealistic notions of replacing humans altogether. According to the dictionary of Computing and Digital Media, AI relates to software that makes decisions based on accumulated experience and information and uses functions such as learning, adapting, reasoning and self-correcting". A scenario of AI is the neural network which stimulates human brain by use of a multilayer perception network rather than rules-based system. It responds to new situations by analysing previous responses, applying them to new situations, evaluating feedback on the selected response and learning a new successful response. The unique characteristic of a neural network is that its knowledge base is accumulative, therefore it become more proficient with claims experience and identifying fraudulent occurrences in insurance, more

likely as human beings do. The most common use form of AI is the rules-based system which applies a set of rules to a data set. When presented with an issue of most likely to be a fraudulent act, it searches a database for statements/logic to provide a decision. Rules-based system cannot establish new rules on their own and must be defined for business issues to be understood such as fraud presenting itself. The inclusive insurance industry can leverage AI in fraud detection during claims processing, in that neural networks and rules-based systems can flag relationship among claimants, doctors, lawyers or any stakeholder involved as well as any other events associated with fraud. After learning the characteristics of fraudulent claims, the network can then speedily spot potential fraud in new claims. A similar approach is used in the credit industry to identify credit card fraud.

When customers submit their application for insurance, there is an expectation that the potential policyholder provides honest and truthful information. However, some applicants choose to falsify information to manipulate the quote they receive. To prevent this, insurers can use AI to analyse an applicant's *social media* profiles and activity for confirmation that the information provided is not fraudulent. For example, in micro-insurance, mostly life insurance policies, social media pictures and posts may confirm whether an applicant is a smoker, is highly active, drinks a lot or is prone to taking risks.

However, convincing social media sites to allow insurers access to their data may prove difficult. Last year, insurance companies attempted to launch an AI which would analyse a subscriber's Facebook page to determine their level of risk; should the AI have deemed the driver as "low risk", they would have benefitted from a discount on the insurance. The project was suspended when Facebook indicated that this technology would breach its rules of privacy.

Even if AI can access all the data contained within someone's social media, it does not prevent people from falsifying information; it merely places another hurdle in the fraudster's way. When insurance schemes are discussed, privacy groups are concerned that people would be encouraged to censor their online presence. It was thought that some may even present false pictures on social media. In theory, fraudsters could simply adjust what they upload and post on social media to convince the AI that the information they have provided in their insurance application is accurate. The idea of "beating" AI in this way can apply

further than in social media. For example, low-income life insurance policyholders who monitor their activity levels via their own applications could allow another more active person to be equipped with their activities, so as to increase the discount the insurance holder receives on their policy.

Insurers can also use AI to detect patterns of insurance fraud within claims. AI is able to spot these patterns using self-educating software that processes ***"big data"*** (extremely large amounts of data from varying sources that can be "mined" to provide information on patterns and trends) to flag claims considered to warrant further investigation. For example, it can help to identify potential large-scale manipulated insurance fraud and duplicate claims by sensing patterns between various claims. AI's high sophistication level means that it will not only consider the policyholder's or third parties' names and addresses (as these can change) but by assessing, for instance, whether similar death circumstances are occurring in the same town, involving comparable alleged injuries. The more claims AI reviews, the better it becomes at spotting those claims that are fraudulent.

AI can also assist insurers with individual claims by querying the alleged events of an incident. For example, if a driver passes away due to an accident and indicates in their claim that it was raining at the time of the incident, AI can check weather reports to confirm if this was the case. If a policyholder's alleged circumstances are disproven by the AI's searches, this indicates that the claim could be fraudulent; the system can then flag that it requires further investigation.

As the AI involved in reviewing fraud in claims relies heavily on "big data" from a variety of sources, it is harder for fraudsters to manipulate this information to fit their requirements. AI's assistance in preventing insurance fraud will only continue to grow, as more and more data is collected and the software increases its ability to spot fraudulent activity through self-education.

5. FUTURE DIRECTIONS FOR RESEARCH

Due to technology and digitisation evolving in the midst of Industry 4.0, it is evident and obvious that more research studies need to be carried out on AI by academics, practitioners and academics in respect of detecting new ways to improve fraud detection in enhancing fraud preventing measures in the low-income cover niche. An even more prominent and persistent issue is to liaise/team up and carry out research and collaborative discussions in understanding how better to pursue fraud combatting incident investigations when AI technological platform is not working in time and how investigations should be undertaken in such case scenario to combat fraud in the inclusive niche market.

6. CONCLUSION

Those who wish to defraud insurance companies currently do so by finding ways to defeat the system. For some uses of AI, fraudsters can simply modify their techniques to “beat” the AI system. In these circumstances, whilst AI creates an extra barrier to prevent and deter fraud, it does not eradicate the ability to commit insurance fraud. However, with other uses of AI, the software is able to create larger blockades through its use of “big data” as explained earlier. It can therefore provide more preventative assistance. As AI continues to develop, this assistance will become of greater use to the insurance industry in their fight against fraud. The value of AI lies in its ability to improve the quality of decisions in preventing frauds and to improve the skills/competencies of humans working on the AI technology. Although equipped with speedy and error-free efficiency technological attributes, AI cannot use common sense or intuition on its own and put a decision into context. The insurance will rely on the expertise of its human resources and talent. AI will deliver on its promises in combatting fraud only if insurers in the low-income cover segment take time to understand when and how best the technology revolutionising the Fourth Industrial Revolution may best be used. AI can certainly increase the collective human intelligence about preventing fraud in the inclusive niche market but it certainly cannot replace it.

REFERENCES

AGOSTINHO PJF & CHERRY CJ. 2016. The significance of claims fraud in micro insurance and a statistical method to channel limited fraud identification resources. *South African Actuarial Journal* 16.

ARACHCHILAGE NAG & LOVE S. 2014. Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behaviour* 38:304-312.

BARNETT BJ & MAHUL O. 2007. Weather Index Insurance for Agriculture and Rural Areas in Lower-Income Countries. *American Journal of Agricultural Economics* 89(5):1241-1247.

BIENER C & ELING M. 2012. Insurability in Micro insurance Markets: An Analysis of Problems and Potential Solutions. *Geneva Papers on Risk & Insurance - Issues & Practice* 37(1):77-107.

BOYER MM. 2000. Centralizing Insurance Fraud Investigation. The Geneva Papers on Risk and Insurance Theory 25(2):159-178.

CHURCHILL C. 2012. Protecting the Poor: A Micro Insurance Compendium Volume II. Geneva: International Labour Organisation.

COHEN M, MCCORD MJ & SEBSTAD J. 2005. Reducing vulnerability: demand for and supply of micro insurance in East Africa. *Journal of International Development* 17(3):319-325.

DAHLMAN C, LASAGABASTER E & LARSEN K. 2016 Inclusive Innovation: Harnessing Creativity to Enhance the Economic Opportunities and Welfare of the Poor. In: Haar J, Ernst R. eds. Innovation in Emerging Markets. International Political Economy Series. Palgrave Macmillan: London. (271-290.)

ERNST & YOUNG (EY). 2014b. Operational Excellence for Insurers—Providing Insurance for the Emerging Customer. [Internet:http://www.ey.com/GL/en/Industries/Financial-Services/Insurance/EY-operational-excellence-for-insurers; downloaded on 25 February 2018.]

GIESBERT L, STEINER S & BENDIG M. 2011. Participation in Micro Life Insurance and the Use of Other Financial Services in Ghana. *The Journal of Risk and Insurance* 78(1):7-35.

GLAUBER J W. 2012. The Growth of the Federal Crop Insurance Program. 1990-2011. *American Journal of Agricultural Economics* 95(2):482-488.

GUARNASCHELLI S, CASSAR G & DALAL A. 2012. Selling More, Selling Better: A Micro insurance Sales Force Development Study. [Internet:http://www.ilo.org/public/english/employment/mifacility/download/brnote14_en.pdf; downloaded on 16 February 2018.]

INTERNATIONAL ASSOCIATION OF INSURANCE SUPERVISORS (IAIS). 2007. Issues in Regulation and Supervision of Micro insurance. Basel, Switzerland.

INTERNATIONAL LABOUR ORGANISATION (ILO). 2017. The Role of Micro Insurance as a Tool to Face Risks in the Context of Social Protection. [Internet::http://www.ilo.org/wcmsp5/groups/public/---ed_protect/-soc_sec/documents/instructionalmaterial/wcms_secsoc_93.pdf; downloaded on 25 February 2018.]

ISACA. 2011. Data Analytics- A Practical Approach. [Internet:https://www.isaca.org/KnowledgeCenter/Research/ResearchDeliverables/Pages/Generating-Value-From-Big-Data-Analytics.aspx.; downloaded on 16 February 2018.]

JENNER A. 2017. Can AI prevent insurance fraud? [Internet:http://disputeresolutionblog.practicallaw.com/can-artificial-intelligence-ai-prevent-insurance-fraud/; downloaded on 11 February 2018.]

KUMBLA S. 2016. The Big Data Effect on the Insurance Industry [Internet:http://www.cuelogic.com/blog/big-data-effect-on-the-insurance-industry/; downloaded on 17 February 2018.]

LLOYDS. 2009. Insurance in Developing Countries: Exploring Opportunities in Micro insurance. Lloyd's Micro Insurance Center: London. (1-38.)

MACHARIA K. 2011. Fraudsters eye mobile money. [Internet:http://www.itweb.co.za/index.php?option=com_content&view=article&id=41727; downloaded on 04 March 2017.]

MCCORD MJ, WIEDMAIER-PFISTER M & CHATTERJEE A. 2008. U.S. Agency for International Development (USAID). Micro insurance NOTE 8 Facilitating an Appropriate Regulatory and Supervisory Environment for Micro insurance.pdf.

MCAFEE. 2013. Mobile Security: McAfee Consumer Trends Report. (Trends in risky apps, mobile misbehavior, and spyware. [Internet:http://www.mcafee.com/us/resources/reports/rpmobile- security-consumer-trends.pdf; downloaded on 02 March April 2018.]

MAHUL O & STUTLEY C. 2010. Government Support to Agricultural Insurance. Challenges and Options for developing countries. Working paper no. 53881. World Bank.

MARTINI B & CHOO KR. 2013. Cloud Storage Forensics: own Cloud as a Case Study. *Digital Investigation* 10(4):287-299.

MINSKY M. 2016. Marvin Minsky reflects on a life in AI. [Internet:https://www.technologyreview.com/s/543031/marvin-minsky-reflects-on-a-life-in-ai/;downloaded on 3 March 2018.]

MONEY LAUNDERING AND PROCEEDS OF CRIME ACT. 2013. Zimbabwe Legal Information Institute. [Internet:https://zimlii.org/zw/legislation/act/2013/4;downloaded on 03 March 2018.]

NATIONAL TREASURY OF SOUTH AFRICA. 2011. The South African Micro insurance Regulatory Framework. [Internet:microinsurance@treasury.gov.za; downloaded on 02 March 2018.]

OLAKA H. 2017. Bank fraudsters focus on customer identity theft- Kenya Bankers Association. [Internet:https://www.capitalfm.co.ke/business/2017/05/bank-fraudsters-focus-customer-identity-theft-kba/; downloaded on 02 March 2018.]

ROUSE M. 2008. Data Analytics. [Internet:http://searchdatamanagement.techtarget.com/definition/data-analytics; downloaded on 15 February 2018.]

SCHWAB K. 2016. The Fourth Industrial Revolution. World Economic Forum. Davos.

SPINK J & MOYER DC. 2011. *Defining the public health threat of food fraud. Journal of Food Sciences* 76(1):57-163.

SYMANTEC. 2016. Cyber resilience. [Internet:https://www.symantec.com/page.jsp?id=cyber-resilience; downloaded on 23 April 2017.]

TENNYSON S. 1997. Economic institutions and individual ethics: A study of consumer attitudes toward insurance fraud. *Journal of Economic Behavior & Organisation* 32(2):247-265.

TENNYSON S. 2008. Moral, Social, and Economic Dimensions of Insurance Claims Fraud. *Journal of Social Research* 75(4):1181-1204.

TOM TR & SELVAM V. 2010. A Study on Fostering Rural Growth through Micro Insurance. *Global Management Review* February 4(2):7-13.

WHARTON. 2013. Micro Insurance: A Safety Net with Too Many Holes. [Internet:http://www.wharton.universia.net/index.cfm?fa=viewArticle&id=1787&language= English; downloaded on 15 February 2018.]

WHEATLEY VM & SPINK J. 2013. *Defining the public health threat of dietary supplement fraud. Comprehensive Reviews in Food Science* 12:599-613.

WORLD BANK. 2012. [Internet:http://siteresources.worldbank.org/INTAFRICA/Resources/social-protection-policy-brief-insurance-EN-2012.pdf.; downloaded on 11 February 2018.]

WORLD ECONOMIC FORUM. 2016. The Global Risks Report 2016. [Internet:http://www3.weforum.org/docs/Media/TheGlobalRisksReport2016.pdf.; downloaded on 25 February 2018.]

YUSUF TO & BABALOLA AR. 2009. Control of insurance fraud in Nigeria: an exploratory study (case study). *Journal of Financial Crime* 16(4):418-435.