FINANCIAL EXPLOITATION OF THE ELDERLY, WHAT IS THE WAY FORWARD?

BY

RICHARD MAMBWE

Master's in Criminology, 15 Credits
Degree Project, August 2020.

Malmö University Faculty of Health and Society
205 06 Malmö.

FINANCIAL EXPLOITATION OF THE ELDERLY, WHAT IS THE WAY FORWARD?

ABSTRACT

Studies indicate that the elderly population is more susceptible to crime than other age groups as they are socially lonely and tend to stick to obvious behavioural patterns. The mental and physical limitations caused by old age further aids to a profile of a potential victim of fraud. The elderly often succumb to various types of crimes; one such crime is fraud. In Sweden elderly fraud only constitutes a minor part of all the fraud that is reported. However, statistics from the Swedish National Council for Crime Prevention indicate that cases have been on the increase since 2017. The present study seeks to explore in more detail the methods used to defraud the elderly and offer possible solutions and recommendations. The study used semi-structured interviews with participants from the Banking Sector and Swedish National Council for Crime Prevention all of whom have a nexus with elderly fraud. The findings show that there are several methods used. However, Social Engineering emerged as the most prominent. Several efforts have been put in place by relevant authorities. Nonetheless, it was suggested that more efforts be channelled into the evaluation of existing programs, conducting research on the matter and sensitising the public about the risk factors, perpetrator warning signs and how they can avoid the many different types of fraud amongst other things.

Keywords: Fraud, elderly, risk factors, victimisation, financial exploitation, crime prevention.

ACKNOWLEDGEMENT

Fulfilling this piece of work has not been an easy task, I am exceedingly thankful to the research participants that took part in the study, I am grateful to Juliana Holeksa, my supervisor for her tireless academic and professional guidance. May the Good Lord be with her always. Allow me to thank the following special people, Hanna, Gertrude, Brenda, Lars, Carolina and Nneka for moral support throughout the writing process. I am truly grateful and much love to all. Finally, I dedicate this piece of writing to my sister Clare, a person who believed in me even in difficult times. You have been with me since day one and truly showed me that success comes with hard work and determination. No words can express how grateful I am, I owe this one to you. Thank you, Clare.

TABLE OF CONTENTS

ACRONYMS

AARP	American Association of Retired Persons
NCCP	National Council for Crime Prevention
PRO	Swedish National Pensioners
SPF	The Swedish Association for Senior Citizens Seniors
SKPF	Swedish Municipal Pensioners' Association
CSEW	Crime Survey for England and Wales
SCS	The Swedish Crime Survey
RAT	Routine Activity Theory

DEFINITION OF TERMS

Elder financial exploitation: “An unjust, improper, and/or illegal use of another’s resources, property, and/or assets” (Bonnie & Wallace 200314: 38).

Elderly: Any person over the age of 65, although legal statutes for the elderly may differ across states (NCCP, 2016).

Fraud: Any deliberate misleading representation, including failure to assert information or exploitation of a position that is carried out to achieve gain, cause loss or expose anyone to the risk of loss (Bonnie & Wallace 2003).

Scam: An illegal or dishonest plan or activity, that involves tricking people for making money (Kirchheimer,2011).

Defraud: to take something illegally from a person, company, etc., or to prevent someone from having something that is legally theirs by deceiving them (MetLife,2011).

Social engineering: A manipulation method that exploits human psychology leading victims into making security errors or giving away private information or valuables (Fatima & Naima,2019).

Phishing: A fraud that involves searching for bank-related information that is then used for criminal purposes (Kirchheimer,2011).

Vishing: A process that involves a fraudster contacting a victim on the phone and purports to be someone else, such as an employee from the bank, a doctor, or the police (Consumers International, 2019).

Smishing: A process someone receives fake SMS with links to pages where they are asked to enter personal codes such as passwords or credit card numbers (Consumers International,2019).

Ponzi schemes: A deceptive investing cheat promising high-level returns with little risk to investors. The Ponzi system produces returns for first investors by securing new investors (Cohen,2008).

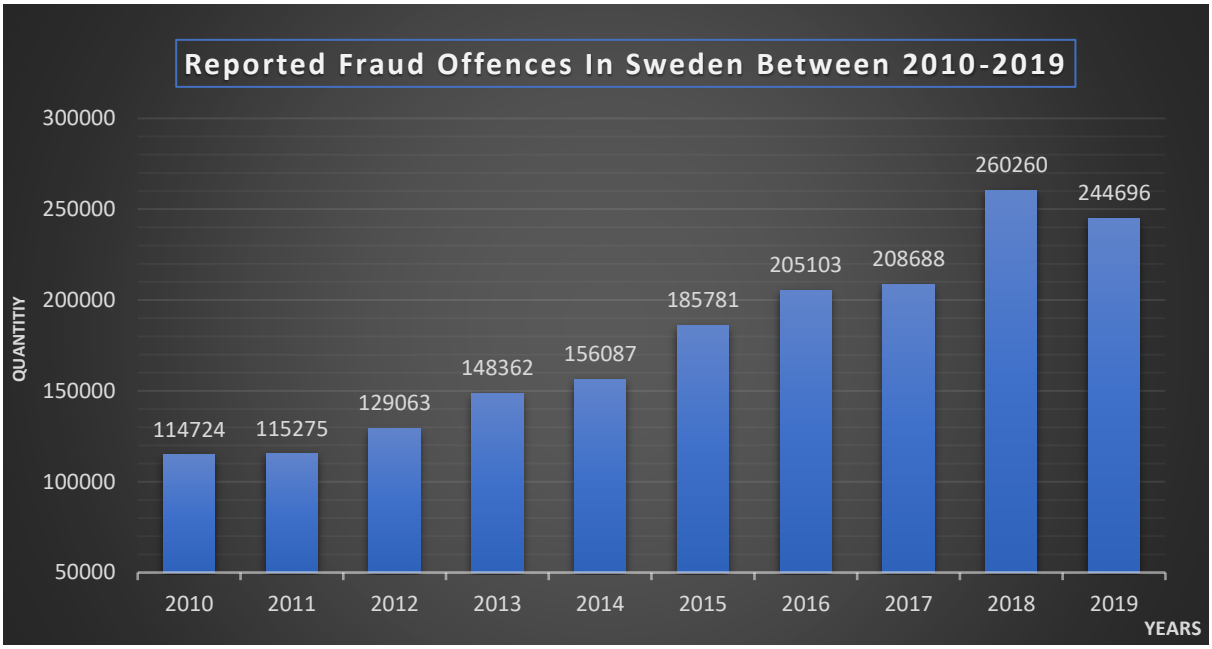
CHAPTER ONE

1.0 Introduction

The rising prevalence of fraud on the elderly is leaving many seniors in peril, threatening to deprive them of their resources, their autonomy and trust. Elderly fraud is a substantial problem and is anticipated to become worse with the ageing of the overall population (Burnes et al 2017). As the world becomes more innovative and technologically advanced, so are criminals equally devising new means and techniques to perfect their criminality. It is, therefore, paramount to understand the various methods criminals use and offer suitable measures to avert the problem. Financial victimization on the elderly include crimes such as scams and fraud. Examples include identity fraud, investment fraud and mass marketing scams among others (Bonnie & Wallace 2003). Although people of all ages can be victims of fraud regardless of their cognitive status. Research indicates that the elderly population are the most vulnerable and ideal victims globally (Holtfreter et al, 2014; Christie 1986). The elderly citizens are disproportionately targeted by fraud attempts and fraud happens to be the most momentous and recurrent form of crime that the elderly are subjected to (Jackson & Hafemeister 2013).

For instance, conservative estimates suggest that the annual financial loss by elderly fraud victims is at least $2.9 billion in the United States alone (MetLife, 2011). Anderson, (2013) further claims that, on average, 9.1% of the population aged over 55 become victims of consumer fraud every year. Similarly, it is estimated that 4.0% of the people aged 75 + fell victims to fraud, based on the (CSEW) data (Office for National Statistics, 2016). Another meta-analysis study revealed that overall elderly fraud prevalence was 5.6% among community residence (Burnes et al., 2017). A study of fraud between age groups of (16-84) conducted by Swedish Crime Survey (SCS) in 2018 indicates that the elderly above 65 years were more exposed to card/credit fraud with a rate of (7.4%). 20-64 years represented 7.0% while the least exposed was the youngest age group (16-19) years representing 2.6 %. The report points out that vulnerability has increased especially in the oldest age group since 2017 (NCCP 2019). This provides some sobering indication of the potential scope of the problem that calls for distinct measures that will constantly protect the elderly based on the methods used to defraud them. Although elderly fraud only constitutes a minor part of all

the fraud that is reported in Sweden, fraud is a significant problem in Sweden as can be seen from the figure below of reported fraud over the last 9 years (2010-2019).



Source: NCCP 2020

Figure 1 shows that during the past nine years, the development of the reported fraud crimes has been steadily rising overall. The development of fraud offences is partly due to increased use of the internet in society and technological development contributes to the growth of new methods and opportunities to commit fraud offences (NCCP, 2019).

1.1 Aim

The study's overall aim is to explore what methods are used to defraud the elderly and provide some applicable solutions.

1.2 Research questions

What are the risk factors of elderly fraud?

What methods are used to defraud the elderly?

What measures have been put in place to combat fraud on the elderly?

CHAPTER TWO

2.0 Literature Review

In this section, the research explores information relevant to elderly fraud. The literature review covered the following aspects and theories about fraud/financial exploitation of the elderly.

- Risk Factors
- Routine Activity Theory
- Methods used by fraudsters

The first step involved in understanding and intervening against elderly fraud is determining its prevalence and incidence. However, accurate estimates regarding the prevalence and incidence of elderly fraud will likely remain unknown as many elderly citizens are unaware of or unwilling to report fraud (Pak & Shadel, 2011). This is because most elderly victims of fraud are unwilling to report their experience of victimization to relevant authorities (Titus et al., 1995; Van Wyk & Mason, 2001). For example, the study by the American Association of Retired Persons (AARP) (2003) revealed that no more than 27% of known fraud victims admitted their victimization. Furthermore, the difference between various forms of fraud may also be a factor to the underreporting aspect, since fraud is not a single concept but, rather, comprises a broad scale of unique crimes (Fischer, & Evans, 2009; Titus et al., 1995).

For instance, the meta-analysis study conducted by (Burnes et al., 2017) confirmed that the varieties of fraud considered in scientific studies varied from 3 to 22. Equally, there was considerable variability in incidence, risk factors and victim characteristics recognised throughout the studies. Nonetheless, it is still imperative to grasp why the elderly are usually victims of financial fraud. Many scholars have been working towards identifying individual and demographic risk factors for fraud among the elderly to precisely pinpoint those who are at greater risk. To this effect, numerous major risks have been found to cause fraud susceptibility among the elderly, such as an overly trusting nature, psychological vulnerability, social isolation and risk-taking. These risk factors may lead the elderly to be more defenceless to fraud via the manipulation of their decision-making. These aspects are highlighted in greater detail in the proceeding text.

2.1 Risk Factors

a) Overly trusting nature

An overly trusting nature has been considered as a crucial factor in the elderly's weakness to fraud. Encouraging the elderly's loyalty, affection, and trust as a key method to hook them into scams and financial exploitation. Many reports have indicated that elderly citizens are commonly more gullible than their younger colleagues and give primacy to emotionally profound goals (Kirchheimer, 2011; Li & Fung, 2012). This predisposition for the elderly to overly trust others, particularly strangers, may also make them susceptible to falling victim to fraud (Castle et al., 2012; Greenspan et al., 2001).

Furthermore, the elderly's elevated amounts of trust for strangers may indicate tangible changes in their brain circuitry. Castle et al. (2012) assessed the neural foundation of trust and noticed an indication for age-related variations in the anterior insula. The elderly demonstrated subdued activation of the anterior insula to unfamiliar faces, while the younger counterparts did not show such a weakened response. The findings imply that variations in neural circuitry may contribute to the elderly's vulnerability to fraud (ibid.)

b) Psychological vulnerability

Elderly citizens with social isolation, negative life events, low social needs fulfilment or depression display a great psychological need to connect or get on with others including outsiders which leaves them vulnerable to be pursued by con artists (Olivier, & Brown, 2015). For instance, Lichtenberg et al. (2016) observed that psychological susceptibility which they described as a blend of poor fulfilment of social needs and depression can longitudinally envisage new incidents of fraud with highly vulnerable people showing a dual probability of being defrauded. A comparable study by Lichtenberg et al. (2013) also discovered that the elderly with psychological susceptibility were roughly three times as prone to be victims of fraud, thus underscoring the significance of considering the psychological weakness in establishing vulnerability to fraud.

c) Social isolation

Social isolation is usually seen as a risk factor of fraud among the elderly, this is so because secluded elderly people may engage criminals in a misguided endeavour to develop social connections (Lachs & Han, 2015). Research indicates that the elderly who experience social seclusion are more projected to fall victim to telemarketing fraud (Consumer Fraud Research,

2006), and loneliness is a key risk factor for fraud, especially among the elderly (Alves & Wilson, 2008). Fraudsters may display untruthful concern for the lonely elderly and establish "bonds" with them via the telephone to win their confidence and later lure them into the fraud setup.

The elderly citizens are considered ideal targets for "fraudsters," as a large proportion of them live alone in the wake of the demise of a spouse and the subsequent seclusion may make them more eager to interact with strangers, as well as motivated culprits who are attempting to fulfil their social needs (Cohen, 2008). Apart from that, the elderly who live solo are more easily pursued by fraudsters because they habitually do not get effective care and guidance from family members (Ibid.)

d) Risk-taking

The financial risk-taking actions may enhance the probability of fraud victimization among the elderly, as victims of fraud are highly prone to be risk-takers (Consumer Fraud Research, 2006; Pak & Shadel, 2007). Interestingly also, victims of telemarketing fraud have been found to show comparable investment conduct as that of bettors, such that they are more prone to rely on the stroke of luck when making investments and invest a lot of money with an expectation of recouping any losses (Gross, 1999). There is increasing indication that the elderly display diminished negative awakening to expected loss (Samanez-Larkin et al., 2007), therefore, they may engage in perilous financial decision making and subsequently make more poor choices (Denburg et al., 2007). Consequently, these age-associated changes may raise the probability of elderly fraud due to declines in anticipated damages or losses.

2.2 Research paradigms on elderly fraud

Existing research regarding fraud victimization among the elderly has focused on a variety of susceptibility factors; however, theories that provide causal explanations regarding the high prevalence of elderly fraud are quite rare (Jackson & Hafemeister, 2013; DeLiema, & Conrad, 2017; Goergen & Beaulieu 2010). However, in this document, we are going to focus on the routine activity theory to better understand financial fraud among the elderly.

Routine Activity Theory

Routine activity theory (RAT) centres attention on offenders and the responsibility of capable guardians that offer protection. (RAT) is one of the prominent cited theories in the field of

criminology (DeLiema & Conrad, 2017). In contrast to models of criminality which focus on the character of the criminal and the social, biological and psychological factors that may cause the criminal act, the attention of RAT is the inquiry of crime as an event, stressing its nexus to time and space and underscoring its ecological nature and the inferences thereof (Ibid.) The principle behind RAT is that criminal acts necessitate the merging of three elements: (1) a motivated offender, (2) a suitable target, and (3) the absence of capable guardians. The theory centres on how particular behavioural arrangements and the crossroads of people in space and time create prospects for a crime (Cohen & Felson 1978).

To this effect, the first crucial element of RAT is the existence of a motivated offender. A motivated offender is merely anyone with the aspiration and capability to carry out a crime. Coleman (1987) suggests that generally, offenders are influenced by a desire for financial gain. RAT contends that people are sensible or reasonable and will be drawn by any prospects for gain and dissuaded from taking these opportunities by any direct obstacles or risks. Implying that, anybody can be a possible contender of a criminal act.

The second element of the RAT is the existence of a suitable target. For example, Criminals target the elderly for reasons such as their retirement benefits which make them ideal targets as well as the perception that they are more susceptible to being conned. In short, they are considered easier targets and offenders equally have faith that elderly victims will not detect and report the crime to law enforcement. Furthermore, there is a perceived small risk of detection by would-be offenders (Goergen & Beaulieu, 2010).

The third and final component the absence of capable guardians concedes that the act of committing fraud on the elderly is dependent on the prospect to do so. As the elderly become gradually more defenceless with age, compassionate friends, family, as well as institutions, may step in to avert fraud. A big social network i.e. more ears and eyes, dependable family members, legal documents and financial professionals that safeguard assets are all considerations that play as capable guardians defending against fraud (Goergen & Beaulieu, 2010).

2.3 Current identified methods used by fraudsters

Social media

Social media presents many opportunities for fraudsters. While a majority of the elderly hardly use social media, 3 billion people that is about 40% of the universal population are active users of social media, such as Instagram, Twitter WhatsApp and Facebook among others with an estimated million new users each day (Consumers International, 2019). The magnitude of use as well as the open disposition of social media daises makes it possible for offenders to reach extremely huge numbers of people with ease including the minority elderly. It facilitates 'social engineering' of scams, providing offenders access to enormous quantities of personal information, which subsequently is utilised to target demographic groups and customise scams to make them more compelling. For instance, applying an individual's real name, or referring to their friends, recent holiday, hometown, and hobbies.

Fischer & Evans (2013) note that social media offers fraudsters the capability to hide their genuine motives and identities behind the inconspicuous bogus accounts and profiles, which they use to deceive consumers, masquerade as reliable sources and give offers that are too good to be true. These tricks can be challenging to identify as they seem to come from credible sources such as reputable online community or very well-known brands. Furthermore, fraud can propagate with startling speed across social media, as retweets and shares transmit content to a large range of people. Consequently, the social media model permits fraudsters to lay back and allow consumers unwittingly, perform much of the hard work (Lachs & Han, 2015). Approaches to fraud can vary, for instance, Consumers International, (2019) observes that most scams fall into three broad categories that are:

I. E-commerce scam

Fraudsters alleging to be legitimate online sellers on platforms such as Facebook Marketplace. Consumers pay for commodities, which then turn out to be fake for example, fake clothing or substandard. In some other cases, merchandise never arrives.

II. Investment scam

Fraudsters make public a 'too good to be true' investment prospect, every so often using news tales and commercials that seem to be from legitimate sources. Consumers who are enticed to invest lose part and in worst cases all their life savings.

III. Impostor scam

Fraudsters pose as original brands, genuine family or friends to obtain a consumer's trust asking them to buy commodities or click on links which transfer malware/viruses on their personal computer. It is paramount to note that methods used for fraud extend beyond social media and they are not exclusive to the elderly, but the prospect and bearing on the elderly can be superior to the average person considering that some elderly citizens lose their life savings/pension which in reality are not able to retain back. Some of the most common methods include:

a) Advance Fee Fraud or "419" Fraud

Named after the Nigerian Criminal Code, this fraud is a prevalent offence with West African organised criminal groups. There is a multitude of schemes and scam telephone, email, ordinary mail, and fax promises that are devised to induce victims to send finances for a variety of reasons. Victims are told they will be given a proportion for their support. There are many variants of 419 schemes, but they all have a similar goal: to rob the victims' cash or personal information (Fischer et al 2013).

b) Identity Theft

Using the victim's personal information including, but not limited to, account login credentials, account information, social security number, date of birth, name, driver's license, and address, among others. A criminal can take over a credit or other monetary accounts in the victim's name. Fraudsters collect the victim's data through different means; however, The elderly are often susceptible to social engineering techniques that fraudsters utilise, such as "phishing" to lure victims to supply personal data such as passwords, login IDs, account numbers, and other verifiable data that can then be used for fraudulent motives (Holtfreter et al 2014).

a) Misappropriation of Income or Assets

An offender attains access to an elderly's ATM cards, savings account, social security or pension payments or withholds part of cheques cashed for oneself (Alves & Wilson, 2008).

b) Pigeon Drop

Victims are approached by typical strangers alleging to have discovered a substantial sum of money and offers to split it with the victims. Though, the fraudsters ask for "good faith" money and propose to escort the victims to the bank to withdraw the cash. In return, the victims are offered

a bag or an envelope that only contains blank pieces of paper rather than money there were promised (Cohen, 2008).

c) Sweetheart/Romance scam

The offender enters the victim's life as a love interest to secure influence and subsequent monetary control. This kind of fraud every so often goes undocumented owing to the humiliation and emotional bearing on the victim. In some cases, the victims are aware that they are being swindled but they merely do not want to be lonely (Deevy & Beals 2013).

d) Telemarketing or Charity Scam

With this one, the victims are persuaded to purchase worthless or non-existent merchandise, contribute to a fake charity, or finance a fictional enterprise. The elderly are especially at risk to this type of fraud owing to that they are usually at home during the day to answer the telephone. Due to the social seclusion, fraudsters prey on isolated elderly eager for someone they can interact with. Fraudsters perform this by inventing schemes that necessitate numerous phone calls and the advancement of a gullible relationship (Cohen, 2008).

CHAPTER THREE

3.0 Methodology

This chapter explains in detail the methods that were used in the data collection process, the type of data collected, sample and sampling methods and it further justifies and motivates the choices made for the specific methods in the research. The study employed a qualitative method as it was thought to be the most suitable approach to address the research question and objectives. Liamputtong & Ezzy (2005) observe that qualitative methods are most appropriate in investigating susceptible populations, the elderly are among the most vulnerable populations. While the study did not deal with the primary victims of elderly fraud, this method proved ideal for uncovering, methods used by fraudsters, risk factors and measures put in place.

3.1 *Why the qualitative approach?*

The approach is fluid and enables the researcher to be flexible thus, in this case, ideal for grasping the interpretations, meanings, and experiences of the respondents in their professional line of work towards preventing fraud. The in-depth nature of this method enables the participants to voice out their experiences and feelings in their own words (Gregory & McKie,1996). The objective of the qualitative methodology is to produce in-depth and illustrative information to understand the various dimensions of the problem under analysis, hence is ideal for answering our research questions of the study.

Druckman (2005) further notes that qualitative research works with the creation of meanings, motives, aspirations, beliefs, values and attitudes, which corresponds to a deeper space of relationships, processes and phenomena that cannot be reduced to the operationalization of variables. This method also helped me get a profound and better understanding of the informant's experiences and opinions regarding the methods used to commit fraud against the elderly. Denscombe (2007) further suggests that a researcher is likely to gain important understanding from the extensive data obtained and knowledge from key participants.

3.2 Sampling and sampling techniques

The sample consisted of 4 respondents and since I only conducted interviews with 4 individuals over the phone, it was rather difficult to come up with a sampling frame. Participants were interviewed within four weeks. Two of the sample were contacted through a snowball sampling

technique as one of the participants was already my contact. Snowball sampling is an efficient method for coming up with a reasonable size sample (Denscombe, 2007). The method makes it easy to engage with a new participant, having been in a sense backed by the person who had mentioned him or her Liamputtong & Ezzy (2005). In this study, I used the proposer as a reference to boost my legitimacy and credibility other than engaging a whole new person. As in this case, Denscombe (2007) suggests that snowball sampling is convenient where there is no sampling frame of any sort, which in turn, can enable the investigator to make contact and identify participants necessary for the study.

3.3 Data collection

The data collection instrument comprised of an interview guide with semi-structured questions. All the interviews were conducted over the phone. This all together took approximately 6 weeks.

3.4 The Interview process

The interviews started with a conversation of about 2-4 minutes where I asked the participant's role and background. I also reassured them of confidentiality regarding my study explaining again to each respondent that the study was only meant for academic purposes. This was performed to motivate them to speak as freely as possible. The interviews were also conducted with a few follow-up questions where necessary. All the interviews were conducted in English, and on average each interview lasted about 30 minutes, ranging between 25 and 40 minutes.

3.5 Transcribing Interviews and Data Analysis

Bryman, (2016) notes that often, a word recognition software or transcription machine is utilised to transcribe interviews. In this study, transcription of the interviews was done by Otter, a voice transcription app, the transcripts were checked thoroughly for accuracy, this was to ensure that no significant data was missing. The analysis section employed thematic coding and analysis. Thematic analysis is a method for analysing, identifying, and narrating patterns or themes within data. It minimally describes and organises information set in detail (ibid.) The data was refined into themes and concepts, and these themes were therefore coded to facilitate easy retrieval of what the participants had to say about financial fraud of the elderly. This approach enabled me to consolidate and assess the information with the help of conceptual and theoretical frameworks outlined in the literature review.

3.6 Ethical Considerations

The study considered that it essential that ethical considerations are observed and maintained throughout the research process. For instance, participants responded based on informed consent and priority was given to the dignity and respect of participants ensuring that use of discriminatory tones or language is avoided by all means especially with regards to the formulation of interview questions. Thirdly, no personal information about the victims was disclosed during the interviews. The study further ensured that data analysis and questions in the interview guide were structured in a way that would not identify elderly victims of fraud.

3.7 Limitation of the Study

The author would have preferred to interview more people from different institutions such as the law enforcement that directly work with and investigate fraud, but due to the limited time, resources and the COVID-19 situation, the study was restricted to 4 people. Furthermore, interviewing more people from different institutions would have added more value to the study by virtue of having a rich variety of information regarding the topic in question. Another factor worth mentioning is the method used, qualitative analysis findings cannot be generalised to broader contexts with the same degree of certitude compared to quantitative analyses. Bryman (2016) notes that this is mainly due to findings not being tested to determine whether they are statistically significant or achieved by chance.

CHAPTER FOUR

4.0 Findings

4.1Introduction:

In this chapter, I present the research findings I obtained from all my data sources as well as discuss the findings. I attempt to discuss them in detail borrowing ideas from the literature review presented in Chapter two. This chapter will also endeavour to answer my research questions in the discussion section and thereafter, conclude with reflections and recommendations.

I interviewed three representatives from the Banking Sector and one from the Swedish National Council for Crime Prevention and their responses gave me valuable insight regarding fraud against the elderly which was used to answer my research questions.

To present and discuss the findings coherently and logically, I used the initials (P1-P4) to represent the participant's views and I further used themes which were reoccurring when I transcribed the interviews and made them as subheadings to help structure the chapter. Henceforth, the chapter is tied on the following main themes: Means, technology vulnerability, strategies, initiatives and opportunities. The chapter seeks to answer the following research questions:

- What are the risk factors of elderly fraud?
- What methods are used to defraud the elderly?
- What measures have been put in place to combat fraud on the elderly?

4.2 Means

They are various approaches fraudsters use to deceive their victims. As the world advances in technological developments, fraudsters equally continue inventing new methods to exploit their victims. With the element of time, certain methods become rare while others become more prominent. Based on data from the interview guide, it was observed that they were three major methods fraudsters were using to exploit their victims, in order of prominence, these include Social Engineering, Investment Fraud, and Romance Fraud. According to the research participants, social engineering is the most popular method criminals are using now. Participants noted that there has been an increase of social engineering crimes in the last three years and they further predicted that cases are likely to increase because of its complexity and the many ways it manifests. These

include Phishing, Vishing and Smishing. Because of the many ways of manifestation, how social engineering occurs also varies, the participants provided a few examples.

> *In some cases, the fraudsters pretend to be the elderly person's doctor, offering a new and better medicine which usually is extremely expensive and does not even exist.* (P1)

> *Another way is that someone calls and pretends to be from a bank or a credit institution to gain access to card numbers and codes. Real banks and credit institutions never call their customers and ask for codes and account numbers.* (P3)

> *Another method is the so-called grandchild scam, where the caller induces the elderly person to believe that they are relatives, therefore, is tricked into making a financial contribution because they believe there is an emergency.* (P1)

On the other hand, investment fraud is another prevalent method the participants pointed out. It is a deceptive practice in the stock or commodity markets that induces investors to make purchase or sale decisions based on false information, often resulting in losses. Investment fraud may involve the victim being directed to register on a website to take advantage of an offer advertised on social media or the internet in general (Consumer Fraud Research, 2006).

> *It often starts with an English-speaking broker or adviser calling the intended crime victim's home. S/he offers the person to invest in some kind, such as buying shares. The advisor often refers to web pages and calculation models that look serious but contain incorrect information. The victim is misled to deposit money into the fraudster's account.* (P4)

4.3 Technology

Fraudsters use the internet and sometimes the phone to offer victims the opportunity to invest in very lucrative deals claiming they are from highly reputable companies or sellers yet it is false information as there only intend to swindle the victim's hard-earned resources (Finke et al,2016).

> *In recent months, it is often about bitcoin investments that are marketed with the help of reputable institutions. Often the deal is very urgent, and victims are advised to seize the opportunity before the offer ends.* (P2)

Love/Romance is another type of fraud that was mentioned by the research participants. Love or Romance fraud usually targets single elderly women who are either divorced or widowed. The conversations usually start online on platforms such as Facebook or dating sites. In many cases, the impostor is a military personnel on a mission or assignment abroad. The victim and fraudster start chatting, exchanging emails, and talking on the phone. Without delay, the impostor announces his love and talks about a future together with the victim. This contact can often last for months and after a while, the impostor begins to demand money under various pretexts, such as hospital costs, accidents, and travel.

> *Due to the affection and emotional attachment that is created between the victim and perpetrator, romance fraud is among the most devastating. Because of this, many victims do not report the crime, estimates of this crime are often not accurate due to low levels of reporting by victims.* (P2)

> *It is difficult to intervene because most victims do not believe it is fraud even when it is evident. We have had situations where some victim chooses to lie to us saying they have met the person physically and it is just a normal transaction like any other, yet it is not true.* (P4)

4.4 Vulnerability

The ageing development can bring about physical and rational changes that increase the perils of elderly fraud. An elderly person with a cognitive deficiency may not possess the information managing proficiencies essential to detect deception. Furthermore, factors such as retirement funds, availability at home and isolation all contribute to elderly fraud as pointed out by the respondents.

> *Ageing itself may bring about problems related to mental deficiencies, physical health, and dependency on others, all of these are factors associated with elderly fraud* as observed by (P3).

> *The fortune that elderly citizens have amassed throughout life makes them ideal targets for fraud. Money is the most notable reasons for elderly fraud.* (P1)

> *The elderly people are targeted because they are at home for the calls, less mobile and retired. Criminals can find victims simply by calling or dropping by.* (P3)

> *Isolation is another factor, due to this seclusion, the elderly usually lack people to help them evaluate critical decisions.* (P1)

4.5 Strategies

The banks have put in place systems that monitor all transactions. The role of these systems is to detect non-conventional and suspicious behaviours. The banks are responsible for detecting and preventing suspected money laundering and reporting these to the Financial Police. It is the police who then investigate whether any crime has been committed.

> *These are technologies I cannot discuss in detail but for example, the bank has established the Anti-Financial Crime Unit (AFC), which works to combat money laundering, terrorist financing and fraud. If the system detects signals about possible fraud, the personnel perform a thorough analysis of the possible crim*e. (P4)

In August 2017, some new guidelines on measures against terrorist financing and money laundering came into effect. Among other things, the law compels insurance companies, banks, and financial institution to perform:

> *Risk assessment, that is assessing the risk of using the products and services they offer against money laundering or terrorist financing.* (P2)

> *Training, that is training all employees with sufficient knowledge on how to follow guidelines and procedures of anti-money laundering.* (P1)

4.6 Initiatives

Also, the national fraud centre was established so that the Swedish police can work more efficiently. The purpose of the centre is to work with fraud coordination and preventive measures

with a primary focus on reducing crime and increasing prosecution. The police also cooperate with other authorities and the business communities to minimise the number of fraud offences.

> *The idea is that the police coordinates their resources as well as detecting the fraud that is related, this can be identity theft, invoice scams, skimming or any related fraudulent crimes. (P4)*

Do not try to fool me is another measure put in place, it is simply an information package launched to strengthen the elderly's ability to defend against fraud. Don't try to fool me is a meeting package developed by the police together with the Crime Victim Journals, Swedish National Pensioners' (PRO), The Swedish Association for Senior Citizens Seniors (SPF)and the Swedish Municipal Pensioners' Association (SKPF).

> *The purpose is to raise awareness of fraud offences where primarily the elderly are affected, what warning signals and situations to be aware of and how to protect themselves from being deceived. (P4)*

Another similar initiative is the *"Bag"* a film which was produced in 2010 in the city of Gothenburg. It included a study circle material for the elderly focusing mainly on vulnerability, security and health. It was made possible by a consortium of actors including the police and other pensioner's associations. However, this type of measure has limitations as discussed by (P4).

> *Scams constantly vary in approach as criminals develop new techniques to exploit people over time. Hence, it is significant that we develop interventions that match the crimes constantly.*

4.7 Opportunities

Banks have a critical role to play in helping clients avert fraud. They can warn and educate not only the elderly but all clients at large. They are in a better position to question and spot irregular payments thus denying criminals access to bank accounts and overall extend assistance to clients who become victims. Also, the local police forces and other law enforcement agencies have a vital role in safeguarding and assisting people in susceptible situations. A question on what should be done, respondents had this to say.

> *Early financial planning can be used to limit opportunities for fraud, For instance, educational outreach materials can be used as dialogue to help*

> *the elderly think about whom and when they should assign a legal representative should they be in a position not to make financial decisions themselves.* (P2)

Emphasis was also placed on the decentralisation of prevention efforts to include other actors in the fight against fraud. Participants felt that this would spread the message faster and it would be a holistic process by involving everyone in communities.

> *The efforts to prevent elderly fraud should move beyond frontline staff. For example, they can be community outreach events to educate the elderly and their family caregivers about fraud. These can be held in communes, churches, and local businesses.* (P1)

Also, the research participants further highlighted the significance of evaluation, conducting research and collaborating with the media houses in the fight against fraud.

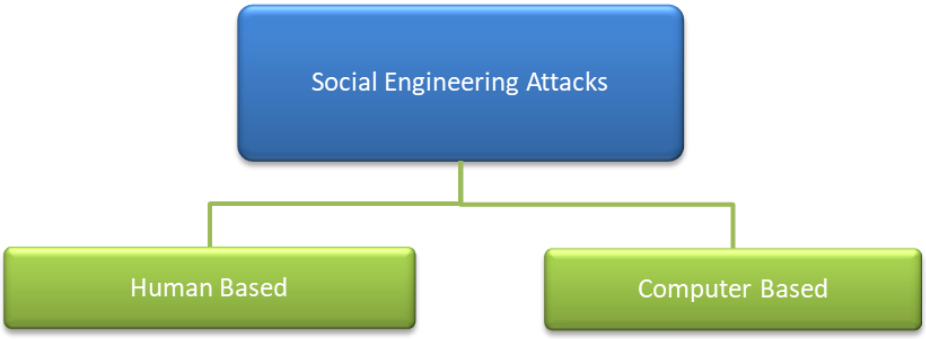
> *It is essential to evaluate the efficiency of existing training and prevention programs of fraud to ascertain whether they increase detection and reporting of fraud. We need mechanisms that will highlight the overall value of resources that have been recovered or protected employing various prevention approaches.* (P1)

> *I think it would be a good thing if we can conduct research on these aspects so we can learn more and perhaps target certain audiences better. Also, banks should turn to research before investing resources and time on possible unsuccessful programs.* (P3)

> *We can also partner with the media houses to convey messages about the existing fraud methods to the public. The messages via media such as TV or Radio can help reach a huge number of people, across various demographic settings.* (P4)

5.0 Discussion

When it comes to social engineering, different motives drive criminals to create such an attack. For instance, glutton, financial gain, or economic profit. To carry out social engineering attacks, one must know the psychological principles and underlying human traits that can be utilised in exploiting their targets. The research participants indicated that social engineering attacks can be categorized into two groups: i.e. computer-based or human-based as depicted in the figure below.



In human-based, the criminal carries out the offence in person by interacting with the victim to collect required data. Hence, they can only exploit a small number of people. The computer-based, on the other hand, uses software to obtain info from the victims. Therefore, a criminal can strike down numerous victims in just a few seconds. For example, social engineering toolkit (SET) is known as one of the computer-based methods utilised in spear-phishing emails (Salahdine & Kaabouch 2019).

Furthermore, participants indicated that fraudsters find social engineering an extremely effective method in obtaining material from innocent victims and applying it for illegal purposes, all under the radar of the victims. The more gullible the victims are, the simpler it is to lure and extract data from them. It is the very reason why more elderly people fall for social engineering fraud, particularly with their banking operations. Criminals view the elderly population as profitable targets, as initiating a call to their telephones can make them reveal their banking data. Consequently, social engineering incidents continue to rise, necessitating banks to discover ways to defend mobile and online banking against the ever-changing trojan or individuals in the browser attacks. One of the research participants indicated that an increasing number of European banks

are preventing social engineering attacks using One Span's Cronto mechanism. Provided either through a mobile app or via hardware, Cronto aids banks avoid social engineering attacks employing a patented graphical transaction login mechanism that encodes the details of the transaction and precludes the transaction from being altered by fraudsters. Cronto enhances the transaction signing and bank's login experience, enabling clients to easily scan and enter an eight-digit code to authorise a transaction.

On the other hand, investment fraud is another problem that the participants highlighted, it is equally complex as it manifests in different settings. As the research participants pointed out, it has been more about bitcoin more recently, many elderly victims are enticed to invest into cryptocurrencies by fraudsters deeming it is as the newest way to get rich instantly. Many of these crypto investor victims are promised massive disbursements from venturing in cryptocurrencies alongside enjoying the benefits of having investment in a decentralised exchange. While this sounds like an exciting prospect, there is a dark side to this nascent cryptocurrency market. Fraudsters have progressed with the times, discovering new techniques to defraud inconspicuous crypto investors every day. For instance, they have discovered ways to carry out Ponzi schemes, make fake initial coin offerings as well as devise various schemes to embezzle investor's cryptocurrencies. It is projected that as the popularity of cryptocurrencies comes to light, many people will continue to lose funds to these frauds (Olivier et al,2015).

Another dimension of investment fraud is when a fraudster alleging to be a stockbroker calls and offers some investments advice. The person will claim to be offering a low-risk investment that will provide you with quick high returns and encourages you to seize the opportunity while it lasts. The offer often seems genuine as it is supplemented by manipulated data to back up the fraudster's claims. Kirchheimer (2011) observes that the investments proposed is usually foreign currency trading share, real estate high-return schemes or mortgages. This is all false information as victims end up losing most if not all their resources as the swindler is often from overseas and with no financial services licence.

Let us further consider love or romance fraud as another aspect brought forward by the research participants, this form of fraud is not necessarily a new trend, it became more apparent in the year 2008 (Whitty & Buchanan 2012). One of the participants indicated that the secrecy of the internet means that the victims cannot know the real gender, employment, marital status, age, or name of

the correspondent. A correspondent is often a fictitious person created only to entice the victims into sending cash. The fraudsters create both male and female characters to lure same-sex victims as well as those of the opposite sex. Whitty & Buchanan (2012) predict that romance fraud will likely increase as social media platforms are on the increase, particularly online dating sites. It is plausible to think that they will be more cases as long as there are gullible victims who are oblivious to the fraud. Due to the hefty sums incurred, the victims are unwilling to report due to being emotionally devastated. The embarrassment that this brings is difficult to comprehend by many victims. However, more research is essential to understand the psychological impact on victims. The prevalence rates are likely higher than estimates due to the underreporting of the crime to law enforcement across the globe. This discrepancy suggests that efforts to ensure such crimes are reported must be prioritised to facilitate easier ways for victims to report this form of fraud.

The study further brought to light some aspects that make the elderly vulnerable such as age-related dementia, isolation, retirement and less mobility (at home for calls) and lack of credible people to help them to review large decisions. It is fair to state that from the above-highlighted risk factors to take effect, there is a convergence of at least three elements i.e. a motivated offender, a suitable target and lack of a capable guardian as discussed earlier in the RAT. Interestingly, we may also argue that the lifestyle of the elderly unwilling puts them into harm's way, more so if we consider applying the lifestyle theory. Coined by Hindelang, Garofalo and Gottfredson (1978) Lifestyle theory is one of the primary systematic philosophies of criminal victimization. Initially proposed to account for differences in the risks of violent oppression across social groups, but has been extended to encompass property crimes, the basic premise is that demographic differences in the likelihood of victimization are credited to different individual lifestyle of victims. From this viewpoint, an individual's lifestyle is the crucial factor that decides risks of criminal victimization, for instance, fraud in this case.

Lifestyle is defined in terms of "routine daily activities, both vocational activities (work, school, and leisure activities" (Hindelang, Gottfredson, and Garofalo 1978: 241). In simpler terms, the elderly's day-to-day activities may naturally bring them into contact with crime or raise the risk of being defrauded. Lifestyle stands as the cornerstone of the theory of individual victimization as it

is the patterned routines of an individual's normal activities that predict or envisage the risks of exposure to criminogenic situations.

Due to the steady surge in fraud cases, many institutions are investing in systems to improve and detect customer susceptibility before they lose funds and are also developing procedures to counter swiftly and effectively. These systems facilitate in safeguarding client assets, restoring trust in institutions, and strengthening brand value (Gunther, 2016). Most Swedish banks provide user-friendly and secure solutions for all their services. As observed from the findings, they are constantly upgrading and developing their security solutions to ensure that the systems have good information security. For instance, when you use the internet and mobile banking, the information transfer between the bank's system and your device is encrypted.

Additionally, it is evident that there are strides to improve customer awareness of fraud specifically when an individual becomes a customer and most notably almost all banks have a section that educates the masses about fraud and how to protect yourself from such vices. But the question perhaps should be how many people do take time to read about fraud or security measures provided by the respective banks? More especially the elderly citizens where a significant number may not be as computer literate as the younger generation. It is possibly very few, one reason could be that information regarding fraud is quite hidden and most banks have a lot of other information they consider paramount appearing as the first things that people who visit the website see. Let us also consider some of the requirements on the Money Laundering and Terrorist Financing Prevention Act that of 2017. Is the Act enough to combat or prevent elderly fraud? It seems plausible to say yes, for instance, if we consider risk assessment, a bank performs a general risk assessment taking into account among other things the following factors; type of products and services offered to customers, distribution channels and geographic risk factors.

However, more can still be done especially with fraud that involves home visits or the type which defrauds the victims gradually. It is imperative to understand that not all fraud cases entice the victims to make large withdraws. Some tend to happen very gradually and because of this, transactions may appear legitimate enough not to be detected by the monitoring systems established by respective banks. This can go on for a very long time and inevitably the victim loses out a lot of money in the long term before it comes to light. Financial institutions are well-placed to recognize the trademarks of fraud which include unusual withdrawals, forged signatures on

financial documents, unexplained asset transfers, abrupt changes in powers of attorney, and strangers taking over financial affairs of a particular client (Deevy & Beals,2013). It is fair to state that these institutions help in preventing fraud via different security measures. However, most solutions to tackle fraud are taught in corporate defence training programs.

Unfortunately, the victims we are referring to here are primarily retired and do not have access to such defensive training. Hence, the onus falls on the financial institutions, law enforcement and all those that are security inclined and cognizant of these crimes to assume responsibility in advising or sensitising potential victims on how to defend themselves. As an example, a mitigation approach can be designed for crimes associated with emails, link clicks or phone calls notifying someone of a lottery win. This will help propagate knowledge about the psychological triggers of social engineering crimes. If anyone receives this sort of news, they should be concerned that they cannot win a prize or be it lottery they never took part in, and no individual gives away a prize or wealth to them as a donation. Understanding this can hinder anyone from replying to the criminal. This sensitisation can further extend to software developers, although not easy to achieve, they can equally build strong products which meet certain certified and efficient security measures by default and these, in turn, will make it difficult for criminals to exploit but obviously, these would come at a high cost.

Based on routine activity theory discussed earlier, capable guardians are essential to crime deterrence. Henceforth, there is a necessity for laws that state that before or upon reaching a certain life landmark or age such as superannuation, the elderly ought to have certain basic legal documents to appoint a substitute decision-maker in cases they cannot make autonomous health and financial decisions. For example, appointing a general power of attorney, s/he can make monetary decisions when there is consensus that the person in question is no longer able to do so. Furthermore, it would equally cushion the situation if more than one caregiver or family member is liable for overseeing an elderly person's finances. Reliable friends and family members must ensure that beneficiary names are as intended, and documents are not altered without the elderly's citizen's permission or consensus with all that are involved. Although this provision might still be abused by some individuals, refining it by appointing multiple trusted people can cushion this weakness thus adopting a mechanism that operates like a joint account in the banking sector, you

need the consensus of the other parties to make any changes or withdraws. These are legal safeguards that can help prevent financial fraud of the elderly.

Besides that, the banking sector has great potential to collaborate with researchers to better comprehend elderly fraud, mostly by plotting patterns of customer saving and spending habits to holistically identify those who are highest at risk. As an example, additional studies could be conducted on decision neuroscience and behavioural economics, this could potentially enlighten the institutions how age-related differences in decision making rise the probability of fraud, this process would ultimately enable them to establish probable tracepoints for sensitising elderly on how to avoid fraud.

Another aspect that could improve the situation is financial institutions constantly updating clients regardless of their age on the types of fraud that are currently trending since fraud is one of the elements they constantly have to contend with. It is not enough to only write such information on their websites. It is debatable that most people hardly read the security section which informs people of such crimes. Hence, the banking sector can do more. For instance, they could initiate tailored newsletters aimed at informing both old and new clients about fraud how to report and ultimately avoid it. While we admit that the financial industry has a vital role to play in decreasing financial fraud. It is also imperative that we acknowledge that preventing financial fraud is beset with risks. Laws designed to uphold customer rights to autonomy and confidentiality occasionally impede with the bank's financial protection efforts. For instance, customers have a right to make choices where, how they invest and how they spend their money regardless of whether these choices are in their best interests or not. Lichtenberg (2016) therefore, suggests that even though banks have risk and relationship management incentives to intercede when fraud is presumed, they must also be careful not to infringe on their customer’s freedoms. This entails that they must try to distinguish when losses are due to fraud as opposed to poor customer choices in uncertain financial markets.

5.1 Lessons Drawn

The study identified social engineering, investment fraud and romance fraud as some of the prominent fraud trends in Sweden. It is noteworthy to state that these type of crimes are not new to Sweden, However, the study does confirm that there has been a spike in these types of crimes

in their own accord, For example, evidence from the study indicates that there has been an increase in cryptocurrency or bitcoin under-investment fraud. While romance fraud may not be as prominent as the former, statistics for romance fraud are likely to be much higher than what has been documented due to the low reporting rates not just in Sweden but across the globe. What does stand out among the identified methods is social engineering. It is more rampant than any than method possibly due to the many ways it can be executed by criminals. For many criminals, it is a lucrative and almost effortless crime as you do not need to be a skilful programmer to execute social engineering attacks. The expansion of internet use has evenly acted right into the criminal's hands and just like many other frauds, the results can bear terrible financial outcomes for affected victims.

5.2 Conclusion

In summary, the paper had the following objectives: (I) What are the risk factors of elderly fraud, (II) What methods are used to defraud the elderly (III)What measures have been put in place. The document uncovered different types of methods, however, social engineering emerged as the most prominent and since it tends to happen in many ways such as vishing and phishing etc, it has the potential to be used by criminals for a long time. On the other hand, several risk factors were further revealed by the study. Among them, including age-related dementia, the naivety of the elderly, isolation and less mobility due to old age. All these factors can put the elderly in harms' way. To sum it up, the study further looked at the measures put in place to address the problem. It was observed that financial institutions have put in place several mechanisms to detect suspicious behaviour one such system is the anti-financial crime unit. Furthermore, new laws that apply to financial institutions have been enacted to help fight money laundering and terrorist financing. Besides, initiatives such as "*Don't try to fool me*" have been launched by the police, PRO, SFP and SKPF. Furthermore, to ensure efficiency, the police have a department called the national fraud centre that solely focuses on fraud. Despite the strides that law enforcement and financial institutions have put in place, it was suggested that more efforts be put into evaluating existing security programs, conducting routine research and sensitising the public about different types of fraud and how to avoid them. For instance, public campaigns can be designed to inform the public about perpetrator warning signs and risk factors which ultimately may be key to prevention. To achieve rapid dissemination of information it is ideal that media houses are engaged.

5.3 Opportunity for further Research

- While this study named some important risk factors that enhance the likelihood of elderly fraud, the accurate causal mechanisms involved still necessitate further research. For instance, we can contend that seniors who engage in routine activities, such as socializing with their colleagues, are less likely to be exposed or experience fraud. What exactly bears this effect needs closer inquiry. It could be that such events lessen prospects for elderly fraud, but they could also expose the elderly to a broader network of individuals who might have sinister intentions. If we apply the lifestyle theory, on the other hand, the elderly can still be at risk whether they decide to stay home carrying out their day to day routine.
- The banking sector has the opportunity to conduct research on the effectiveness of the current security mechanism in place. Since technology is constantly improving, the need to constantly evaluate the efficiency and effectiveness of existing programs and mechanisms is essential. Doing so will give an insight to many aspects, for example, the strength and weakness of the current strategies, customer vulnerability characteristics as well as developing a psychological profile of a potential criminal thus coming up with better and effective approaches to prevent fraud.

5.4 Recommendations

- The variety of methods through which fraud occurs is extensive, Therefore, the abundance of such methods, in turn, specifies that any exertions to decrease fraud must be multifaceted. For example, the panacea should be holistic enough to address the different methods as well as inform the masses about how fraud can occur.
- Considering that only a few fraud cases are reported to law enforcement. There is a necessity for education regarding the significance of reporting such incidents as well as efforts to ensure that law enforcement reacts to such reports in a well-publicised and proactive manner. Prospective offenders may be less willing to engage in fraud if they hear or read about the nature of how law enforcement is aggressively responding to any form of fraudulent activity.

REFERENCES

American Association of Retired Persons (1993) The behaviour of older consumers: An AARP study. Washington, DC: American Association of Retired Persons.

Anderson, K. B. (2013). Consumer Fraud in the United States 2011: USA, The third FTC survey.

Alan Bryman (2016) Social research methods, Oxford: Oxford University Press.

Alves, L. M., & Wilson, S. R. (2008) The effects of loneliness on telemarketing fraud vulnerability among older adults. Journal of Elder Abuse & Neglect, 20(1), 63–85.

Bonnie R, & Wallace R. (2003) Elder mistreatment: abuse, neglect, and exploitation in an ageing America. National Research Council (U. S.) Washington: National Academies Press.

Burnes, D., Henderson, C. R., Jr, Sheppard, C., Zhao, R., Pillemer, K., & Lachs, M. S. (2017) Prevalence of financial fraud and scams among older adults in the United States: A systematic review and meta-analysis. American Journal of Public Health, 107(8) 13–21.

Carcach, C., Graycar, A., & Muscat, G. (2001) The victimisation of older Australians. Canberra, Australia: Australian Institute of Criminology.

Castle, E., Eisenberger, N. I., Seeman, T. E., Moons, W. G., Boggero, I. A., Grinblatt, M. S., & Taylor, S. E. (2012) Neural and behavioural bases of age differences in perceptions of trust. Proceedings of the National Academy of Sciences, 109(51), 20848–20852.

Christie N, (1986) 'The ideal victim' In Fattah E A, (Eds.) From Crime Policy to Victim Policy: Reorienting the justice system. New York: Martin's Press.

Cohen, C. A. (2008) Consumer fraud and dementia. Lessons learned from conmen. Los Angeles Sage Publications.

Cohen, L., & Felson. (1979) Social change and crime rate trends: A routine activity approach. American Sociological Review, 44, 588–608.

Coleman J. W. (1987) Toward an integrated theory of white-collar crime. New York: Routledge.

Consumers International (2019) Social media scams: Understanding the consumer experience to create a safer digital world. England, Consumers International.

Consumer Fraud Research. (2006) Investor fraud study final report. Washington, DC: NASD Investor Education Foundation.

Deevy, M., & Beals, M. (2013) The scope of the problem: An overview of fraud prevalence measurement. Stanford, California: Financial Fraud Research Centre.

DeLiema, M. (2015) Using mixed methods to identify the characteristics of older fraud victims

Los Angeles, USA: University of Southern California.

DeLiema, M and Conrad, J. K (2017) Financial Exploitation of Older Adults. Stanford USA: Springer International Publishing.

DeLiema, M. & Deevy, M. (2016) Aging and Exploitation: How Should the Financial Service Industry Respond? Pension Research Council, University of Pennsylvania.

Denburg, N. L., Cole, C. A., Hernandez, M., Yamada, T. H., Tranel, D., Bechara, A., & Wallace, R. B. (2007) The orbitofrontal cortex, real-world decision making, and normal ageing. Annals of the New York Academy of Sciences, 1121(1), 480–498.

Druckman D. (2005) Doing research. London: Sage Publications.

Fischer, P., Lea, S. E., & Evans, K. M. (2013) Why do individuals respond to fraudulent scam communications and lose money? The psychological determinants of scam compliance. Journal of Applied Social Psychology, 43(10), 2060–2072.

Fatima, S & Naima, K (2019) Social Engineering Attacks. Grand Forks, University of North Dakota.

Finke, M. S., Howe, J. S., & Huston, S. J. (2016) Old age and the decline in financial literacy. Management Science, 63(1), 213–230.

Goergen, T & Beaulieu, M (2010) Criminological Theory and Elder Abuse Research Fruitful Relationship or Worlds Apart. New York; Springer Science.

Gregory, S., & L. McKie (1996) ‘Reflecting on the Process and Methods of Researching Women's Health’. Pp. 251–65, in Researching Women's Health: Methods and Process, edited by L. McKie. Dinton: Quay Books.

Greenspan, S., Loughlin, G., & Black, R. S. (2001) Credulity and gullibility in people with developmental disorders: A framework for future research. International Review of Research in Mental Retardation, 24(1), 101–135.

Gross, E. A. (1999) Elderly victims of telemarketing fraud: Demographic, social, and psychological factors in victimization and willingness to report. Los Angeles, USA: University of Southern California.

Holtfreter, K., Reisig, M. D., Mears, D. P., & Wolfe, S. E. (2014). Financial exploitation of the elderly in a consumer context. Final Report. Washington, DC: National Institute of Justice.

Hesse-Biber, S. N. & L.P. Leavy (2005) The Practice of Qualitative Research. Thousand Oaks, CA: Sage Publications.

Jackson, S. L., & Hafemeister, T. L. (2013) Financial abuse of elderly people vs. other forms of elder abuse: Assessing their dynamics, risk factors, and society's response. Washington, DC: National Institute of Justice Final Report.

Jackson, S. L. (2015) The Vexing Problem of Defining Financial Exploitation, Journal of Financial Crime, 22(1): 63-78.

King R, Wincup E, (2007) Doing research on crime and justice (2nd edition). Oxford: Oxford University Press.

Kirchheimer, S. (2011) Scams trap older adults. Washington, DC: American Association of Retired Persons.

Kvale, S. (1996) Interviews: An introduction to qualitative research interviewing. London: Sage publications.

Lachs, M. S., & Han, S. D. (2015) Age-associated financial vulnerability: An emerging public health issue. Annals of Internal Medicine, 163(11), 877–878.

Lang, F. R., & Carstensen, L. L. (2002) Time counts; Future time perspective, goals, and social relationships. Psychology and Aging, 17(1), 125–139.

Lee, R. M. (1993) Doing Research on Sensitive Topics. London: Sage Publications.

Liamputtong, P. & D. Ezzy, (2005) Qualitative Research Methods, 2nd edition, Melbourne: Oxford University Press.

Li, T., & Fung, H. H. (2012) Age differences in trust: An investigation across 38 countries. Journals of Gerontology Series B: Psychological Sciences and Social Sciences, 68(3), 347–355.

Lichtenberg, P. A., Stickney, L., & Paulson, D. (2013) Is psychological vulnerability related to the experience of fraud in older adults? Clinical Gerontologist, 36(2), 132–146.

Lichtenberg, P. A., Sugarman, M. A., Paulson, D., Ficker, L. J., & Rahman-Filipiak, A. (2016) Psychological and functional vulnerability predict fraud cases in older adults: Results of a longitudinal study. Clinical Gerontologist, 39(1), 48–63.

Martyn Denscombe (2007) The Good Research Guide for small-scale social research projects; Maidenhead: Open University Press.

MetLife. (2011). The MetLife study of elder financial abuse crimes of occasion, desperation, and

predation against America's elders. UK: Oxford University Press.

National Council of Crime Prevention (2019) Money laundering offences: A follow-up of the application of the law. Stockholm: Brottsförebyggande rådet.

National Council of Crime Prevention (2018) Crime against the elderly on victimisation and insecurity. Stockholm: Brottsförebyggande rådet.

National Council of Crime Prevention (2016) Fraud crime in Sweden. Stockholm: Brottsförebyggande rådet.

Office for National Statistics. (2016) Overview of fraud statistics: Year ending Mar 2016. UK, Crime statistics.

Olivier, S., Burls, T., Fenge, L. A., & Brown, K. (2015) "Winning and losing": Vulnerability to mass marketing fraud. The Journal of Adult Protection, 17(6), 360–370.

Pak, K. & Shadel, D. (2011) AARP foundation national fraud victim study. Washington, DC: America Association of Retired Persons.

Rubin, Herbert J. & Rubin, Irene S. (1995) Qualitative interviewing: the art of hearing data. London: Sage Publications.

Samanez-Larkin, G. R., Gibbs, S. E., Khanna, K., Nielsen, L., Carstensen, L. L., & Knutson, B. (2007) Anticipation of monetary gain but not loss in healthy older adults. Nature Neuroscience, 10(6), 787–791.

Titus, R. M. Heinzelmann, F. & Boyle, J. M. (1995) Victimization of persons by fraud. Crime & Delinquency, 41(1), 54–72.

Tom Buchanan & Monica T. Whitty (2012) The Online Dating Romance Scam: A Serious Crime. Cyberpsychology, Behaviour, and Social Networking, 15(3), 181-183.

Van Wyk, J. & Mason, K. A. (2001) Investigating vulnerability and reporting behaviour for consumer fraud victimization opportunity as a social aspect of age. Journal of Contemporary Criminal Justice, 17(4), 328–345.

APPENDICES

TO WHOM IT MAY CONCERN

Dear Sir/Madam

I am a student at Malmo University pursuing a master's degree programme in Criminology. I am in my final semester and in the process of writing my thesis. My research topic is "Financial exploitation on the elderly, what is the way forward"? The main aim of the project is to determine what methods are used to defraud the elderly and provide some solutions. The information provided will strictly be used for academic purposes and will not be used in any other form. Any formation rendered will be highly appreciated.

Interview Guide

1. What are some of the risk factors among the elderly when it comes to fraud?
2. What are the most common methods used?
3. Do banks inform customers about fraud beforehand?
4. Who do you think are the main targets of fraud in general?
5. Do you think it is a growing problem?
    a) Why do you think so?
6. What are some of the measures in place?
7. Do you think these measures have been successful?
    a) Why do you think so?
8. What is the way forward to this problem?
9. Do you think Perpetrators of fraud are from Sweden or other countries?
    a) Why do you say so?