

Turnitin Originality Report
 Dissertation (test) (723355) by Abdiaziz Ahmed Siad
 From Self-Check (0 - Special 2021)

Processed on 23-May-2021 05:10 CEST
 ID: 1592069319
 Word Count: 14645

Similarity Index	Similarity by Source
9%	Internet Sources: 3% Publications: 4% Student Papers: 6%

sources:

- 1 2% match (publications)
[Guma Ali, Mussa Ally Dida, Anael Elikana Sam. "Evaluation of Key Security Issues Associated with Mobile Money Systems in Uganda". Information, 2020](#)
- 2 2% match (student papers from 13-Jul-2016)
[Submitted to Utrecht Sales Team on 2016-07-13](#)
- 3 1% match (Internet from 14-Dec-2020)
<https://academic.oup.com/wbro/article/33/2/135/5127166>
- 4 1% match (student papers from 18-Sep-2019)
[Submitted to National University of Ireland, Galway on 2019-09-18](#)
- 5 < 1% match (Internet from 13-Nov-2020)
<https://academic.oup.com/icc/article/29/2/395/5566381>
- 6 < 1% match (student papers from 07-May-2021)
[Submitted to Canterbury Christ Church University on 2021-05-07](#)
- 7 < 1% match (student papers from 07-Apr-2021)
[Submitted to Colorado Technical University on 2021-04-07](#)
- 8 < 1% match (student papers from 28-Jan-2015)
[Submitted to Ghana Technology University College on 2015-01-28](#)
- 9 < 1% match (student papers from 19-Apr-2021)
[Submitted to University of the Philippines - Main Library on 2021-04-19](#)
- 10 < 1% match (student papers from 19-Apr-2021)
[Submitted to Westminster International University in Tashkent on 2021-04-19](#)
- 11 < 1% match (student papers from 28-Aug-2019)
[Submitted to Zambia Centre for Accountancy Studies on 2019-08-28](#)
- 12 < 1% match (student papers from 07-Oct-2016)
[Submitted to Birkbeck College on 2016-10-07](#)
- 13 < 1% match (student papers from 17-Jan-2014)
[Submitted to University of Salford on 2014-01-17](#)
- 14 < 1% match (Internet from 21-May-2020)
<https://www.deepdyve.com/lp/oxford-university-press/mobile-money-and-the-economy-a-review-of-the-evidence-bhCQFnMXoP?articleList=%2Fsearch%3Fquery%3Dmobile%2Bfirst%2Beconomies>
- 15 < 1% match (Internet from 06-Dec-2020)
https://hiiraan.com/news4/2020/July/179284/somalia_s_mobile_money_penetration_high_data_costs_lowest_in_a
- 16 < 1% match (Internet from 28-Feb-2021)
<https://hi.player.fm/podcasts/fincast>
- 17 < 1% match (Internet from 29-May-2020)
<https://pt.scribd.com/document/214105418/All>
- 18 < 1% match (student papers from 25-Apr-2019)
[Submitted to Institute of Technology, Tralee on 2019-04-25](#)

- 19 < 1% match (student papers from 22-Mar-2021)
[Submitted to Kuala Lumpur Infrastructure University College on 2021-03-22](#)
- 20 < 1% match (student papers from 28-Feb-2021)
[Submitted to Lilongwe University of Agriculture and Natural Resources on 2021-02-28](#)
- 21 < 1% match (student papers from 28-Mar-2020)
[Submitted to The Nelson Mandela Africa Institution of Science and Technology on 2020-03-28](#)
- 22 < 1% match (Internet from 14-Oct-2020)
<https://www.researchsquare.com/article/rs-7499/v3>
- 23 < 1% match (Internet from 18-Oct-2017)
<http://article.sciencepublishinggroup.com/html/10.11648.j.jbed.20170202.13.html>
- 24 < 1% match (Internet from 23-Dec-2019)
<https://www.tandfonline.com/doi/full/10.3109/17483107.2014.913716>
- 25 < 1% match (Internet from 26-May-2016)
http://fletcher.tufts.edu/~fmedia/Fletcher/Microsites/IBGC/Gates%20Residency/2013%20Policy%20Memos_ALL.pr
- 26 < 1% match (Internet from 17-Jul-2020)
https://conservancy.umn.edu/bitstream/handle/11299/185186/Wieser_umn_0130E_17706.pdf?isAllowed=y&sequence=1
- 27 < 1% match (Internet from 27-Jul-2020)
https://mafiadoc.com/financial-inclusion-policy-guide_59be95f01723dd4428e59e2f.html
- 28 < 1% match (publications)
[Feng Wang, Ge Bao Shan, Yong Chen, Xianrong Zheng, Hong Wang, Sun Mingwei, Li Haihua. "chapter 44 Identity Authentication Security Management in Mobile Payment Systems". IGI Global. 2021](#)

paper text:

Salford Business School A Robust System to Protect Mobile Money Transfer against Financial Frauds

Student ID : @00566996 A dissertation is submitted in partial fulfilment of the requirements of The University of Salford for the degree of MSc in Information Systems Management. March 21 Declaration Salford Business School

[I've pasted this declaration as a picture so as to reduce the match percentage a little more.] Formatted: Font: (Default) Times, Font color: Black Signature Name (print) ID Number Date : : Abdiaziz Ahmed Siad : @00566996 : March 2021 [Confirm final word count here: should be no more than 16500 words in the main body, excluding tables and illustrations] Formatted: Highlight 1 Instant transactions, as the name implies, enable consumers to pass money in seconds rather than days. Although this capability provides customers with new options, it also has a very real and extremely dangerous side effect: the possibility of immediate fraud losses. The study uncovers the types of financial frauds that are involved in the money transfer system used by people in Somalia. It evaluates the possible measures taken by mobile payment services to prohibit financial fraud. While also identify the network structure(s) implemented by the mobile payment services in Somalia to provide a secure mobile payment system and assess the critical factors related to fraud activities in mobile money transfers. The proposed This research is based on a

mixed method approach, in which **both** the **quantitative and qualitative data collection methods** is **used**

to gather more relevant information [from where? Give some information of data sources]. According to the collective outcomes of this study, the most common

uses of mobile money are for buying **top-ups and local money**

transfers, which are also the

most common uses **of mobile money in most African countries**

. In Somalia, the questionnaires were sent to mobile money users. When asked

if they have ever shared their mobile money PIN, there is a

2

chance

that there could be a response bias based on the possibility that it could occur to

2

users polled that, for example, sharing of mobile money PINs may lead to fraud.

Consequently, the

answer findings cannot necessarily and could not accurately represent the user's actual behaviour. The learner conducting the survey will have an unintentional effect on the input offered by the respondent, causing them to give feedback that they believe is correct rather than what currently occurs. 2

Table of Contents Chapter 1

4

55 1.1 Introduction

55 1.2

Background of the

research 66 1.3 Research aims, objectives, and

questions 77 1.4 Summary

.....

88 Chapter 2

20

99 Literature

Review..... 99

2.1 Mobile payment system 99

2.2 Usage of

the mobile payment system in Somalia 1010 2.3 Impact on the residents

of Somalia for using Mobile Money 1010 2.4 Financial frauds related to mobile

money services 1111 2.5 Execution process of mobile money services to

prohibit fraud 1212 2.6 The infrastructure of the mobile payment system in Somalia

..... 1313 2.7 User Perceptions of Security, Mobile Payments, and E-Commerce

..... 1515 Emerging Market Frauds

..... 1616 Network Busy

..... 1616 Telecom Employees

..... 1616 Identity Theft

..... 1717 Reasons why regulations are

insufficient 1717 Regulatory Issues

..... 1818

Chapter 3

6

..... 2020

Research Methodology

2020 3.1 Research philosophy and method

..... 2020 3.2 Data collection

method 2020 3.4 Data analysis

..... 2222 3.5 Ethical

issues..... 2424 Field Code Changed 3 3.6

Foreseen Limitations..... 2525 Chapter 4

..... 2626 Data analysis and

results 2626 Secondary Data and

Discussions 3333 Chapter 5

..... 3635 Recommendations

..... 3636 Limitations and future study

..... 3838 References

..... 4140 Appendix

..... 5049 Research

methodology 5655 Research philosophy

..... 5655 Research method

..... 5655 Data collection method

..... 5655 Data analysis
 5655 Ethical
 issues..... 5756

**Field Code Changed Field Code Changed Field Code Changed Field Code
 Changed Field Code Changed Field Code Changed Field Code Changed Field
 Code Changed Field Code Changed Field Code Changed Field Code Changed
 Field Code Changed Field Code Changed Field Code Changed Field Code
 Changed Field Code Changed Field Code Changed Field Code Changed Field
 Code Changed Field Code Changed Field Code Changed Field Code Changed
 Field Code Changed Field Code Changed Field Code Changed Field Code
 Changed Field Code Changed Field Code Changed Field Code Changed Field
 Code Changed 4 Chapter 1 1.1 Introduction**

4

The enhanced dispersion of power for mobile devices like smartphones has been transforming how operators and consumers provide and access

financial services, such as mobile money which **has** rendered various emerging
Nations adopting **mobile money as**

1

an easy and emerging platform for payment. Mobile money is also

defined as a major possibility **of financial services** that is reachable **on a mobile
 phone and**

1

provides a service that permits the users to get entree to any Financial service while aexpanding the mobile devices and Ireland the formless accompanying service data codes (USSD) (Vaishnavi and Ibrahim, 2012). Mobile money is now accessible in more than

90 countries with three quarters being the lower and middle-income countries

1

permitting the survey of the

Global System for Mobile Communication. **Mobile money is now**

1

emerging

as the major payment platform for the digital market having around **866 million**
 listed **accounts** with **\$1.3 billion**

21

handled (Weygandt, Kimmel and Kieso, 2017). Despite its benefits, a particularly challenging task comes with managing mobile money, particularly when it comes to the danger of fraud because it not only leads to financial loss to the customers but also the mobile money providers (Rulangeranga, Mpaata and Muwema, 2016). There are also costs to the status of the service to the customers while causing a risk to the status of the business. But lessening the risk of fraud is the major strategy in a strong risk management system. The third parties, banks, and MNOs easily recognize the risk management which is important to the success of sustainable commercial mobile money deployment.

mobile money is a very quick and easy value-added service where the
operators having **risk management strategies are** conscious **of the** complex
nature of mobile money and

11

constantly involved in investing the dedicated resources for handling the fraud as well as a review the assurance activities (Tum, 2015). The risk management strategies usually differ from the operator to operator and such types of policies are also affected by various factors like the stage of development, the structure of the organization, amount of product contributions, governing environment, and the context of the local market. as the entire structure of managing the frog and may vary but there is a present of general Framework which is agreed broadly to be the foundation to any threat management approach present in mobile money (Tobbin and Adjei, 2012). The Framework is composed of four elements that manage the risk for mobile money deployments while determining the appetite of risk, identifying it, monitoring the effectiveness, and established the controls. Various platforms of mobile money and several players as well as stakeholders like MNOs, financial and regulatory institutions, networks of agents, retailers, businesses,

merchants, users of mobile money, and providers of platforms (Tawfik Jelassi, Enders and Martínez- López, 2014). Such players perform various roles and gain distinct advantages from the ecosystem of mobile money. The field of finance, health, education, agriculture, and business use mobile money broadly. An extensive range of services is offered by mobile money which includes credit and withdrawal of the money while transferring the money to other users and paying the service bills (Conklin et al., 2016). Paying for goods from the store, purchasing airline tickets, betting on sports, saving the money for future purchases or the payment, paying the school fees, and taxes (Suryotrisongko, Sugiharsono and Setiawan, 2012). These services are being increasingly implemented across emerging markets as a key instrument for furthering the 5 78% financial inclusion target of Uganda. Several reasons have guided the use of mobile cash systems over the past few years. Technology, consumer behaviours, the distinction of goods and services, supporting laws and legislation, operational partnerships, customer perception, customer preferences, quality of operation, availability, comfort, usability, reliability and protection (Sumit Sharma, 2013). The development of the world's first mobile money services

took place in the Philippines in 2001 when

1

, in collaboration with Banco de Oro (BDO), Smart Communications deployed Smart Money to tackle the

problem of restricted access to banking infrastructure

1

Globe Telecom later launched GCash in 2004 after the

1

successful Smart Money deployment. The inaugural deployment of mobile cash in the East African region

was in Kenya when Safaricom initiated M-Pesa in March 2007. M-Pesa was launched in Tanzania in April 2008 by Vodacom Tanzania and Z-Pesa by Zantel

1

. Mobile

Telephone Networks (MTN) initiated its first mobile cash service for Uganda in 2009, after the effective unveiling of M-Pesa in Kenya

1

(Stevenson Smith, 2012). But, apart from many advantages in enhancing the entree to Monetary Services and also accepting as well as in incorporating the usage

of mobile money has been minimal due to various security doubts and the issues related with the system. young few lengthy long pieces studies have been

1

performed recently regarding the security of mobile money especially in Africa where the topic has not been served in Uganda (Singh and Sharma, 2014). The research contains mobile money security, challenges, method of authentication, and issues in Somalia (Silic and Back, 2016). Various threats and vulnerabilities of the application of mobile wallets are discussed for the respective area. the study primarily focuses on the security system of mobile money where it intends to add to the literature of mobile money security while majorly assessing the safety problems that are coupled with the system of Somalia (Shu, 2014). A very descriptive Research design is adopted by the paper where the results of

this study will accommodate the mobile money workers and the decision-makers in addition to the government

1

for rectifying as well as evaluating the issues that are related to the mobile money system so that original methods are the events can be proposed to discourage the security holes. Somalia's payments are largely obtainable in US dollars, unlike Kenya's popular Mpesa mobile money transfer services. Although, as in Kenya, mobile network operators are firms offering mobile money services, they are gradually creating part of large companies that also propose banking and money transfer services (Shin, 2015). 1.2 Background of the research The increasing use and prevalence of the Internet and technology enable people to be more engaged with digital platforms. The use of mobile payment systems of mobile wallets is increasing day by day because of its ease of use and quick facility of money transfer (Shelton et al., 2014). As well as the technology helping to make the lives of people easier through these mobile payment systems, there are also risks related to it (Mudiri, 2013). The threat of fraudulent activities that can be acted by outsiders is a major risk for mobile payment methods. Financial fraudsters misdirect the user to get their details through which money is taken from the users without their consent. The fraudulent activities are a major drawback as well as a risk of the mobile payment system (Gas, 2017). In Somalia, about 73% of people over the age of 16

use mobile money transfer facilities. The people who have high-level income use most. The proposed research aims to be performed to reveal the usage of mobile payment systems and how the effect of fraudulent activities affects their usage (Owuor, 2018). Along with that, the proposed study will also reveal how the mobile payment services in Somalia developed a robust system to provide more security to the users to keep their data safe against fraudulent activities (Sánchez et al., 2018). 6 Mobile cash transfers in Somalia are worth around \$2.7 billion a month (Omar and Belder, 2016). The remarkable absorption of mobile money has been promoted by many variables: Around nine out of ten Somalis, above the age of 16, own one (Pelletier, Khavul and Estrin, 2017), and most Somalis own cell phones. Almost 60% of the population of Somalia is itinerant, or semi-drifting, and they travel around a lot to discover suitable foraging and water for their livestock (Madise, 2015). Mobile money, therefore, enhances their way of life and is utilized to expedite trade as well (Rowles, 2017). Mobile money is also an important replacement for cash because of concerns about the high frequency of fake money, lack of monetary control, capability, and restricted gain entrance to conventional banking services. Mobile money today also promotes large remittance flows that, owing to a shortage of jobs in the Somali labour market, are crucial for most Somali households. Taking benefit of this development, payment firms are gradually working with telecom providers to directly move funds to the mobile money accounts of receivers (Ramada-Sarasola, 2012). Mobile Money and/or the Agency Banking model that it enables have been used in 192 live deployments to:

- Make inventory deposits and transactions
- Bill transfers made in person
- Remittances throughout the region, both over the counter and dependent on the Mobile ? Accounts for transactions
- Remittances from abroad
- Money-saving products
- Goods for lending (Secured and unsecured)

Selling and servicing each of the above products through mobile and agency banking entails a range of risks, some of which are general to all product lines and others that are exclusive to each product. Some forms of theft include using stolen credit cards to pay prepaid cards and sending money abroad using stolen credit cards. MMM Ponzi-type schemes have been recorded in Nigeria, India, and Ghana, where promises of high returns have enticed mobile money subscribers to invest in digital pyramid schemes that later crash, resulting in significant losses (Gumba, 2018). 1.

3 Research aims, objectives, and questions The main aim of this study is to

18

evaluate how financial fraudsters affect the mobile payment system and its usage in Somalia. Along with that, the proposed study also aims to evaluate the steps taken by the mobile payment services and government of Somalia to act against the financial frauds and to provide data protection to the users. To achieve this, the following objectives will need to be addressed: 1. Uncover the types of financial frauds are involved in the money transfer system used by people in Somalia. 2. Evaluate the possible measures taken by mobile payment services to prohibit financial fraud. 3. Identify the network structure(s) implemented by the mobile payment services in Somalia to provide a secure mobile payment system. 4. Assess the critical factors related to fraud activities in mobile money transfers. In addressing these objectives, answers will also be sought for the following research questions: 7 1. What are the types of financial frauds involved in the money transfer system used by people in Somalia? 2. How the execution process is undertaken by mobile payment services to prohibit financial fraud, and what are the possible measures? 3. What is the network structure implemented by the mobile payment services in Somalia to provide a secured mobile payment system? 4. What are the critical factors related to fraud activities in mobile money transfers? 1.4 Summary The study covers various types of financial frauds that are implicated in the money transfer system used by people in Somalia and evaluate the possible measures taken by the mobile payment services to prohibit financial fraud. Following this introduction, the second chapter presents the literature review where data is gathered from peer-reviewed journals, articles, and government website. Chapter 3 details the methodology where the techniques used, the approach is taken, and the selected research approach are discussed. The results of the survey are highlighted in chapter 4, and the dissertation culminates in chapter 5 that will provide recommendations based on the collective results and along with the conclusions. 8

Chapter 2 Literature Review The section of the literature

26

review covers the system of mobile payment and its usage in Somalia. Various articles, journals, published papers, authentic websites, and government data are utilized for the findings (approach and procedure are described in methodology chapter 3: methodology). Fraudulent activities in the field of mobile money have also impacted the President of Somalia so the section covers the influence of mobile money as well as its fraud with the process of execution of mobile money services dun to prohibit fraud. the section also highlights the infrastructure of the mobile payment system in Somalia while describing some emerging market frauds.

2.1 Mobile payment system A mobile payment

28

system or e-payment system is the easiest way to transfer money or making a monetary transaction via an electronic medium (Purwohedi and Gurd, 2019). It is an electronic payment system that enables people to carry out their regular monetary transactions in a paperless way and requires less time compared to a traditional transaction system (Wróbel-Konior, 2016). The use of mobile payment systems has increased due to the increased usage of the internet and more awareness about payment services among people. Mobile money is coming out as a most essential innovation having potential advantages, and it enhances the access of users to financial facilities having

a large number of people who cannot

1

retrieve the bank (Raghavan and Dawson, 2011). A convenient way is being provided by the mobile money for sending the money to anybody who possesses a smartphone or has admittance to the mobile money agent (Pierre-Laurent Chatain, 2011). Reliable options for savings may also be obtained from mobile money for various low-income earners and a decrease in the loss of sales in addition to a good audit path and faster operation, as compared to the cash at a point of sales. Many experts (Rulangeranga, Mpaata and Muwema, 2016) believe that the structure is way safer because the money is not on the SIM card of a user but a crucial server and it has generated huge prospects in the delivery of financial facilities. The standard of mobile money services has improved the living of people which has led to the stimulus of financial advancement (Wright and Cache, 2015). This system of mobile money allows people to retain their funds concealed from relatives or friends who could ask for money (Omwansa and Sullivan, 2012). It also greatly cut down the expenses as well as prevent lags in time which are correlated with operating, launching, and handling a conventional bank account (Pirinççi and Demirtaş, 2020). Various successful deployments in the arena of mobile money have preceded the expansion of mobile trade in the evolving world. The transfer services of mobile money have entirely transformed the way users used to transfer money because it is cheaper than electronic transfer services and comparatively considered to be more trustworthy than actually transporting money. Small and medium-sized firms enable mobile money to obtain and make payments instantaneously with the help of smartphones and enhanced the networking of business. Mobile money may also lead to economic development with the help of increased savings and Investments. The services of remittance are also increased due to productiveness (Money, 2014).

9.2.2 Usage of the mobile payment system in Somalia

The increasing usage of mobile payment systems was started many years back when mobile network operators formulated mobile money services (Mensah, Chuanyong and Zeng, 2020). At that time, it was convenient and quickly usable for people. After the increasing use of mobile money services, the companies in Somalia started expanding the operations and formed many conglomerates that provide money transfer and banking services (Zeadally, 2018). According to the report of Owuor (2018), mobile money transactions worth \$2.7 billion/ month in Somalia. The lifestyle of people in Somalia matches the requirement of mobile money payment. Almost 9 out of 10 people above 16 years of age have a mobile phone (Gilman and Joyce, 2012), and domestic analysis data reveals that almost 73% of Somalis who are at their age of 16 and above use mobile money facilities. Apart from that, high-income earners are also the most likely to use mobile money services. However, the most common thing for which mobile money transfer is used is to pay bills (Owuor, 2018). The payment of things like electricity, groceries, livestock, water, charcoal, and durable goods are mostly the reason for using mobile money service (Malala, 2019). Mobile cash penetration is over 80 per cent in urban centres and has also become the currency of preference in rural areas, with a penetration rate of 55 per cent (Dong et al., 2019).

A 2018 World Bank study showed that nearly three-quarters of the population aged 16

15

and older in Somalia used mobile currency (Maddi Davidson, 2012). By contrast, just

39.7 per cent of adults had mobile money accounts in 2018

15

in Nigeria i.e., the largest economy on the continent. It is said that only after the collapse of the conventional financial system, the degradation of its banking systems, and the lack of confidence in the Somali shilling, did the country see this development (Qureshi, 2020). Money transactions are mainly in US dollars with 98 per cent of the Somali shilling counterfeit. Although regardless of what caused this highly unprecedented revolution, it brought fiscal prosperity, against all odds, to one of the most notoriously war-torn nations in the world (Luther and White, 2011). Unlike other countries in Africa, Somalis prefer to keep their money in their mobile wallets rather than pay it out: the cash-out figures on our mobile money sites are less than 5 percent, according to research at Hormuud (Asongu, Agyemang-Mintah and Nting, 2021), as individuals transact with merchants directly and digitally. A network that people naturally trust has been planned and developed by Somali telecommunications firms, and this can be seen clearly in the everyday digital buying of products on the busy streets of Mogadishu (Levi, 2010). At the heart of the unique Somali paradigm, this consumer confidence illustrates how the telecommunications sector has been able to make universal use of digital payments, while mobile network providers everywhere continue to fail to convince their customers to keep their money in their mobile wallets. The collapse of the conventional financial system of the world laid the foundations for this development, but its telecoms firms have played a key role (Lartey, 2012).

2.3 Impact on the residents of Somalia for using Mobile Money

At Hormuud, Somalia's largest telecommunications group, people worked to collaborate with local traders and merchants to make money transfers as effective as possible for goods. A mobile payment service, subsidized by the telecoms sector has been developed which is free to connect and free to use (Kwadzo, Adroe and Asante, 2018). And in the same process, it helps in establishment meaning the thriving market of mobile money which has contributed to knock-on effects for the whole country like the creation of a job, price in the local investment, and narrowing the gap in genders through accessing into Financial Services (Kuma et al., 2017).

10 The mobile money network and its services are also positively impacting women in communities throughout Somalia (Zhang, 2020). Various difficulties were encountered by the small businessman due to scaling up their business and challenges from the commercial environment because of the ongoing conflict and many people were reluctant to keep cash saves on their premises for the fear of being targeted by thieves and robbers (Eun et al, 2014). show the introduction of mobile money has benefited in providing such small businesspeople with an account

utilized for buying the supplies and pink employees. the distance between the communities is also decreased by mobile money because it facilitates commercial activities in Somalia. Even the people can send money to those who live and regions far from their shop and they can scale up their enterprises while contributing significantly to the development of Somalia's economy (Huang, 2014). The value of mobile money should not be overstated in a world that has been ravaged by conflict, terror, drought and sectarian violence. One of the main agents of Somalia's economic recovery, its increased security and its political stabilisation has been domestic telecommunications firms (Hazan, Margalit and Rokach, 2019). In 2019, Somalia's GDP increased by an estimated 2.9 percent and is projected to rise at 3.2 percent and 3.5 percent respectively in 2020 and 2021, strong numbers in any region, but especially in one that faces such severe challenges. Special mention of Somalia and its unlikely turnaround was made in 2019 by the Vice President for Africa of the World Bank, Hafez Ghanem. Somalis have been offered an alternative to mere survival after so much suffering: for the first time in many years, hope remains. To Western ears, it can sound odd, but there is something that the West may gain from the example of Somalia (Ramada-Sarasola, 2012). The transition to cashless economies is underway in developing countries around the world, and there are growing fears that the most vulnerable may be excluded, particularly the elderly and those in rural areas (Gupta and Mehta, 2020). 2.4 Financial frauds related to mobile money services The usability of mobile payment systems also increasing the threats related to it. The key fraud related to mobile money services is the data breach of personal information. The other common types of fraud that may occur while using mobile money services are systems fraud, subscribers' fraud, and employee and agent's fraud (Akomea-Frimpong et al., 2019). The fraud that is related to mobile money services is an intentional act that is plotted by financial fraudsters, so there is a high risk while using these payment services. In the context of Akomea-Frimpong et al. (2019), certain reasons cause the weak structure of mobile payment service, and they are weak regulation, weak process, compliance monitoring, less awareness among consumers, and many other things (Rampat and Hildick-Smith, 2015). Some serious security concerns need to be considered apart from the vast advantages posed by mobile money in Somalia. because such troubles have led to the in fragments of the system and causing low acceptance as well as adoption among people, so the associated security issues are: 1. The attack of authentication is a major factor because it has been noted that various attackers are using ways for gaining access to the users' accounts. Attackers are taking advantage of personal identification numbers and resetting the weak procedures (Gumba, 2018). The PIN is used by the present form of mobile money authentication which involves all the mobile money facilities to use the same PIN. the attackers who understand the applications of mobile wallet payment code use quash engineering to damage the passwords for the encryption keys. So, most of the mobile money structures are not safeguarded by considering that the fraudster's skill in the IT 11 department is

to hack the system and steal the customer's money

1

(Stremlau and Osman, 2015). 2. The technology vulnerabilities of

USSD as a session-centred real-time Communication Technology utilized by GSM network

1

for providing the extra services among the mobile client and the request server (Guillén et al., 2015). The main

risk of USSD is that the data carried contained by the channel of communication is not encrypted and making the information of USSD

1

susceptible to attacks. During the process of verification, the client shares the PIN which passes via the system of USSD to the server in plain text where the attacker utilizing the software of the network sniffer intercepts it. There is also the presence of thread to the rerouting of USSD by invaders. ThinSIM is utilized for leveraging the call management to transmit the link of USSD to the server retained by the attacker (Grimwood, 2019). 3. An additional fake or emotional SMS is being used by fraudsters to fool users to disclose their mobile money PIN. This type of scam is called vishing and SMiShing attacks (Gong, Yang and Poellabauer, 2020), and the invader can transmit an

SMS to the user for confirming a payment when no money has been

1

shifted. anonymous phone calls are utilized by the fraudsters for doing false promotions in order to track the customers into revealing their PINs or any other vulnerable private data that is utilized for stealing from their mobile money accounts (Suárez, 2016). The call or message is being sent by the number of the fraudster or either they use very popular with mobile money fraud as employees of service providers who give some random advertisements to consumers that they have won prizes and to say such rates that

they need to send money to the number

1

of fraudsters. Mobile phones are computers to customers or the managers while guiding them across several steps and later resulting

in the removal of money from their bank account to the frauds account

1

(Gas, 2017). No significant study has been conducted to provide a solution, thereby impacting the integrity of mobile purchases,

with the increase of vishing outbreaks on many Somali mobile platforms

1

. "some concerned people have got

PINs from customers under pretences and have consequently withdrawn funds from customer mobile money accounts

1

. "rendering to

MTN Uganda, some sceptical individuals have acquired PINs from customers under pretences and have consequently removed funds from mobile customer money accounts. 4. The denial-of

1

-service (DoS) attack takes place where the invaders are pursuing a specific system of the network with the help of false traffic for blocking the request from the users of

mobile money to access the database (Farha and

1

Chen, 2018). Network instability provides opportunities for theft that largely passes by SIM offline swaps and over-the-counter transfers. The organizations lose revenue and the account of mobile money when the DoS attack takes place by making it more inaccessible to the customers (Eilu and Auma, 2017). 5. Replay attacks occur when SMS-centered services like GCash are majorly susceptible to interference as well as replay attacks. it takes place in the emerging Nations where algorithms like A5 protects SMS. The invaders get these messages because they have the scanning software so while in transit, they modify them and recent them to the designated receivers (Du, 2018). 2.5 Execution process of mobile money services to prohibit fraud The risks related to mobile money transfer can be controlled by adequate monitoring by the organizations that provide money transfer services. The end-to-end encrypted process is an 12 adequate way to safeguard the payment information as well as the personal information of users during the payment as well as after the payment (Akomea-Frimpong et al., 2019). The main mediums through which the fraudulent are done are via scam, anonymous calls, messages, false promotion, and false cash-out message. The organization needs to provide a secure platform for the users, in which the users can reliably complete their money transaction (Owuor, 2018). The security can be increased by making the users aware that about such fraud to keep them away from such fake calls and messages. Many entities strengthen the security of the payment platform to provide more secured services to the users (Dong et al., 2019). The controls in mobile money can be either preventive or detective. Preventive checks can decrease the risk of criminal conduct, whilst the investigator can track and record patterns or events that have already occurred. (Crockett, 2019). Preventive Control ? The preventive controls can control the access rights of the attacker to protect the customer information. segregation of duties can also be performed to lessen the error or scam on procedures of elevated risk like reconciliation in e-money. ? This control can limit the threshold for reducing the risk associated with AML. The awareness of the customer campaigns is initiated to increase education and customer and protection (Bucur, 2015). ? Training of the agents also comes under preventive controls on the acceptable practices, terms, and conditions. ? Training of the employees on roles and responsibilities is also performed (Szabó, 2018). ? They are stronger if they can be applied as the technological elements on the mobile money system. If various controls like access rights, segregation of duties, or hardening of networks are adopted then it becomes essential for this control to be applied (Bhardwaj and Gupta, 2016). Detective control ? This control monitor and analyses the suspicious activities accessing the system. It also creates robust customary course and escalation procedures. ? The agent transaction activities are also monitored by sending SMS alerts to customers. High-value transactions are reviewed by the management (Bashir and Khalid Khan, 2012). ? Deployment scale and resource presence may have a huge effect on whether deployment depends more on preventive or detective controls (Agbor, 2020). 2.6 The infrastructure of the mobile payment system in Somalia The usage of mobile money services is more dependable for people in Somalia compared to traditional services. One of the main reasons that the payment system infrastructure has changed in Somalia is the financial system collapsed in 1991(Gas, 2017). Due to this financial collapsed situation, the people in Somalia faced severe difficulties. The figure below shows a brief framework of mobile money services and their infrastructure in Somalia. 13 Figure 1: Mobile money system in Somalia Source: (Gas, 2017) The increased use of mobile money services, therefore, lead to a greater chance of financial fraud, which is a major challenge for service providers to provide secure payment services. In Somaliland, there is a lot of trusts and a lot of disagreements This section outlines some of the most common categories of disputes that arise by using mobile money platforms: 1) abuse and corruption, such as login theft and unapproved payments; 2) erroneous transfers, such as transferring money to the wrong number; and 3) payment disputes, such as whether one side rejects the transaction, or the sum transferred. Confidence and conflict settlement within a social and

government system focused on personal relationships and clan affiliations are defined in qualitative research on mobile money in Somaliland (Al-Jawad, Connor and O'Sullivan, 2020). Xeer law, which governs relationships and prohibits conflicts from turning into conflict, is founded on clan agreements and favours the wealthy. Zaad, the most popular mobile money service, was introduced in 2009 by Telecom, a mobile phone operator. It was built on the foundation of trust-based networks and a structure based on Xeer law. While some people believe they have no choice but to use Zaad due to societal factors and the network impact, trust in Zaad was found to be surprisingly strong. Customers prefer mobile wallets to cash because they are more secure. When it comes to investments, consumers are less trusting than when it comes to transactions. Customers still have privacy issues and lack interest in digital information. International privacy laws are tightening and placing pressure on the industry. Customers were pleased with Zaad's response to their problems. Zaad has a mechanism in place to report and freeze erroneous transactions, which is normally resolved by the company's administrators (Tawfik Jelassi, Enders and Martínez-López, 2014). If the company cannot resolve problems, Zaad informs the appropriate authorities, who include judicial agencies, traditional elders, and religious figures. The individuals involved determine whether or not a clan chief is involved. Repeat criminals are not meditated with by clan leaders. Many that are not members of a clan must comply with the courts or the police, which can result in fines or jail time (Aydin, 2016). Telesom's business model and outreach approach, along with Zaad's versatility, visibility, and free transfers, are credited with the company's overall growth. Zaad expanded as a result of 14 its ability to meet the need for US dollar currency. Users choose the US dollar to deal with the domestic economy's fluctuations. To access remote areas, there are several issues to consider, including less stable network coverage, power outages, local expectations of utilities, and the provision of an official identification card to use the service. Farmers that come to town on market days are the primary contact with rural areas. The majority of people who live in rural areas are subsistence farmers. The use of US currency causes a gap in urban areas between those who use US dollars, such as businesspeople and NGO workers, and those who are "stuck" in the Somaliland shilling market, such as civil servants (Argent, Hanson and Gomez, 2013). 2.7 User Perceptions of Security, Mobile Payments, and E- Commerce Much research on security in the field of information systems are mostly concerned with technological and deployment concerns. Many consumers, on the other hand, only view protection from a subjective perspective, which is often cultivated by advertising and public knowledge. M-Payment systems are being adopted for a variety of reasons, including security and trust. In a focus group study on mobile payment acceptance, for example, it was discovered that a lack of perceived protection is one of the barriers to adoption. Addressing this barrier to the introduction of mobile payment applications or other electronic payment mechanisms necessitates a thorough examination of security; however, who is responsible for security: the service provider or the user? Researchers also divided the definition of security into two dimensions: quantitative and subjective security. Platform or programme security that is founded on concrete functional characteristics is known as objective security. Security experts, system managers, and backend IT workers are often concerned with these security characteristics. It has been argued that not every user is capable of comprehending or evaluating objective security technicalities. Subjective protection, or the user's perception of the procedure's security, is argued to be a more important metric for determining

how mobile payment security influences **consumer** acceptance (Robinson, 2015). **Adopting a security** strategy **that** tackles **both**

8

objective (security with technical characteristics) and subjective security (mostly bureaucratic and from the perspective of the client) is critical for

2

businesses to maximise revenue potential while maintaining customer trust in the security of their services. Confidentiality, integrity, identification, permission, and non-repudiation are all important security standards for mobile payments, both subjectively and objectively. Subjective and objective defence are not mutually exclusive. However, since users' security attitudes and behaviour can affect objective protection, it can be argued that subjective security influence's objective security. Confidentiality was listed as the top concern of customers in a survey of 4,998 respondents on the subjective protection of m-payment (Mpwanya, 2019). Subjective protection, such as the mobile phone by users with the mobile money service, may influence objective security, as previously said. The following aspects have been listed as influencing how mobile phone users secure their phones in a study conducted in Somalia to identify mobile phone users' information security practises: ? The longevity of mobile phone use affects mobile phone security: a prolonged duration of mobile phone use has a positive impact on mobile phone security policies, and, by extension, the information security risks that the mobile phone consumer faces. Furthermore, users' security habits change over time as their level of sensitivity and understanding of security techniques increases, reducing the risk of user errors. 15 ? The study further shows that a faulty dominant practise culture has a detrimental effect on security activities which may lead to a rise in security threats and instances of those threats. Perfect dominant security culture and strong sensitivity standards,

on the other hand, have a positive impact on

27

a mobile phone user's security habit (Morel, 2019). ? Self-obligation, ideals, and decisions: The commitments

that mobile phone users have to themselves, their values or principles, and their personal decisions all affect their security

8

habits when it comes to protecting their phones. Environment and usage environment: the physical and logical environments in which mobile phones are used affect the security policies followed by users. In a hostile environment, for example, consumers will be more cautious about the protection of their mobile phones than they would be in a secure environment. The value of the handset and the content of the data stored on it: the more mobile the phone is, the better it can be held to avoid loss and unauthorised access. This has an indirect effect on aspects of the mobile phone user's security habits. Those who use less costly phones, for example, are less concerned with how they treat their phones than those who use more expensive phones, regardless of the amount of data collected on the handset (Miller, Bagheri and Vavvas, 2017). Emerging Market Frauds Network Busy Thugs often use network outages in a given location to deposit money on their machines (Gas, 2017). When the agent hands over his phone for them to enter the cell money pin code, they immediately transfer the money but delete the sent message and inform the agent that the network is still down before leaving without paying. With a false message displaying funds on the handset, a fraudster may claim to be in a hurry and ask the agent for cash, then keep the phone to retrieve the money when the network is restored. Con artists often impersonate MTN staff to use the MTN backup customer support for connections or Sim card verification, backed up or registering Sim cards (Luther and White, 2016). They may use a stolen card to commit crimes after replacing it for another. When officers follow the line, they can apprehend an unwitting victim. Money transmission companies like Western Money Union and Money Gram are now being targeted by fraudsters. They hack emails and get all of the sender's and receiver's personal information. They fake the receiver's identity and then remove the funds. By the time the rightful owner arrives to collect the funds, the con artist has already moved on to his next victim (Chaiyasoonthorn, 2019). Telecom Employees Many mobile money consumers can be unaware of how to check their phone's balance and believe that receiving a message equates to receiving real money. Some criminals are now posing as priests or pastors who sent money intended for orphans in error (Alex De Waal, 2015). Many people have no idea how to give money back to another human from their mobile. Some people depend on agents to help them submit the money, and they even give 16 them their passwords. They later discover that no money has been sent to them, even though they have already sent them money. According to investigators, some of the fraudsters are retired telecom workers who conspire with current employees to steal large amounts of money from accounts (Frith, 2019). Identity Theft When identifying details that can be used to identify someone is stolen, it is known as identity theft. This can happen, for example, where technology is used to access or extract a person's identification information in collusion with a rogue agent or a mobile money provider's employee (Samuel Munzele Maimbo and World Bank. Conflict Prevention And Reconstruction Unit, 2006). In key mobile financial services markets, fraud affects both customers and agents. Identity theft by SIM swaps, phishing, advertising and social engineering scams, bogus money deposits, and ATM withdrawal frauds, to name a few, have all been prevalent forms of fraud for years. Internal manipulation has also caused major financial losses for operators in these markets, affecting many mobile money customers (Zavoli and King, 2020). Six MTN workers, for example, robbed \$3.4 million from the company in 2011. Data hacks, unsecure internet surfing on a cell phone, ransomware activity, and smishing/SMS scams can all lead to identity theft (Ji Eun, Jeong and 반영환, 2014). Smishing/SMS fraud is the most prevalent way of stealing identity information by specifically targeting 8end users in countries where feature phones are the dominant mobile platform. Despite massive investments in information management infrastructure, identity fraud continues to be a huge issue around the world. In 2014, for example, a computer protection breach at the country's biggest bank revealed the names, identities, phone numbers, and emails of almost two-thirds of US households (Sharman, 2011). Over years in the United Kingdom, the number of registered identity fraud cases rose by 125 percent to 175,000 in 2017 (Schäferhoff, 2014). A major telecom network reportedly experienced a data breach that compromised the sensitive information of 11.5 million consumers (Muhammed, 2018). Such events show that, while investing in data protection controls is necessary to manage the risks of data leaks and identity theft, it is also important to invest in data security. Identity fraud isn't enough on its own (Jack and Suri, 2011). Reasons why regulations are insufficient Fraud detection is becoming more of a priority for regulators. Although laws mandate providers to devise and enforce appropriate anti-fraud controls, they frequently lack clarity about what should be included in a robust fraud prevention programme (Memmi, Ulf Blanke and Springerlink (Online Service, 2014). This is because the more prescriptive a fraud law is, the faster it will become obsolete. Given the complex and fast-changing nature of fraud, suppliers are increasingly responsible for determining what constitutes effective prevention. International best practices, guidelines, and frameworks can also be followed by financial service providers. A cybersecurity governance system for mobile money providers was recently released by the GSMA. The report examines the "people," "technology," and "process" facets of internal controls and makes suggestions for mitigating the risks associated with each feature (Zhang, 2020). The GSMA Mobile Money Certification, which identifies and encourages competition

in the provision of mobile money services, is another example of

5

a robust risk management system. The certification is a bold step forward for the mobile money industry, highlighting its contribution to

anti-money laundering and counter-terrorist 17 financing (AML/CFT) and

16

providing secure and equal services to consumers (Mas and Radcliffe, 2011). The Certification includes nearly 300 requirements that go beyond legislation in terms of detail and breadth, setting an aspirational bar of professionalism that providers should strive for to reduce the risk of mobile money fraud. Simultaneously, it is critical for providers from various industries to improve their cooperation in the fight against fraud. In Zambia, for example, the local GSM Association and the Banker's Association have agreed to collaborate to address fraud problems under the supervision of telecom and financial sector regulators (Lepoutre and Oguntoye, 2018). Regulatory Issues MMT adoption is increasingly increasing in developing markets, which has resulted in some regulatory problems. In general, both telecommunications and central banks are regulated

in the area of mobile money services. The role of

5

regulators in the mobile money environment is vital to the ecosystem's long-term survival (Liang, Ma and Qi, 2013) (Liang, Ma and Qi, 2013). This emphasises the importance of teamwork and partnership between the two industries to reduce consumer risks. The primary aim of the regulation is to ensure that different laws are followed to protect customer preferences, increase confidence in the payment system, and provide participants with appropriate tools for detecting, assessing, and mitigating market risk.

Mobile Network Operators (MNOs) that offer mobile money services

25

, for example, are regulated in the Philippines; customers must register in person with the service providers using legitimate photographic identification before they can deposit or withdraw cash (K.V.S, 2015). They often limit the amount of money that a subscriber can pass at any given time, day, or month. There are no specific regulatory frameworks for mobile financial services in certain developed countries. Kenya and Cambodia have not released formal rules, but they have allowed MNO-centric models to operate on an ad hoc basis by "no objection" letters, conditional permits, and other means. According to the Jehong Lee (2010) study, based on the business model used, the regulation of mobile money services can vary from country to country. It would be difficult to outsource the cash handling work to a service provider outside the financial institution in a country where only banking institutions manage cash in the form of mobile money transfer. Another question is whether or not a business that provides mobile money services should be licenced as a bank. In Pakistan, unlike Kenya, this is the case. The rise of mobile money remittances has sparked widespread debate over certain compliance challenges that are not covered by conventional financial institution rules (Boik, Greenstein and Prince, 2019). 18 Figure: Depicting regulatory issues 19 Chapter 3 Research

Methodology The conceptual "how" of any piece of research is referred to as research methodology

10

. This section of the study describes how the remainder of the work will be structured and executed to

ensure valid and consistent conclusions that address the study's goals and objectives. The

19

methodology chapter will aim to validate the

design decisions by demonstrating that the approaches and strategies selected are the right match for the research goals and objectives and can provide accurate and consistent outcomes. The findings of a strong research methodology are statistically sound

10

3.1 Research philosophy and method The four philosophies of research are Positivism, realism, pragmatism, and interpretivism. The present proposed research is

6

based on interpretivism philosophy because it aims to provide qualitative information about the research topic (Žukauskas, Vveinhardt, and Andriukaitienė, 2018). This research is based on the interpretivism philosophy as it aims to add new information about the research area along with analyzing the existing information. The research in this dissertation will employ a mixed method, in which both the quantitative and qualitative data collection methods will be used to gather more relevant information (Snyder, 2019). The mixed method is useful for the proposed study because it will help to gather new information for the research, which will add new insights, and the analysis of existing data will provide clear findings of the research area.

3.2 Data collection method Primary data will be collected

23

via a survey that will be conducted online. Survey participants are selected based on their background, occupation, and age, and the population is restricted to Somalia. Participants will also be asked to ensure they have either a smartphone and bank account or a bank account to verify that they are relevant and able to answer the questions in the survey such that relevant information can be captured. As the main aim of the study is to evaluate how the financial fraudsters are affecting the entire system of mobile payment in the people of Somalia. The survey questions are also made while keeping in mind the research objective and research questions. The learner made sure that the research objective is achieved through the responses. As the study indicates that it is only limited to the residence of Somalia so the researcher's started by only asking if they are still living in Somalia or not. This helped in only considering the people of Somalia. As the objective indicates to rectify all the financial frauds present due to utilization of money transfer system so the survey questions are designed two first check if the people are aware of the financial frauds and if they are then what type of fraud they have encountered in past. In addition to others, respondents were asked that where does their run after facing trouble in money transfer and do they trust the bank executive. And it came out little surprising that people and Somalia are aware of almost every mobile money transfer fraud and they know how to react and keep themselves safe. As the research question indicates that what is the process of execution taken by the mobile payment services to restrict financial frauds and what can be the possible measures. so the respondents were not expected to know the legal or technical aspects of the particular process but they were asked if they have some 20 recommendations for possible measures that can be implemented to avoid future frauds. Lack of awareness and knowledge was the only leading factor that made the respondents avoid using mobile money frauds and most of them even admitted while making promises to learn more and explore the system of mobile money transfer. Respondents were a little sceptical regarding the services because they were never trained regarding the operation of mobile money transfers so there was always a fear of using the money and instead of exploring and trying out by themselves, they preferred contacting any bank agent or making any e known individual to pay bills or transfer money on their behalf by giving them cash. The survey was conducted using Google forms and designed concerning the research questions which was shared as a link to the participants. Participants were mostly contacted through the LinkedIn platform and via friends via their emails. The purpose of the research was explained to all respondents and indicated their

participation in the survey is completely voluntary and all of their responses will be kept confidential. No personally identifiable information will be associated with their responses to any reports of these data. Participants were also asked to

12

sign a consent form before they took part. The expectation was that around 35 to 50 participants will take part, thus giving a healthy body of data for final analysis. The above screenshot is one of my contacts I made with the participants.

Secondary data will be collected from online data sources such as Google scholar, Statista, and many other sites that provide relevant information about the research criteria. For the 21 secondary data, relevant sources are selected based on the relevancy of the research aim

6

, and these are summarised below. Inclusion &

exclusion criteria Inclusion criteria Exclusion Criteria ? ? ? ? ? ? Studies related to the

24

topic Studies providing data on Somalia. Studies after the year 2005 Government data regarding Somalia Recent mobile money frauds Studies in the English language Studies with complete results and conclusion ? ? ? ? ? Broad literature not solving the purpose of the study. Studies before the year 2005 Studies have written in a different language apart from English. Studies highlighting other areas of Somalia, but not mobile money frauds. Published journals with only abstract 3.4 Data analysis The primary data is being collected through Google forms where a survey is distributed among the residents of Somalia while the responses are gathered. The secondary data is analysed and collected through hey keyboard search and implementing Boolean operators; which helped in extracting the exact findings to accomplish the research aim. through content analysis, which will help to extract the exact findings from the data. Major secondary data Secondary Source Contribution to study (Vaishnavi and Ibrahim, 2012) ?

Mobile money is now accessible in more than 90 countries with three quarters being the lower and middle- income countries

1

permitting the survey of the Global System for Mobile Communication. (Weygandt, Kimmel and Kieso, 2017) ? ? Despite its benefits, a particularly challenging task comes with managing mobile money, particularly

when it comes to the danger of fraud because it not only leads to financial loss to the customers but also the mobile money providers. The third parties, banks, and MNOs easily recognize the risk management which is important to the success of sustainable commercial mobile 22 money deployment.

mobile money is a very quick and easy value-added service where the **operators** having **risk management strategies are** conscious **of the** complex **nature of mobile money and**

11

constantly involved in investing the dedicated resources for handling the fraud as well as a review the assurance activities. (Argent, Hanson and Gomez, 2013) ? ? Telesom's business model and outreach approach, along with Zaad's versatility, visibility, and free transfers, are credited with the company's overall growth. Zaad expanded as a result of its ability to meet the need for US dollar currency. Farmers that come to town on market days are the primary contact with rural areas. The majority of people who live in rural areas are subsistence farmers. The use of US currency causes a gap in urban areas between those who use US dollars, such as business people and NGO workers, and those who are "stuck" in the Somaliland shilling market, such as civil servants. (Gas, 2017) ? ? ? Thugs often use network outages in a given location to deposit money on their machines. When the agent hands over his phone for them to enter the cell money pin code, they immediately transfer the money but delete the sent message and inform the agent that the network is still down before leaving without paying. With a false message displaying funds on the handset, a fraudster may claim to be in a hurry and ask the agent for cash, then keep the phone to retrieve the money when the network is restored. Con artists often impersonate MTN staff to use the MTN backup customer support for connections or 23 Sim card verification, backed up or registering Sim cards ? The GSMA Mobile Money Certification, which identifies and encourages competition

in the provision of mobile money services, is another example **of**

5

a robust risk management system. ? The certification is a bold step forward for the mobile money industry, highlighting its contribution to

anti-money laundering and counter-terrorist financing (AML/CFT) and

16

providing secure and equal services to consumers. (Sharman, 2011) ? Despite massive investments in information management infrastructure, identity fraud continues to be a huge issue around the world. In 2014, for example, a computer protection breach at the country's biggest bank revealed the names, identities, phone numbers, and emails of almost two-thirds of US households (Al-Jawad, Connor and O'Sullivan, 2020). Most common categories of disputes that arise by using mobile money platforms: 1) abuse and corruption, such as login theft and unapproved payments 2) erroneous transfers, such as transferring money to the wrong number 3) payment disputes, such as whether one side rejects the transaction, or the sum transferred. Confidence and conflict settlement within a social and government system focused on personal relationships and clan affiliations are defined in qualitative research on mobile money in Somaliland. The above secondary data were analyzed to highlight groups of data taken from each study and to produce a collective evaluation of their outputs. 3.5 Ethical issues The expected issue that the study may face is the relevant information from primary data sources, as many people may feel hesitant to share information. The aim of the study and the 24 purpose of the survey will be cleared to them before conducting the survey. Throughout the entire research, the ethical factors will be followed. The research will not share any information of the respondents with a third party, or the privacy will not be harmed. The confidentiality of participants has been taken care of as information of participants is not shared or even in future, will not be shared with any third party. The participants were told before surveying surveying the aim, objective and importance of their responses in the study. nformed consent was sent where the responses were only collected after the acknowledgement from the responders. The participants were not carried through any undue pressure which cajoled or coerced into taking part in the survey. 3.6 Foreseen Limitations The key forecasted limitations that the research may have include limited information from primary sources, limitation to cover up all the research objectives through the primary sources, and the finding might not cover up all the areas of the money transfer system and fraudulent activities related to it. A full discussion of study weaknesses will be given in chapter 5. 25 Chapter 4 Data analysis and results The techniques for gathering survey data have evolved as a result of technological advancements. From face-to-face surveys and telephonic surveys to internet and email surveys, survey data collection has progressed. Each method of survey data collection has benefits and drawbacks, and any researcher prefers to gather accurate data from the target audience. The survey response rates can vary depending on the nature and impact of each of these data collection techniques. Various methods are chosen based on the target group's characteristics and the aim of analysing human behaviour in various ways. The learner used an online survey to collect data because, compared to other methods, it is the most cost- effective and can draw the greatest number of participants. Such data collection techniques are much less successful than these surveys. Since there are many questions to be answered by the target audience, some researchers prefer conducting internet surveys to traditional face-to-face or mobile surveys. Since online surveys are so

efficient, they require **the use of computational logic and branching** **technology to collect survey data that is exponentially more accurate than**

9

any other tool. They're easy to put together and take the least amount of time from respondents. Unlike other

methods, online surveys need very little money to gather survey data.

Data is collected in real time so researchers can analyse it and take corrective

9

measures. Few factors were kept in mind by the learner before framing research questions which led to exploring various characteristics of conducting surveys: ? The survey questions should be related to the survey's goal. That is when the information gathered can be useful to readers. ? Using a cross-tabulation format, learning about the different segments of the target group and their views. ? It's crucial to analyse the data collected. ?

It's futile to survey without getting access to the results and being unable to conclude from the survey evidence. ? It's important to have access to

7

its statistics.

Standard survey techniques, such as pen and paper, are difficult to interpret and need extra manpower. When utilising sophisticated online data collection techniques for an online survey tool including consumer study survey software or consumer survey software, survey data processing gets even simpler

7

. The survey questions were made through Google forms based on various literature and generals that were used in the literature review of the study. Reading multiple papers helped in forming the research question, objective, outcomes, and expected results of the survey. The survey questions for primarily formed based on the research objective and they were sent for review and feedback to the professors. After few improvements, the survey link was distributed through professional social media platforms and email addresses. The population was restricted to only the individuals of Somalia, and the section of being the resident of that country was marked as mandatory. Almost all the survey questions were set as compulsory and hence even if one is left out then the form will not submit the responses. This was done to ensure full completion, even though it may have reduced the overall number of completed surveys. Due to time constraints and technical barriers, a total of 43 responses were received in the set time. As the entire process of filling the form and receiving the result is relatively easy, no major problem was encountered during the survey. 26 Using tools such as graphs, pie charts, and other tables that were made based on responses, this chapter will present the key results as derived from the survey and secondary data. A total of 17 questions were presented in the survey and were written in easy formal language to keep in mind the target audience. Graph 1: showing the somalin residents for making study more precise. Graph 2: Asking the professional background of respondents Graph 3: showing activity of respondents towards using bank facilities 27 Graph 4: showing the usage of mobile money services which will help in interpreting the awareness in Somalia regarding mobile money Graph 5: Current status using mobile money Graph 6: Asking the reason behind respondents not using MMS(mobile money services) 28 Graph 7: Purpose of starting to use MMS Graph 8: Issues encountered during transactions Graph 9: Awareness about the banking process 29 Graph 10: Services provided by MMS Graph 11: Asking respondents about their experience and observations regarding banking managers taking responsibility for their work Graph 12: Potential frauds faced in MMS 30 Graph 13: paying bill digitally Graph 14: Asking for recommendations Graph 15: opinion on security and extra cost in MMS 31 Graph 16: asking if respondents feel the services of mobile money are cheaper or not Graph 17: Perspective based on services offered by mobile money According to the responses, it is demonstrated that the majority i.e., 97.7% of the respondents are residents of Somalia (graph 1). The survey first asked if they use a banking agent or the banking correspondent (graph 2) for performing any online transactions so out of all the responses it is 6% of people use banking agents or banking correspondent which implies that most people nowadays in Somalia are getting aware of all the digital money (graph 3). It is quite exciting to get the responses when around 72.1% used the bank account for transactions that can we deposit or withdraw, and this shows the activeness of residents towards the banking activity (graph 4). Of all the responses around 93% of people use mobile services for day-to-day activities and paying bills so the exchange rate of using mobile money services is quite high and most of the transactions are done through their account only rather than relying on someone else(graph 5&6). But out of the people who have never used mobile money services responds that they are not either aware of it or they do not have enough money to use such services. This shows that people or not actively engaged in what is happening around them because there are various options of opening a zero-balance account also and another factor is that they do not find themselves capable of using the services(graph 7). But apart from not having the money at all, they must be doing daily activities and paying monthly bills so there is a need to encourage such people to at least try mobile money services for making life easier and faster. Beyond this, the main reason people seem to use mobile money is to send money to another person while they also seem to rely on mobile money services because they believe that keeping money and account is a safe place to store 32 and invest (graph 8). People of all age at one point or another in their life experience certain issues while making transactions even though some usually preferred to consult an agent for the same while all the services interrupted, or they send the money to anything wrong number (graph 9). Though people should try to get in touch with the agent if they are not comfortable or short enough to make

transactions as this will lead to a reduction of frauds and unnecessary loss of funds. So for the people who have used mobile money services without an agent and faced issues. They usually run to a mobile money agent or any customer helpline of their particular Bank (graph 10). Around more than half of the respondents believe that, on a scale of 1 to 10, they have multiple options that are available financially to them after they started using the mobile money services (1 being extremely bad to 10 being extremely good) (graph 11). When an individual gets stuck during the transaction to face any issue by losing the trust they usually consult the bank managers or other employees so while experiencing such issues they have encountered that around 68% of bank employees understand their duties towards assistant the consumer in any type of mobile money scam (graph 12 & 13). So, the scans which are being and counted by the people and mobile money is due to a false transaction where an anonymous message was sent to them for sharing the bank details or doing any particular transaction to earn more money and they got manipulated and lost money (graph 14). Due to such scams and interactions in the payment method while facing any network issues people tends to cache directly to the particular organisation or payable rather than relying on someone else or to the bank as it takes comparatively a longer period for showing that transaction done successfully (graph 15). The respondents want the financial service providers to contact them through telephone calls or directly. Out of all the respondents, 42% of people believe that the cost and security of the mobile banking services are comparatively free, and which is very constructive thanks towards the mobile money while some even feel that they are cheap and affordable. Yes, 60.5% of people reply this to the services offered by mobile banking when compared with the traditional banking services if they are cheap or not (graph 16). Lastly, mobile banking services are considered to be extremely good and every aspect but there is only a lack of awareness and some amount of trust issues that people have due to some transaction fraud they have encountered in past (graph 17). Secondary Data and Discussions It can be deduced that mobile money customers assume

that the security of the mobile money provider is unrelated to the security of the

2

mobile phone. In this situation, it seems

that there is no link between mobile phone security and mobile money security.

2

This may imply that, in addition to ensuring the security of the mobile phone

, proper security procedures for the mobile money service would also be implemented. In contrast to this study's findings, a Tanzanian study found that both consumers and non-users of mobile money are unable to use it because

they are afraid of losing money in their mobile wallet if their phones are lost or stolen

2

. Unlike this study, the Acimovic et al., (2018) result concludes

that there is a clear correlation between mobile phone security and mobile money

2

security, although this research indicates otherwise. Improvements in infrastructure and fraud prevention. Taking into account the above, the researchers suggest that, despite the numerous security steps implemented

by both the service provider and the users, the security of the mobile money service should be further improved to deter fraud by implementing the following:

8

33 Set PIN Age

: Since PIN sharing is one of the most common sources of customer-driven fraud, the

service provider should set a PIN age parameter to remind users to update their PINs every quarter

2

(Ahmed, 2019). To complete the PIN update, you must first answer certain personal identity questions about the registered customer. According to the researchers, even though users exchange

their PINs with close relatives and each of those close relatives has access to the phone

2

when

a PIN change request is made, the individual cannot easily change the PIN because the person would not easily know the answers to the initial user's personal identity questions. securing the

2

mobile money wallet at the time of registration. This can be supplemented by the service provider sending mobile money protection tips to customers via SMS at least twice a year to remind them of their security commitments, which can help to improve the service's security. Currency detectors may also be available at service centres and merchant points of sale, according to the recommendations. This will discourage people from depositing and withdrawing bogus currencies (Balasubramanian and Drake, 2015). False currency detectors are now installed in banks, so this will not be a problem at their service centres. The Micro-view of Mobile Money Economics Because of the originality of

mobile money and its new arrival in many countries, few studies have looked at its economics. The mobile money

14

storage and payment system, as well as its payments

to bank savings accounts, micro-insurance, and credit through algorithmic credit scores, could

3

have a variety of effects on households and businesses. In developed countries, mobile money can help alleviate a variety of business failures (Balasubramanian, Drake and Fearing, 2017). Costs of Transactions are being reduced Mobile money lowers the cost of sending and receiving money, which is particularly important considering the insufficient and costly transportation system. Transfers fly an average of 200 kilometres in Somalia,

where families and social networks are scattered due to internal migration

3

(Wright, 2020). Transportation costs, such as going to

a bank, utility company, or government office; travel time and standing in long lines; coordination costs between individuals, firms and customers, and government and individuals, which may be significant in terms of time and money lost; and the costs of delays and "leakages" caused by corruption (or

3

complete loss through theft from insecure methods of money transfer). There's also the cost of wasted money and time. The money

3

, as well as the time, may have been better distributed, invested, or saved. Cash transfer scheduling certainty is improved by automated electronic distribution of cash flows, benefits, social security accounts, and private remittances, allowing for further planning. As a result, coordination, delay, and incentive costs are reduced even more. Improving Transparency and Reducing Asymmetric Information Financial transactions are recorded, which increases financial transparency and eliminates asymmetry of details. Owing to asymmetric data and fixed account processing rates, the structured banking system is unable to forward

credit to vulnerable customers who lack assets and financial records. When cash is passed from under the mattress to an electronic account, it becomes registered cash

3

. A financial history is created for any mobile money

deposit, withdrawal, transfer, or payment transaction

3

. The connection between

algorithmic credit scores and the granting of small loans was

3

addressed previously (Whittaker, 2019). 34 Consumers can be protected against theft, fraud, and disinformation if their payments are recorded electronically. Market purchase costs can be reduced, and

market usage can be increased as a result of confidence. Thoenig and Kim (2011), for example, mentions how the "anonymity of cash" will make it difficult for traders and new vendors to trust each other. Greater transparency across documents, such as the distribution and publishing of reports on purchase costs to foster competition, will better monitor the service. Cheaper international remittance transfers are often made possible through recorded transfers with proper ID documents. Using Digital Means to Change the Nature of Savings and Increase Savings There are a variety of reasons to save. Saving for school, recreation,

marriage, consumer durables, home expenditures, **retirement, and funeral**

3

costs are examples of life-cycle motivations that

compensate for variations **in timing between income and expenditure**

3

sources (SWAILES, 2016). Precautionary reasons (

buffer stock saving) represent **the** uncertainty **of** potential **income and** spending, such as **saving for**

3

jobs, disease, deaths, natural disasters, and the dangers of

old age. Finally, there's saving for bequest

3

purposes, such as giving gifts during one's lifetime or leaving an inheritance to heirs. Thus, saving aids in the allocation of usage over time and the reduction of risk. Their "immersion of tangible cash causes tremendous frictions in their financial lives" for the unbanked poor. Cash-based households have three informal investing options: cash under the mattress, asset investment such as jewellery or dogs, and carrying money in informal savings clubs, both of which are vulnerable to fraud or "liquidation." Savings are often wasted in this manner (Pruzek, 2011). Electronic wallets for mobile money have safe cash storage without the need to pay interest. Secrecy is another advantage. As opposed to

cash receipts, the reduced observability of the timing and sizes of mobile

3

transactions, as well as the unpaid electronic balances, could save the recipient money. Furthermore, in economic psychology literature,

mobile money accounts provide **a practical template**

3

for how the poor can be encouraged to invest, such as by the

use of "commitment" savings accounts(Potnis, 2016). Insurance **and**

3

Risk: Multiple communal shocks, such as floods, scarcities, pestilence, other natural catastrophes, war,

and medical epidemics, as well as idiosyncratic shocks, such as **theft**, disruption **to the homestead**, sickness, **and death in the**

14

household, threaten the poor's living standards. There are just a few options

for insuring against these dangers. **Formal insurance is** rarely available, **but**

3

informal insurance networks may be formed by family, household, and network links, which mitigate risks by frequent transfers and are supervised through trust relationships among network members. Obiora (2010) suggests a few ways in which mobile money can help spread risk. For example, networks' regional footprint may expand, while prompt money transfers may halt significant losses that could be unlikely or difficult to reverse. Smaller and more regular money transfers are possible with mobile money technologies, allowing for

more flexible handling **of negative shocks**. As a result, **informal insurance networks** could be **more**

3

competitive. As a result, more effective investment choices can be made, resulting in a better risk-reward trade-off. There could be an additional buffer against negative shocks if mobile money expands enough to enable access to micro-insurance (Mynenko, 2017). 35 Chapter 5 – Conclusions and Recommendations The most common uses of mobile money in Somalia, according to the collective findings of this reportdissertation, are purchasing top-ups and local money transfers, which are also the most common

uses of mobile money in most African countries. According to the researchers

2

, this usage has become very popular because

more people have access to cell phones than bank accounts, and money transfer can be done conveniently on their phones

2

(Aker, 2010). Furthermore, opening a bank account is time-consuming since many materials are needed, including government-issued identification cards, endorsements from previous customers, and proof of users' location. In the meanwhile, relative to keeping a mobile money account, opening a bank account is not as difficult. It's It is also likely

that people are looking for easier and faster methods of sending and receiving money. It may also be argued that

2

the extensive use of mobile money for payment purposes is due to the fact that most mobile money transactions are made from cities to rural areas, where most people do not have a bank account but do have access to a mobile phone (Ahmed, Coulibaly and Zlate, 2017). The findings of the study and responses from the study group answer the major financial frauds encountered by people of Somalia, since network interruptions, sending to the wrong number, and PIN sharing are all major causes of consumer-driven fraud, this is not a standard occurrence, according to this study. However, the 9% who exchanged their PINs did so with family and friends, as well as customer service representatives, to assist

them in transacting one or more services from their mobile currency. It can be witnessed from this that PIN sharing

2

is built on confidence, and if fraud is perpetrated by obtaining a user's PIN, the fraud must first aim to gain the user's trust, either by claiming to be a member of the service provider or a parent who is attempting to assist the user (Adelman, 2017). To answer the execution process taken by mobile payment services, the researchers believe that MNOs should warn users to check the validity of any suspected request with them before disclosing any details that could expose them to fraud. Even though customers are aware of the security steps they should take to deter fraud, the service provider has a significant role to play in protecting the mobile money service, as many people think the service's security is largely dependent on the service provider. According to the analysts, this group of consumers will seldom rarely excuse themselves if fraud occurs because they think the service provider is responsible for complete security. It was also discovered that, even though mobile money offers a variety of features, such as bill payment and airtime top-up, consumers seldom use them. This, according to the researchers, maybe due to the complexity of by means of these services. The widespread belief that there is no clear connection among mobile phone and mobile money security can be due to consumers' belief that the service provider has taken appropriate security steps to secure the mobile money service (Acemoglu, 2010). Mobile banking is revolutionising the provision of new ways for consumers to access their finances due to its ease of use and versatility. Consumers can use almost any computer with an internet connection to view and manage their accounts, which allows them to deposit checks, pay bills, move funds between accounts, and even send money to individuals or companies anywhere in the world (Mutsonziwa and Maposa, 2017). Unfortunately, this revolution in simplicity and convenience has opened new opportunities for fraudsters seeking 36

Formatted: Space Before: 0 pt Formatted: Space Before: 0 pt Formatted: Space After: 0 pt to

17

take advantage of flaws in companies and customers' accounts. When banks open more outlets through which consumers can access their money more effectively, the possibility of fraudsters exploiting those channels rises. According to a master circular issued by The Reserve Bank of India (the RBI) on "Frauds—classification and monitoring," the central bank has entrusted banks with the task of protecting and combating frauds, exposing them to a whole new set of financial risks. Furthermore, banks must now report full details on frauds and follow-up actions to the RBI. The Reserve Bank of India (The RBI) has also released operational guidance to govern this stream, recommending that suspicious transactions be reported to its financial intelligence unit. "To combat fraud, banks must implement a higher degree of scrutiny by deploying specialised tools and technology that can shield consumers from unethical cpractices (Moss, Lazonick and Weitz, 2020). Though banks are required to deter theft, Somalis should take action to defend themselves as well. Users should be particularly cautious when using banking or other applications that allow for financial transfers, according to ethical hackers. Ethical hackers are individuals who hack to test the

level of protection without any malicious intent. It is not recommended that people jailbreak their phones. The method of lifting hardware limitations and thereby making free software is known as jailbreaking. They should keep an eye on what they download and what is currently running on their phone. People will choose to avoid using their debit cards at point-of-sale terminals and only use them as ATM card for cash withdrawals (Mbiti, 2016). "Try to use credit cards at PoS so they will file a lawsuit if there is a scam because it is not their income. Keep an eye out for strange items or hidden cameras above the ATM's keyboard. To be extra cautious, people can rub off the CVV number. However, keep that in mind so that they can continue to use the pass. Anti-virus applications can be installed on servers. Passwords, PINs, and OTPs can never be shared with others, regardless of the cause. Banks never call to ask for OTP details. Do not click on links in emails that ask users to revalidate their passwords due to a device update. Do not click on unknown links or those sent by unknown numbers; instead, download applications directly from an app store (Marchionni, 2010). Since PIN sharing has been described as one of the leading causes of consumer-driven fraud, service providers can implement password age criteria that require users to update their passwords every fifth. This must be checked further by completing personal identity questions. It is also recommended that service providers increase their efforts to raise awareness of the facilities offered through the mobile money service. Mobile money consumers must also be made aware that the protection of the app is not solely the responsibility of the MNOs, but that they, too, have a role to play. Both consumers and financial institutions need realistic solutions when it comes to fraud prevention. It is critical to incorporate the fundamental tactical tactics that will provide the best defence from the start. To answer the structure of the network implemented by mobile payment services to prohibit financial fraud, this section highlights methods for detecting and preventing fraud in mobile banking (Ky, Rugemintwari and Sauviat, 2017). Authentication with several factors: Implementing a rigorous multi-factor authentication protocol during account registration is one of the easiest and most powerful steps. A successful multi-factor authentication technique that includes out-of-band authentication is a crucial first step toward mobile banking security. Consumer updates via email and text: When there has been suspicious behaviour related to their account on a mobile computer, one especially useful method for fraud prevention is to alert consumers in real-time (Hasan, 2014). When an electronic transfer is made to a new payee, for example, the bank can send a text message to the customer asking for clarification 37 that the transaction is valid. This method successful in both preventing fraud and growing consumer trust. Behaviour research and online task logging: Regular behaviour can be detected and irregularities, such as entry from international countries, can be identified by tracking the consumer's mobile account access. A successful fraud detecting strategy is the tracking of online activity, which can be done by AI fraud detection tools. New fraud prevention firms, such as Paygiant and BioCatch, are now providing Passive Biometrics to fight mobile fraud (Geoghegan, 2015). Fraud and irregular behaviour reporting across several channels: The following are essential components of a fraud monitoring solution: ? Enterprise view & Fraud Reporting is a feature that allows you to combine data from different outlets and platforms to get a complete picture of a customer's account and suspicious activities. Cheques, online account entry, and mobile transfers will also be included. FCASE connects all your financial crime, risk compliance, and customer service processes, combining warnings and incidents into a single enterprise-wide investigation portal for all of your fraud investigation and fraud compliance reporting requirements. ? Machine learning, Scores, Rules, and Warnings is a function that generates risk evaluations for a consumer account using sophisticated scoring models, customer profiling, and other fraud detection techniques. Simility and IBM Safer Payments are also very elegant account management systems (Ferguson, Jorgensen and Chen, 2020). Malware detection and removal regularly: Through tricking consumers or even bank employees into clicking on links that download malicious software onto a device, hackers have been able to steal large sums of money. This malware infects a computer, allowing a hacker to track keystrokes, display emails, record screens, and steal other sensitive information that allows them to gain access to funds. To detect and delete this malicious virus, you must have the most up-to-date protection software. Used HTTPS for encrypted access: the HTTPS protocol allows for safe internet connectivity, meaning that a person is visiting the place they believe they are. It even encrypts all data to keep it secure from prying eyes. HTTPS protects consumers from 'middle-man threats that can lead to the stealing of personal or banking information. Continual watchfulness: Cunning fraudsters prey on consumers and banks in the online mobile environment by leveraging vulnerabilities. They'll switch tactics, but there'll still be some indication that something isn't quite right with their behaviour or demands. The strongest defence against cyber fraud is vigilance, and FCASE's systematic approach to fraud prevention is one of the most effective resources a company can have (Deaton, 2010). This study took place in Somalia, and mobile money users were targeted as the sampled population. This distribution will likely change if a similar study is conducted in the future (d'Este, Draca and Fons-Rosen, 2020). It should also be remembered that the results of this study are restricted to only one country and do not reflect the views of all other mobile money service providers worldwide. Since the study did not have non-registered participants, it is possible that any of their inputs were missed, which should be considered when assessing 38 the results. The survey had a very positive response rate of 83 percent, which is an answer to the fact that the questionnaires were sent directly to service centre managers, who were tasked with ensuring that the required number of answers were collected. The service centre managers were also given adequate time (2 weeks) to conduct and return the questionnaires. Customers are flocking to service centres in greater numbers for purchases, with mobile money being one of the most common. The remaining 17 percent non-response figure, on the other hand, may be due to users who were not involved in participating in the survey. The questionnaires were sent to mobile money users in Somalia. When asked whether they have ever exchanged their mobile money PIN, there is a risk that there may be an answer stigma based on the likelihood that, for example, sharing mobile money PINs could lead to theft (Austin, 2011). As a consequence, the answer could not accurately represent the user's actual behaviour. The learner conducting the survey will have an unintentional effect on the input offered by the respondent, causing them to give feedback that they believe is correct rather than what currently occurs. It is clear from this study that some aspects of the work should have been thoroughly discussed; but, due to time constraints, this was not possible. Further research is

proposed in the following areas: ? What are the key reasons why mobile money consumers believe it is only used for mobile money transfers? ? An observational study of mobile money fraud was conducted. ? Why, if mobile money users are conscious that exchanging PINs puts them at risk, do any of them want to do so? ? Taking care of the interoperability issue with mobile currency (Aker and Mbiti, 2010). Hi Abdiaziz, I think you are nearly ready to submit – just a few more small suggestions above. Have one final check over all the details along with a thorough proof read. Also remember to remove all Track Changes and confirm the final word count following any final changes. When ready, upload the final draft (call it something like 'Abdiaziz Ahmed Siad Dissertation Final.doc') and click the box to confirm it is the version for marking. The system may also ask you to request the Turnitin Report again, which you will need to have another look at to ensure that you avoid issues with plagiarism by quoting and referencing everything properly, so leave some time for that as well (avoid uploading the final version too close to the deadline as it may take a few hours to generate the Turnitin Report). I've removed some parts of the ethics form below to reduce the match a little more. After you have done all that send me an email to confirm and I will approve it for you – the work will then proceed to marking. It was a pleasure working with you and I wish you every success for the future. Barry 22nd May 2021 39 Upload a copy when complete and I will sign it for you and you can include in the appendix also. 40