Identity crimes in the UK: An examination of the strategies employed by front-line practitioners in the public and private sector to detect, prevent and mitigate against this crime

Aida Fazely

Student no: M00213159

School of law/criminology

November 2020

Abstract

Identity related crimes are becoming increasingly prevalent in modern society. It is a crime type that concerns and impacts governments, private institutions and consumers worldwide. The aim of this research was to provide a better insight into how this crime is perceived by government and commercial institutions in the UK (including their views on offenders and victims), to review the processes employed by the public and private sector to assess risk and develop mitigation and prevention strategies and, in doing so, to discover how the most prominent criminological theories contribute to these efforts. Its final aim was to examine the current state and effectiveness of the collaborations and partnerships which have been developed across the public/private sector spectrum to understand and combat this crime.

The methodology employed to undertake this research was based on conducting interviews with the key identity fraud and crime practitioners within major public and private organisations. Qualitative research was used in order to generate as much information as possible to form ideas. In addition, documents were also examined to complement the data collected from interviews. The researcher, due to previous employment within the UK financial sector dealing payment fraud, was ideally placed to access, and generate participation across government, law enforcement and other commercial organisations.

The study highlights the current thinking and approaches by front-line identity crime prevention practitioners in defining, perceiving, measuring, policing, detecting, preventing and mitigating identity crime. It also highlights how heavily existing situational crime prevention techniques are being used to combat this issue and how they are complemented by partnership approaches and, most importantly, data-sharing which is widely accepted by practitioners as being a vitally effective tool in dealing with this issue. Problems exist in the majority of these areas with the central concern being the lack of leadership from the government in taking ownership of this insidious and escalating crime type which creates commercial and individual victims but also significantly, enables serious crimes such as human and drug trafficking and terrorism. Equally pressing is the need for the commercial sector, instead of treating identity crime as a phenomenon to be denied or ignored (or as one which needs to be accepted as a cost of doing business) to improve data sharing, strengthen its defences and review its approach to the treatment and support of victims.

Table of contents

1. Introduction

This research focuses on the issue of identity related crimes in the UK, a crime type that has been increasing and evolving over the last several years as new technologies emerge and shape our societies and way of life. This crime has presented challenges to the academic community in terms of trying to analyse it and practitioners (including the government, the public sector and the private sector) in tackling and minimizing its impact. This study aims to provide an overall understanding of this issue, capturing views and experiences from front-line identity crime prevention professionals. The public and private sector perspectives on identity crime itself and the prevention methodologies employed to tackle it will be summarised. The novelty and strength of this research lies in the information gathered from the front-line practitioners (from 2009 to 2016) as this data is mostly inaccessible to academia and, for this reason, it is most unlikely that this exercise could be repeated. Based on the analysis of this data the research is then able to provide some recommendations and resolutions for future research.

The research sets out to assess the understanding inside these organisations of offenders and their victims, to study the risk assessment and decision-making processes utilised by government agencies and private institutions to evaluate their risks associated with identity crimes, the types of resources applied and key actions taken by them to detect, prevent and mitigate against identity crime. Finally, the aim is to learn about the multi- agency collaborations that currently exist to tackle identity related crimes and examine their effectiveness in cooperating with each other and their effectiveness in combatting identity crime.

The study comprises of an abstract and introduction, a review of current literature, an explanation of the methodology used to address the research questions, a chapter examining identity crime from the perspective of the public sector, then a chapter exploring the perspective of the finance and private sectors followed by a discussion on key themes emerging from the data, recommendations of areas worthy of further academic research and finally, a conclusion.

The literature review examines a wide range of theories and previous literature and therefore is divided into distinct sections. It commences by providing a brief background on identity crime, examining identity and identifiers and then explores the various definitions offered by academics and government organisations to explain identity crime, identity theft and identity fraud. It then examines literature on the criminological theories which underpin identity crime,

followed by highlighting existing knowledge of the different methods that fraudsters use to commit identity theft/ fraud. It moves on to examine literature surrounding identity crime offenders and investigates current knowledge on identity crime victims. Finally, this chapter closes with considering crime prevention literature to date which offers valuable insights into tackling identity crime, with particular emphasis on the development of collaborative, multi-agency and partnership approaches.

The methodology used to conduct this research was of a qualitative nature to allow the generation of detailed information regarding this subject. Primary data and documentary analysis were used to undertake this study. Primary data was generated by open-ended questionnaires from the selected sample (which included public sector and private organisation representatives responsible for dealing with identity crime related issues). In addition to the primary data, secondary data was generated from an analysis of documents (obtained from participants and various organisations including documents provided by the researcher from her employment in the finance sector).

The specific questions that were posed to the participants, in order to answer the central research questions were: How is identity crime perceived in your organisation? Are you affected by identity crime? How do you define identity crime? Who are the victims and offenders? What objectives do you employ with regards to identity crime? How do you detect identity crime? What prevention and mitigation measures do you have in place? Do you work with other organisations? And what else needs to be done to tackle the issue?

The next chapter focuses on the public sector and is divided into two main sections. The first part focuses on the degree of acknowledgment of this crime in the UK, examining the government's response to it. In doing so, it highlights the efforts made to measure it, followed by an examination of identity crime from the perspective of the government and the public sector. It then reviews how identity crime has come to prominence and been recognised as a threat, followed by an examination of past and current efforts by government and the major public sector organisations that play an important role in tackling identity crime (such as the National Fraud Authority (NFA), CIFAS (Credit Industry Fraud Avoidance System) and law enforcement), to deal with it.

Next, the impact of the sharp and continued rise in cyber-crime is reviewed as it is a major factor in the commission of identity crime and a major challenge to practitioners (in both the public and private sectors) on the front line of identity crime prevention efforts. The latest public sector strategies employed to tackle this element of identity crime will be examined along with national and international efforts focussing on the contributions from the EU and

UNODC. The second part of this chapter will capture and discuss the responses to the research questionnaire provided by the public sector participants.

The next major section focuses on the private sector and, like the public sector, is split into two main parts. The first focusses on the finance industry (which suffers the most from this crime) and which is the leader in systematically collecting identity crime data and collaboratively working on this issue. Different types of financial identity crime will be examined such as counterfeit payment card fraud, remote purchase fraud, lost/stolen cards, card identity theft and finally mail-non receipt payment card fraud along with cheque fraud, online banking, mobile banking, telephone banking fraud and money mules. The UK payment infrastructure is a complex web of institutions and players all working together to deliver the services and products that have become such a fundamental part of everyday life. These entities will be listed and discussed briefly. The chapter will then move on to highlight the significance of the media and academia in the efforts to tackle identity crime within the finance sector. Emerging criminal methods will be examined next followed by the increasingly frequent data compromises that have occurred, not just with the finance sector, but also other industries and government organisations. The compromises caused by internal staff will be discussed as these play an important role in the arena of identity related crimes. The other topics covered in this section will include the major vulnerabilities present within the finance sector, such as data authentication, online services, customer vulnerability, staff recruitment and documentation.

Organisations in the finance sector use a number of strategies in their efforts to tackle identity crime, those developed from situational crime prevention techniques emerge as the central and most important tools to tackle this issue. Recommendations are made to further utilise these techniques. The second part of this chapter captures the responses of private sector representatives to the interview questions.

The last two sections of this research consist of discussion and conclusion. The discussion brings together the overall findings of this research with a number of themes being highlighted. Firstly, it highlights how this crime generates widespread challenges, with the academic community finding it hard to explain it, law enforcement, government and the private sector finding it hard to tackle it and the general public struggling to keep their identifying information safe. Another issue discussed is victims of this crime. Identity crime creates multiple victims with very diverse types of victimisation and impacts on its victims.

This study has highlighted four strong common identity crime prevention themes amongst respondents' answers. The central strategy consists of education, awareness-raising campaigns, working in collaborative partnerships and dealing with insiders.

Another theme discussed in this section is that some organisations (both public and private) are more concerned about being seen to tackle this issue rather than making a real impact.

It was generally felt by participants that collaboration on policy and strategy was effective but, at the tactical and operational level it was difficult to implement strategies. Collaboration between government and the private sector on tackling identity crime is strained as the latter regards the former's initiatives as expensive and thus rejects them as commercially unworkable. On the other hand, businesses could do more to improve identity crime prevention strategies and defences but do not, preferring instead to accept identity crime as, currently, a small cost of doing business.

The recommendations that were provided by participants were summarised and used as a basis to suggest improvements in key functional areas such as better intelligence sharing, better measurement, enforcement, consumers' involvement with regulatory issues related to identity, data protection, actions on internal fraud, cyber-strategy, mobile services, crime prevention and aftercare and futurology (Horizon scanning)/fraud forecasting. Additionally, a number of recommendations have been made for future research in this area.

And finally, the conclusion draws this study to an end by stating that better understanding of this crime is needed, especially the role of cyber-crime and the international element, that academia has already contributed valuable concepts (such as SCP) and has more to offer the commercial and regulatory organisations if certain hurdles can be overcome, that strong and effective 'ownership' and leadership is needed from those bodies tackling identity crime, that more needs to be understood about offenders and victims and that the work carried out by partnerships needs to be enabled and expanded.

2. Literature review

2.1. Introduction

The aim of this research is to provide a better understanding of identity crime in the UK from the perspective of the front-line professionals within the public and private sector who are tackling this issue on a day-to-day basis. The research will capture their perspectives on this crime and the prevention methods and decision-making processes employed in doing so followed by providing recommendations and resolutions required to enhance current strategies. To achieve this an examination of the existing literature is required in order to highlight the existing knowledge gaps.

The purpose of this chapter is to examine the literature that currently exists on the topic of identity crime, identity theft and identity fraud. This examination will also highlight knowledge gaps and provide a sense of direction and focus for this study. Due to the nature of this topic, there is a need to examine a wide range of theories and previous literature and therefore this chapter will be divided into eight main sections.

The first part of the literature review will focus on a brief background on identity crime, the second part will examine identity and identifiers and the third section will focus on the various definitions offered by academics and government organisations to explain identity crime, identity theft and identity fraud.

Part four will examine literature on the criminological theories which underpin identity crime and part five will move on to highlight existing knowledge of the different methods that fraudsters use to commit identity theft/ fraud. Part six will focus on the literature surrounding identity crime offenders and part seven will investigate current knowledge on identity crime victims. Finally, this chapter will close with part eight which will consider crime prevention literature to date which offers valuable insights into tackling identity crime, with particular emphasis on the development of collaborative, multi-agency approaches.

2.2. Identity crime background in the UK

According to Yang et al. (2014) identity crime has become the defining crime of the information age, with an estimated nine million incidents each year. It is not surprising that this crime has been one of the most talked about types of fraud in recent years, more than occasionally stealing the headlines of newspapers and TV stations. Academics have also

reflected on this ever growing phenomenon with Lo Pucki (2001) stating “Identity theft is out of control” and Alison et al. (2005) holding that “identity theft is growing at a greater rate than any other theft-related offence”. This is further emphasised by Helser (2015) who points out that not only is this crime on the rise but also that it affects individuals, businesses and industry worldwide, compromising the integrity of the systems that are fundamental components of our society. The damage that this crime causes its victims is significant to the point that what is stolen is almost never returned, and criminals keep on selling and trading stolen identities to other criminals for further misuse via illicit criminal marketplaces within the dark net (Lacey et al., 2016).

One reason this type of crime has attracted focus is because it not only causes great financial difficulties for its victims but also causes them a great deal of inconvenience. Camp (2007) emphasises this point by stating that “individuals have lost control of their identities, all the data is publicly available about who we are.” She believes that we are living in the middle of a terrible collusion, using traditional public community information to confirm identities in a world of networked digital wealth. It may also seem that identity crime is a recent phenomenon, but the history books indicate that this form of crime existed centuries ago citing examples such as forging cheques or impersonating a credit-worthy buyer. However, these practices were not widespread. It was really not until 1992 that it appeared with some prominence on the radar of some public agencies (in particular, HM Revenue and Customs and the Passport Service) which were able to detect it for the first time (Cendrowski et al., 2007). Since then it has become one of the fastest growing crimes in the world. This rapid increase is due to a number of factors such as: changes in the way that we conduct our societies, lack of community awareness, increased mobility of individuals, different methods of making payments and also the recent rise and spread of globalisation in electronic commerce, which is enabling criminals to have the opportunity to operate across international borders quicker and easier (National Crime Prevention Programme, 2004:3). This view is further supported by McNally and Newman (2010) stating that “Identity theft has existed for centuries, but the opportunities for its commission have evolved over time as a function of modernisation”. With the internet emerging as not just a tool for sharing information but also as a useful platform for enabling domestic and international transactions (Lim et al., 2016), this new technology-powered environment has caused significant change in the behaviour, habits and trends of modern consumers, which leads to the increase of e-commerce (Fortes and Rita, 2016).

The presence of this crime in policy documents and publications of various jurisdictions is evident. These publications report on the increasing number of cases of identity fraud and the financial and other types of loss it causes to individuals, enterprises, public organisations and society in general. These publications also set out what measures are taken or are proposed to combat identity fraud. In many jurisdictions, identity fraud is not, by itself a criminal offence (Vins et al., 2008).

When examining this crime there are those that believe that there is a 'hype' about this crime and that it is not as big an issue as some journalists make it out to be (Wall, 2013a). Wall's argument is supported by data from the Scottish Crime and Justice survey of 2012 (National Statistics, 2012:6) where it was discovered that 58% of adults were most worried about someone using their personal financial information to obtain money, goods or services and 48% were worried about having their identity stolen. These figures however were in sharp contrast with real victimisation figures of 4.5% of Scottish adults but the NFA found that 9.4% of people who responded to their survey had been victims of identity crime (National Fraud Authority, 2012). In another study carried out by Jordan et al. (2018) it was discovered that once the fear of identity theft and financial loss and reputational damage increased so did the perceived risk- which then impacted consumers' on-line shopping behaviour. If the fear decreased so did the risk and that resulted in increased on-line shopping.

Not even academia has been safe from identity crime. Dadkhah et al. (2017) highlights how in recent years, identity theft has been growing by cybercriminals who create false profiles for prominent scientists in attempts to manipulate the review and publishing process.

It was this constant presence of identity crime in the media, academia and popular culture that instigated an interest in carrying out research in this crime. Most of what is written academically on this issue is USA based and therefore the researcher's aim was to capture the developments in this area in the UK. Additionally, no study has been undertaken where it focused on the practitioners' views and perceptions (more specifically public and private organisations) and their efforts to tackle this issue. Therefore, this study aims to cover gaps that exists in this area.

2.3. Definition of identity and identifiers

Identity is a word that perhaps is very commonly and loosely used in our modern society. Depending on the context in which a specific identity is used, it can refer to one's name, position in an organisation or within society. It can even make references to one's cultural background and ethnicity. Identity is not limited just to individuals, companies and public and

private organisations also have their own identities with which they communicate to their customers or other organisations. They also win and keep their customer's trust using this identity and on the negative side can become victims of identity crime when this identity is used by fraudsters.

In terms of defining "identity" one of the best definitions is provided by Camp (2007:11). She explains that identity is a set of attributes that correspond to the appropriate identifiers. She then elaborates that "an identifier distinguishes a distinct person, place or thing within a given context", believing that each identifier is meaningful only within the context/space that they are identified.

According to Hamadi (2004) an identifier is "a characteristic (such as appearance, fingerprint, full name etc) that, either by itself or in combination with other data, more or less uniquely identifies a person". He refers to a report published by the UK Cabinet Office in 2002, in which it is argued that three basic identities exist. Although dated, this categorisation provides a good summary of the type of identities that exist or are used. Biometric identity which consists of attributes that are unique to an individual such as fingerprints, voice, facial structure, DNA, etc. Attributed identity consists of components of a person's identity that are given at birth such as name, address, date and place of birth. Finally, biographical identity which builds up over time which covers a large range of activities that a person undertakes through his or her life such as details of education/ qualification, one's credit history, insurance information, marriage etcetera.

Cendrowski et al (2007) provides a list of different identity information that are used in our societies and that fraudsters seek to steal in order to carry out their crimes which includes a name, address, National Insurance Number, date of birth, phone number, ATM, debit and credit card numbers, credit card security codes and Personal Identification Numbers (PIN) for bank and credit cards, bank account numbers and balances, income and credit history, driver's license number, passwords, e-mail address, other personal information such as maiden names, retirement accounts, citizenship and family/kin history.

Some of these identifiers are attributed and some are biographical but together they are means by which a person can be identified by various organisations or institutions. For example, debit or credit card numbers help the respective bank to recognise its customer and allow the transaction or requested functions to be carried out on the card or the account.

At the moment, the only identifiers that are used in the UK are attributed or biographical with the exception of the new passports that have an element of biometric data included in them. The financial service providers use these two methods to make decisions on their potential customers and to verify them when repeat business takes place. There has been a vast expansion in credit recording and reporting practices due to this relatively modern practice and businesses, in order to protect themselves from future losses, enthusiastically contribute to these databases by sharing the data that they hold on consumers and use these databases for their decision-making processes at the same time. The way that identities are used in today's society has changed significantly over the last few decades. In the past, a person was not required to identify him or herself or use identity related products or services as often as is now the case in the modern world. A person's name and face used to be sufficient to verify his or her identity to other members of society. Using cash and paper tickets was a norm that did not take much identification. Today, however, this has all changed. People are relying less and less on cash and more and more on electronic cards (payment cards) to conduct transactions. In order to use public transport, they rely on travel cards, such as Oyster, which are another means of payment linked to identification. In the current society, a means of identification and the verification of this identity is becoming increasingly indispensable in order to fully function. This technological aspect is increasingly dominating the life of citizens.

The introduction of identity cards in the UK, however, was to bring biometric factors to the fore in everyday identification situations but the plan was stopped once the coalition government came into power (Identity cards are to be scrapped, 2010).

2.4. Definition of identity crime

Identity crime is an umbrella term comprising two distinct elements: identity theft (which may not in itself constitute a crime) and identity fraud (the illegal use of the stolen identity data to commit crime), with the former acting as an enabler of the latter (Wall, 2010a). Wall (2013a) states that identity crime is a much "contested term" and is a social definition for some very real offending. There are several definitions to describe this type of crime. White and Fisher (2008), for instance, believe that identity theft is the unlawful use of another's identifying information for gain, whereas Koops and Leenes (2006) believe that a precise definition of identity theft can be found in the US Identity Theft and Assumption Deterrence Act (title 18, s. 1028(a)(7) U.S.C.) which sates "Punishable is s/he who: knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal Law, or that

constitutes a felony under any applicable State or local Law." Camp (2007:8) on the other hand provides a more holistic definition by stating that identity theft is "the misuse of information to masquerade as someone else to obtain resources or avoid risk". She elaborates on this definition by stating that identity theft is in no way associated with physical impersonation of someone. Instead, it is the compilation of information in order to access the rights and privileges associated with that person or information. Camp also believes that "identity theft is enabled because of the confusion between authenticating identity and authenticating attributes" (ibid:13). Identity authentication is proving an association between identifiers and attributes (ibid). Wall (2013b) also highlights the distinction between identity and identifiers.

The examination of identity theft and its definitions has also highlighted various statements offered by a number of academics and organisations. McNally and Newman (2010:2) provide a description of the terms used to describe this crime arguing that:

> "Historically identity fraud was reviewed as being committed against the collective bodies (e.g. governments, financial institutions) that received fraudulent personal information rather than against the people who were fraudulently identified by that information. The term identity theft, which did not appear until the late 1980s was initially used to distinguish individual victims (identity theft) from collective victims (identity fraud), both of whom were harmed by the same set of criminal activities. More recently these terms have been applied in a different manner to separate the act of acquiring an individual's personal information (identity theft) from the act of misusing that information (identity fraud) however, since obtaining someone's personal information is a necessary condition for its misuse, many tend to call this combined act identity theft."

Koops and Leenes (2006), in order to address the lack of consistency in defining identity theft or fraud, suggest the use of 'identity-related crime' as an umbrella term for this fraud. They argue that between all the definitions for identity theft there are some common factors which are: a) some means of identity: a name, document, or other identifying data b) which does not belong to the perpetrator himself/herself c) with an element of unlawfulness. The Home Office Identity Fraud Steering Group (2008), in order to bring some clarity and unity into describing this type of crime, stated that: "Identity fraud and identity theft are often used very loosely to describe any situation in which personal details are misappropriated for gain."

It then moves on to provide definitions on the following phrases (ibid):

Identity Crime: a generic term for Identity Theft, creating a False Identity or committing Identity Fraud (ibid).

False Identity: a fictitious (i.e. invented identity; or an existing identity i.e. genuine) identity that has been altered to create a fictitious identity (ibid).

Identity Theft: occurs when sufficient information about an identity is obtained to facilitate Identity Fraud, irrespective of whether, in the case of an individual, (rather than an organisation) the victim is alive or dead. (ibid)

Identity Fraud: occurs when a false identity or someone else's identity details are used to support unlawful activity, or when someone avoids obligation/liability by falsely claiming that he/she was the victim of Identity Theft (ibid).

The above were the best descriptions provided for this crime specially establishing identity crime as the umbrella term covering all different elements and stages of committing this crime. In an effort by Rost, Meints and Hansen (2005 cited in Koops and Leenes, 2006) to provide further clarity on this matter, they examine the link between an identifier and the person (or role) and provide four partly-overlapping types of identifier alteration/modification: identity collision, identity change, identity deletion and identity restoration. The type most relevant to this study is identity change, which is when someone takes on another identity, usually intentionally. This category in itself can be divided to four sub-groups of identity take over, when someone takes over the identity of another person without that person's consent, identity delegation, when someone uses someone else's identity with that person's consent, identity exchange, when two or more people, with mutual consent, use each other's identity and finally identity creation, when someone creates the identity of a non-existing person. They further argue that identity crime falls broadly into the remit of unlawful change of someone's identity. This categorisation is by far the best approach to examining the different ways an identity can be affected and at the same time different identity changes that happen when identity theft or fraud takes place. As it was mentioned earlier the crime under study is not always the result of a stolen identity, it can also happen when a bogus identity is created and furthermore, when someone wrongly claims to have become a victim of identity fraud.

Although the Identity Fraud Steering Group's website provided definitions, in practice there are still issues around this area. The attempts made to introduce definitions that could be used have not necessarily helped to solve the definition issues but rather created further confusion both for the public and for the market and as Wall (2010a) argues identity crime is

a much contested term. Having definitions agreed by practitioners is important as it will have an impact on measuring this crime and any collaborative work that will aim to collectively address this issue. How can something be measured if the terms are not agreed upon? Oranges cannot be compared to apples?

Due to the way that our society is shaped and the way that modern living is organised, an individual's identity is not the only one that is used. Our identities are used to perform important and increasingly crucial tasks in everyday activities such as shopping, accessing buildings and acquiring goods and services. There are three types of identities that can be stolen by an identity criminal: personal individual identity, identity of directors of companies and corporate identity. Personal individual identity crime occurs when the identity of a person is stolen and used to access services or acquire goods. Directors' identity crime occurs when the identity of a director of a company is stolen and used to access company data in order to obtain assets, goods or services. This can be very damaging for small businesses as they rely on cash flow to help them continue trading. Companies House, in order to tackle this issue, introduced PROOF (PROtected Online Filing) which enables companies to protect themselves from unauthorised changes to their company's record as it prevents the filing of certain paper forms. These include documents for an appointment/termination/change of particulars of company officers and the change of the registered office (Companies House, 2020).

Corporate identity crime occurs when the identity of a corporation is stolen and used to obtain data or other goods and services. Mass marketing fraud also falls into this category as fraudsters use this method to pretend to be banks or other institutions, by way of emails or by calling people in order to acquire their personal identifying details. Companies and organisations use their identities/brands to win and keep customers and their loyalties. Any damage to this reputation can have a devastating impact on these entities.

Newman and Clark (2003 cited in McNally and Newman:1) in their analysis of e-commerce crime, argued that the "hot product" of the information age is information itself, and that the tool offenders increasingly use to access this target is the internet environment. They elaborate this point by emphasising that the information fits the attributes of hot products - CRAVED short for Concealable, Removable, Available, Valuable, Enjoyable and Disposable/Durable. And as Clark (1999:2) points out 'hot products' attract theft. Wall (2018) a major contributor to the knowledge on identity related crimes in the UK in his last work argues that big data feed big crime. Big data referring to the information that is generated

during our interactions with the internet (both transactional and content-viewing). He uses two different terminologies to describe some of the crimes being carried out on internet: upstream and downstream. Upstream referring to data breaches, Distributed Denial of Services attacks (DDoS) and mass spam attacks. Downstream describing crimes committed using the stolen data, further elaborating that often these two separate crimes are committed by different people.

White and Fisher (2008) argue that despite its growth, the basic questions about identity theft remain unanswered. They believe that the primary challenges to improve our understanding and response to identity theft are: 1) the limitations of current definitions of identity theft 2) how it is committed, discovered and reported 3) the inconsistent, fragmented response by law enforcement and private industry 4) problems with existing data sources and implications for measuring its prevalence. White and Fisher's list is valuable but lacks in-depth analysis of each of these challenges and instead provides a broad description of them.

In order to get an accurate picture of any type of crime, it is imperative to have some statistics and figures to know what the financial impact of the specific crime type are. Unified and widely accepted definitions have value in helping to accurately measure this. A brief look at the UK indicates the lack of data in this area and the data that is available is reports from the private sector. Currently the only organisation providing figures for this crime is CIFAS.

CIFAS (UK's Fraud Prevention Service, 2019), in collaboration with a several private and public sector bodies, publishes a report that combines research, statistics, maps, prevention tips, case studies and opinion pieces on this issue. The methodology that is used to examine identity fraud is based on the number of reported fraudulent cases. As this data is based on the data provided by CIFAS members, it may present a significant bias and may not reflect all the identity crime incidences.

	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016
Identity Fraud cases identified	77,500	77,600	102,300	217,385	236,516	123,58	108,554	114.000	169,592	173,000

The trend shows a sharp increase in 2009, 2010 and 2011 and even though the figures decline in 2012-2013, they continue to rise year by year thereafter. Underpinning this data is an important assertion that the decreases in identity theft may not necessarily mean that identity fraud or crime is decreasing. This statement is supported by a report published by the Insurance Information institute (2020) sharing the data from Javelin Strategy and Research study published in 2019 which highlighted that identity fraud fell to $14.4milion in 2018 down from £16.7 million in 2017 but the victims bore a heavier financial burden. In 2018 victims' 'out-of-pocket' fraud costs were $3.3million which was more than doubled from $1.7million in the previous year. Mobile account take overs were also doubled to 680,000 in 2018 compared with 380,000 in 2017.

The above literature highlights the issues that exist surrounding the challenges inherent in defining this crime. Those that work to tackle this issue must do so by using certain terms and definitions agreed in these organisations. However, there is hardly any evidence in the current literature reflecting the views of those challenges that these practitioners may have in dealing with this issue. The questions that arise are: how is this crime defined by these organisations? Do they all agree with these definitions that the Home Office provided or are there disagreements with this definition which impact the work carried out to tackle it?

2.5. Criminological theories relevant to identity crime

Having examined the different types of definitions for identity crime, it is imperative to examine, within an academic context, the criminological theories that can be utilised to explain why criminals commit this type of crime and to explain reasons behind the offenders' motivations. As Felson and Clarke (1998) state "Crime theory can and should assist crime prevention". Recent "opportunity" theories of crime have emphasised principles which are close to the real world, easy to explain and teach, and ready to put into practice (Felson and

Clarke, 1998; Kirwan & Power, 2013: 25; Holt et al., 2018:462; Yar & Steinmetz, 2019:27; Lavorgna, 2020: 34). These theories include the routine activity approach, the rational choice perspective and crime pattern theory building on the old adage that “opportunity makes the thief”. Felson and Clark (1998) go on to highlight ten principles of criminal opportunity stating that opportunities play a role in causing all crime, are highly specific, are concentrated in time and space, depend on everyday movements of activity, produce opportunities for other crimes, are focussed on products of high value and low inertia, are stimulated by social and technological change, can be prevented by reducing opportunities, where such reduction does not lead to displacement and where, with focus, their reduction can produce a wider decline in crime (Felson & Clark: 1998; Yar and Steinmetz, 2019: 26; Lavorgna, 2020:34).

Situational crime prevention theories focus on the management, design or manipulation of the immediate environment so as to reduce opportunity for crime and increase its risks as perceived by a wider range of offenders (Clarke,1983:225; Freilich and Newman, 2017). These measures include various forms of target hardening, defensible space architecture and community crime prevention initiatives. It is noteworthy that much of the feedback generated from respondents in this research addresses itself to these objectives. These theories, however, do not extend to the ‘root causes’ of crime which manifest themselves in the social, sociological and psychological traits of offenders such as anomie theory, neutralisation theory and strain theory all of which have a contribution to make in understanding the motives of identity criminals and will be addressed in this chapter.

Williams and McShane (2010:182) state that rational choice theory explains offender’s motivation to commit crime as an attempt to meet common needs with rationality being the decision-making process of determining the opportunities for meeting those needs. Copes and Vieraitis (2012:122-123) used rational choice theory to guide their interpretations of identity thieves but they also discovered that rational thinking was not always the driver behind the offender’s behaviour. They imply in much of their writing that identity thieves were rational to some degree in their decisions to become involved in identity theft, in their assessment of risk and their attempts to manage that risk, and in how they chose to enact their crimes. They continue that applying the elements of rational choice theory was the most effective approach for making sense of the data.

The opportunistic element of the identity related crimes can also be explained by routine activity theories**.** There have been some instances where the offender has had access to the identity information of close relatives which presented an opportunity to take advantage of it (Williams and McShane, 2010:179). The theory basically believes that “the volume of

criminal offences is related to the nature of everyday patterns of social interactions." Routine activity's perspective advanced by Cohen and Felson (1979), initially viewed as a very practical look at crime, gained popularity and became a staple of the 1980s. In a more identity crime focused context, academics have suggested the use of routine activity theory as a framework for identifying risk factors for victimization. In a study undertaken by Reyns and Henson (2016) the relationship between online routine activities and identity theft victimisation among residents of England and Wales were examined using the British Crime Survey. The results indicated that several online routines were positive predictors of identity theft, including online banking, online shopping, emailing or instant messaging and downloading music, films or podcasts.

Cohen, Kluegel and Land (1981) have developed a more formalised version of routine activities theory and renamed it 'opportunity' theory. This considers elements of exposure, proximity, guardianship and target attractiveness as variables that increase the risk of criminal victimisation. However, these are not measured directly. They are assumed from variations in age, race, income, household consumption, labour force participation and residence in different areas of the city obtained from USA crime victimisation surveys. Their findings nonetheless support most of their propositions.

Opportunity theory predicts that reducing the effectiveness of criminal opportunity will lead to a reduction in crime (Ceccato and Benson, 2016) which is one of the reasons why situational crime prevention strategies have been heavily employed to reduce crime in general as well as identity crime.

Huisman and Erp (2013) list 5 categories for a criminal opportunity**:** a) the effort required to carry out the offence b) the perceived risks of detection c) the rewards to be gained from the offence d) the situational conditions that may encourage criminal action and e) the excuse and neutralisation of the offense.

Although the study undertaken by Copes and Vieraitis (2012) has been a seminal work in providing a better understanding of the offenders of identity crime and insight that was lacking and much needed, there are still gaps in our knowledge that this study has failed to fill. For example, where do the hackers who steal millions of data records in one attack sit in this categorisation?

As stated before, certain types of organised identity crime have not been captured by the descriptions provided by Copes and Vieraitis (2012). One example of this is the organised gangs that operate trans-nationally hacking into computers stealing millions of consumer

data in one go then printing fake credit cards on a massive scale and abusing that data. Another example is the chip and PIN factories that were operating back in 2008-2009 who were capturing consumer data on an industrial scale and which had the characteristics of massive organised operations. They also carry out other criminal activities such as human trafficking and prostitution. This level of organised crime presents exceptional risks and challenges to the social, political and economic well-being of states and to the international community (Wright, 2006:1). These data gaps need to be addressed if a full picture of this crime is to emerge. The difficulties in defining the organised crime concept in a way that all parties are satisfied has been acknowledged by Wright (ibid :2) but nevertheless the efforts still need to be made.

Cressey (1969:72), comments that an organised criminal is defined as someone who occupies a position in a social system, an 'organisation' which has been rationally designed to maximise profits by performing illegal services and providing legally forbidden products demanded by the broader society within which he lives in. Croall (2001:147) on the other hand argues that a further problem with attempting to compartmentalize different forms of crime is the blurred boundary, between forms of white-collar crime and conventional crimes, particularly organised crimes.

Neutralisation of criminality

One of the criminal theories that contribute significantly to the understanding of identity related offending is the neutralisation theory. Neutralization, which refers ''to the employment of justifications or excuses for a wrongful behaviour before committing it, in order to alleviate guilt'' was recognised by Green (1990:77) as an attempt to highlight important factors in the psychology of occupational criminals (Lavorgna, 2020:44-45).

There are five neutralization techniques used by delinquents to counteract the guilt arising from their criminal behaviour highlighted by Sykes and Matza (1957). These are denial of injury (no harm was really done), denial of victim (no crime occurred because the entity against whom the act was committed deserved it), denial of responsibility (it was the actor's fault), condemnation of condemners (condemners are hypocrites) and finally appeals to higher loyalties (the act was done because of an allegiance to a more important principle, like loyalty to a group) (Holt et al, 2018:455-456).

In Copes and Vieraitis's (2012) study of identity crime offenders, which is one of the only studies in this area, neutralisation was discovered to be used heavily by offenders justifying the initiation of committing this type of crime and continuing to do so. The types of

neutralization that were most used by these criminals were denial of injury, denial of victim and appeal to higher loyalties (Holt et al, 2018:548).

Another aspect of this theory which is relevant to identity crime is the perception of victims by offenders. It is well known in the study of this phenomenon that victims are diffuse. Green (1990:79) argues that the criminal's denial of injury is more likely to occur when the victims are perceived as more diffuse.

Vold and Bernard (1986) argue that once illegal actions are committed, the offender would be "motivated to continue committing them because he has learned the moral (neutralization) necessary to consider himself guiltless, and because he has learned the technical means to carry out the offences".

Donal Horning (1970) in his study of employees of a large Midwestern electronics assembly plant discovered that over one-third did not consider stealing company property as theft. Erwin Smigel (1956) had similar findings in his investigation of attitudes toward stealing according to the victim company's size (small company, large company, or the government). Most of Smigel's respondents said that they would prefer to steal from larger businesses and from the government rather than from a small business.

Sykes and Matza's (1957) neutralization theory states that people who commit illegal acts, neutralize certain values within themselves which would normally prohibit them from carrying out such acts claiming that other conducts are 'far more harmful' an expression which is commonly used. Therefore, if these views can be challenged and altered it will have an impact on people committing this crime or on shortening the career of an identity criminal. It was evident from the above that this theory plays a significant role in offenders' reasoning and, therefore, it needs to be viewed in the context of devising prevention strategies (Holt et al, 2018:459; Kirwan and Power, 2013:23).

Anomie

Durkheim's (1938) anomie theory cites that social solidarity is the product of two things: integration and regulation. At the time of rapid social change, systems of social regulation may be insufficient causing a state of anomie. This was in some respect a critique of modern industrialisation and its failure in sustaining moral regulation. In such societies, individual ambitions, desires and appetites are stimulated but insufficiently controlled or limited. It can be argued that the same thing is happening now with the massive changes that technology is bringing about (Newburn, 2007:173; Lavorgna, 2020:36). The speed of technological change experienced in the last eighty years from the first programmable computer in 1938

called Zuse to the first portable PC in 1981 and finally to the first smartphone in 1992 has meant that our current world is constantly changing and the way we live our lives is evolving. The speed with which these changes are happening is making it difficult at times to keep up with them and although they are meant to bring society and people comfort and better ways of living, some unexpected negatives are also created as a result. Identity related crimes are one of these negatives. The development of the internet, the widespread adoption of social media platforms such as Facebook and Twitter have created a need for users to desire immediate attention and gratification which has eroded previous societal norms. The voluntary sharing of key personal identifiers and other personal contextual data on social networks along with the increasing need to use and transmit and store such information to access basic goods and services from both the private and public sector has proven to offer identity criminals ample opportunity to commit the crime. In addition, the breakdown of societal norms and moral discipline and the lack of effective regulation of the internet by authorities aid the identity criminals in their endeavours.

Strain theory

Another theory that contributes to the explanation of identity related crime is Robert Merton's strain theory. He believed that the absence of alignment between socially desired aspirations, such as wealth and the means available to people to achieve such objectives are the result of anomie (Newburn, 2007:175; Yar and Steinmetz, 2019:30-31; Lavorgna, 2020:37). He argued that the aspirations are socially learned and not being able to achieve such aspirations through legal means put pressure on individuals to explore and divert their attention to illegal means. Merton (1949:137) also pointed out that "a cardinal American virtue, ambition, promotes a cardinal American vice, deviant behaviour."

In the Copes and Vieraitis (2012) study the major motivator for the offenders was money. Nearly half of the offenders interviewed for this study came from middle-class backgrounds and used the money to maintain affluent lifestyles and, simply put, "trying to keep up with the Joneses". Basically, the reason for their offending was to provide them with a lifestyle that they could not obtain through other legal means.

As identity related crimes are very diverse in nature and by type of offender, the challenge is how to rally all different aspects when developing or utilising the existing theories to explain it. How can this diversity be best managed both in academic perspectives and practical management of this complex phenomenon? Burke (2006:186) states that the third way to assess and construct an explanation of crime and criminal behaviour is through theoretical integration. The objective of such an integrated approach would be to identify commonalities

in two or more theories to develop a synthesis that is superior to any one individual theory (Farnsworth, 1989). As Slapper and Tombs (1999:13) argue, one of the legitimate tasks of white-collar crime criminologists is to reshape the nature and boundaries of criminology while accepting the poverty of its dominant discourses, which to them are a sign of struggle, a practice that would also be very appropriate to the study of this crime. And although a set of categories and their definitions were provided above it should be noted that they are not, as Croall (2001:143) argues, watertight as they have many links with conventional, organised and white-collar crime.

Summary

The above captures the academic studies on offenders of this crime, highlighting approaches that can impact the root causes of this crime and assist in preventing or mitigating against it. This section started with criminal opportunity theory, routine activity approach, rational choice perspective and crime pattern theory and finally situational crime prevention theories which are more focused on the immediate environment of crime. They look at the motivation of the criminals. Neutralisation, anomie and strain theories, on the other hand, focus on the root causes of crime. Even with all these theories, it is clear that no single theory can explain all aspects of offenders of identity crime, especially hackers and the transnational organised groups. What is unclear is the extent to which victim support organisations/ institutions know their enemies. It begs the question “how can they fight them if they don’t know them?”

2.6. Committing different stages of identity crime

2.6.1 Identity theft

As previously established, there are two major elements to identity crime: identity theft and identity fraud. Identity theft is a precursor to identity fraud and where identity theft is an asymmetric phenomenon, identity fraud is symmetric (Wall, 2013a). There are many ways that each of these can be committed but the act of stealing identities is different to the act of carrying out the fraud or ‘cashing out’ which is the phrase widely used by the fraud practitioners to refer to the act of using the stolen identities for illegitimate gains. To this list a new form of identity crime against individuals can be added which includes social media related identity crime such as extortion, (blackmail), cyber-bullying (trolling) and even defamation (Wall, 2013a; Lavorgna, 2020).

There are a number of methods that criminals use to obtain personal information in order to

commit this crime. These methods are diverse and wide ranging in complexity (White and Fisher, 2008). Allison et al (2005) categorises identity theft into two types: low-technology and high-technology or off-line and on-line methods. Despite the general perception, old-fashioned, off-line identity methods play a more significant role in the commission of this crime (11% of fraud cases in 2008) according to Javelin (2009:7). There are significant differences between the online and off-line methods.

Off-line methods

Offline methods relate to those that do not use the internet to steal personal information. The various off-line methods that fraudsters can use to obtain personal information can be summarised as:

Via people in one's circle of trust: such as parents, family, friends, neighbours, colleagues or boss, landlord, employee and business associates (Cendrowski et al., 2007).

Burglaries: previously it was valuable items that thieves were after but now it is people's payment cards or card numbers that they seek to steal. One card's data has a street value between £250 and £500. In some instances, fraudsters work with subcontracted burglars (Newman, 2004).

Insider thieves: Fraudsters are on the lookout for people who work inside businesses where cards or card data are used to conduct transactions. The nature of such businesses usually means that employees are on low incomes, so the lucrative nature of the fraudsters' offer proves to be too good to miss (Archer et al., 2012:18). In some cases, fraudsters even lurk around the offices of such businesses very openly to recruit their staff for their identity crime objectives. In some instances, they even seek jobs in such businesses themselves (Hinde, 2005), these include bars, call centres and retail stores. Often, criminal gangs use threats to coerce employees to comply.

Dumpster diving: this is when the fraudster goes through people's rubbish in order to steal identifying information. It is one of the old-fashioned techniques but one that is still proving successful (Gerard et al, 2004; Archer et al., 2012:18).

Cash point: sophisticated methods to capture card data at ATM cash points. These attacks consist of using devices inside the cash machine to capture card data and hidden cameras to record the PIN (Onyesolu and Okpala, 2017).

The above summary highlights the many methods used by fraudsters to collect personal information and although some of these techniques are old-fashioned ways of stealing personal information they are still proving successful.

Online methods (cybercrime)

Online methods or cybercrime refer to those techniques that use the internet and the on-line world to steal consumer/corporate data. Stealing data through such means is increasing as more people are using this medium. Abubakr et al. (2016) lists the key facilitators of identity theft, quoted from the 2011 Javelin Strategy and Research study, as data breaches, personal information that is publicly displayed on social media sites and neglecting the security of smart phones. Given the rapid evolution of cyber-crime, it is not feasible to provide a comprehensive catalogue of crimeware technologies; nevertheless, several types of crimeware are discussed as representative of the species (Jacobson and Ramzan, 2008: 5). Hatch (2001:1472) emphasises that computers and technology have made information gathering cheap and easy. He also gives weight to the argument that online identity theft is a much bigger and more rapid threat compared to offline identity theft since it can be perpetrated by criminals anywhere in the world (Security Report Online Identity Theft, 2006). However, the internet is rapidly becoming the new frontier for most white-collar crime such as identity theft, especially with links to organised crime and drug rings (Cendrowski et al., 2007). The growth in online transactions has been paralleled by a surge in online identity theft (Walsh et al. 2016)

Malware (malicious software): is a technique used which is distributed by spammed email or by drive-by-downloads which infects the computer either looking for key financial information or keeping a log of victims' keystrokes (such as passwords) (Wall, 2010b).

Keyloggers and screen-scrapers: which are programs that monitor data being inputted into a computer (McCune et al. 2009).

Session Hijackers: In this kind of attack, a user's activities are monitored, typically by a malicious browser component, when the user logs into his or her account or initiates a transaction, the malicious software 'hijacks' the session to perform malicious actions, such as transferring money, once the user has legitimately established his or her credentials (Cremers et al., 2012).

Web trojans: These are malicious programs that pop up over login screens in an effort to collect credentials. When installed on a machine, the Trojan silently waits for a user to visit a particular website or set of websites then the trojan places a fake login window on top of the site's actual login window. The information that is being extracted is then transmitted to the attacker for misuse. Web trojans do not always duplicate the login window exactly. Sometimes they can add extra fields to the log-in window to collect more information. Trojans can be downloaded via common routes such as compromised web sites and email attachments (Security Report Online Identity Theft, 2006).

Transaction Generators (Rootkits): A transaction generator does not necessarily target an end user's computer, but rather typically targets a computer inside a transaction-processing centre such as a credit card processor. These programs also often intercept and compromise credit data. Transaction generators could potentially be installed on the end user's machine as well, which could be then implemented as some type of web browser extension or plug-in, which then modifies transaction details on the fly (Jackson et al, 2007).

System Reconfiguration attacks: System reconfiguration attacks, such as hostname look-up attacks and proxy attacks (a form of man-in-the middle attack), modify settings on a user's computer, which then cause information to be compromised (Damodaram, 2016).

Data Theft: One the techniques is used by criminals is malicious codes that can run on a user's machine and they can directly steal confidential data stored on the computer. Such data can include passwords, activation keys to software, sensitive correspondence and any other information that is stored on a victim's computer (Emigh, 2006).

Man-in-the-middle attacks: in this type of attack a fraudster is able to read, insert and modify at will, messages between two parties without either of them being aware that the link has been compromised (Security Report Online Identity Theft, 2006). More specifically a piece of malware is placed between the computer and the browser which infects the computer by a drive-by-download. So, on opening bank sites a false page is presented which requests additional identity information. The consumer will not suspect anything as Wall (2010b) argues. The significance of this method is that it "demonstrates a shift in the visibility of phishing patterns from overt to stealthy."

Phishing attacks: happen when fraudsters send random emails to consumers, pretending to be from major companies such as banks, in order to deceive them and obtain their identifying information. Worryingly, almost half of women and half of 16 to 24-year olds in the UK do not know what phishing is (Security Report Online Identity Theft, 2006). Spear phishing is a similar but a more targeted and tactical technique where highly personalised emails are sent to specific targets which increases response rate (Wall 2013a).

Botnets and compromised PCs: are also used in cyber-crime. In some cases, fraudsters use PCs as part of a large network of computers used to send phishing emails or Denial of Service (DoS) attacks (Security Report Online Identity Theft, 2006). DoS is an interruption in an authorised user's access to a computer network.

Smishing: which is a relatively new technique, where a text message is sent to potential victims containing the same message as phishing emails. In these messages the recipient is asked to reconfirm security information by SMS messages containing important identity information. 'Vishing' is the VOIP (Voice Over Internet Protocol) which is similar to phishing and smishing the only difference is that a voice message is used to extract information from potential victims (Wall, 2007).

Hacking: The hackers break into the systems of companies which have less secure databases or websites. The data is then sold in specific chat rooms that fraudsters use. Just like the fraud prevention community, fraudsters have forums where they can share information and maximise their illegitimate business. The data that are sold on such sites are mainly payment card data which are then used to make purchases on-line (Yar and Steinmetz, 2019:61) .

Chat rooms: chat rooms and social media sites such as Facebook and Twitter are used to acquire data (Villar-Rodriguez et al., 2016) and have become breeding ground for identity thieves (Irshad and Soomro, 2018).

Tapping into the wireless networks of retailers: is another method used by fraudsters. They achieve this by simply positioning themselves close to the stores. Often these are open networks (such as Starbucks) which have no protection/encryption hence data can be easily stolen (Hunt, 2017).

Data breaches: are very common at the moment. Hardly any day passes without a company losing consumer data to hackers or due to negligence. This is mainly caused by the data that has been entrusted to these organisations by consumers not

being protected properly. Reports published by the Identity Theft Resource Centre and Cyber-Scout indicate that the number of data breaches increased in 2017 by almost a third from the previous year rising from 1,000 in 2016 to 1,300 in 2017 (IDTRC, 2017).

Usage of over-simple passwords and failure to change the passwords regularly are other vulnerabilities that thieves exploit (Security Report Online Identity Theft, 2006). It is believed that 61% of computer owners use one main password wherever possible which will mean that once a criminal has gained access to one account s/he can access the rest (ibid).

Obtaining one set of account details enables the fraudster to defraud others such as in the instances of online auction sites (ibid). Wall (2018) refers to what is known as composite personal profile where different data parts of the stolen data which are within different stolen data batches are connected and a much fuller identity is made for a far more effective abuse. The stolen data using the various methods mentioned above are then sold on various websites or through criminal networks.

The discussion above further highlights the significant contribution that cyber activity and cybercrime make to identity related crimes. In fact, a large part of identity crimes has a cyber element to it. Analysing cybercrime has also been hindered by lack of systemic or official data available (Yar and Steinmetz, 2019:19) and although this topic has increasingly been debated, our understanding of it has been obscured by political and media discussions. To provide some clarity the Office for National Statistics on Crime in England and Wales made provisions to measure cybercrime. In 2017, 7% of people were targeted with 72% of victims subjected to bank and credit account fraud, 25.1% to consumer and retail fraud, 1.9% to advance fraud and 1.1% to other forms of fraud (ONS, 2018b). As cybercrime is only a part of general identity crimes, this data does not provide us with a full and accurate picture, however, it provides an indicator of the cyber element of this crime.

2.6.2. Committing fraud on stolen identities

Once data is stolen in most cases the culprits misuse that data for personal gain. However, this is not always the case. Some criminals may use the stolen data just to avoid being caught by law enforcement or in order to access jobs that they may not be able to secure with their own tarnished identity.

Obtaining services

Wall (2013a) provides a typology for the second aspect of this crime dividing it to 4 permutations: individual to individual, individual to business, business to individual and finally business to business.

Once the criminals obtain personal data, they use it to acquire services such as State Benefit and/ or hospital care. Some criminals use stolen identities of infants to apply for Social Security Numbers for them, eventually, opening bank accounts for them, filing tax returns, registering them to vote, and applying for credit cards in their name. After 25 years they then have a handful of identities ready and waiting for some real people to step into and misuse. This technique is known as identity farming but according to Wall (ibid) the days of this technique are over.

Acquiring goods and products

The second part of committing this crime is the illegal use of the stolen data which also has many manifestations. Perl (2003) identifies three different types of identity fraud: financial, non-financial and criminal record. He argues that financial identity fraud (although he refers to it as identity theft) occurs when the identity criminal uses a victim's personal information to withdraw money from a victim's bank account or open a new bank account, credit card, or other line of credit in the victim's name. Non-financial identity fraud occurs when the thief uses the victim's information to obtain health benefits, to commit telecommunications or utilities fraud, or to receive some other service. Perl states that criminal record identity fraud occurs when the thief commits crimes, traffic violations, or other illegal activities while acting as the victim. When arrested the thief provides the victim's information and the criminal record (and conviction) are attached to the victim not the fraudster. Poore (2001) further elaborates on this point made by Perl arguing that identity fraud is not just for gain. A perpetrator can also introduce false information into records associated with an individual to cause them harm which, if detected late, may enter various and numerous databases. As a result, a large amount of time may be needed to amend the false profiles.

Avoiding arrest

Finally, some criminals use stolen or created identities to avoid arrest or use them to travel to other countries without being noticed by the police or the border agencies. This has been more prevalent in the USA, to the extent the Attorney General's Office provides a service

where victims of identity theft can present their passports to law enforcement agencies to help prevent arrest for offences committed by someone using stolen information.

A brief look at Action Fraud UK (2018), in the News and Alerts section, reveals a list of recent fraudulent methods of which the public need to be aware. By looking at this list it could truly be said that this crime is out of control. Some of the recent attempts include fraudsters targeting university staff in a pay rise scam along with police, government employees and NHS members being targeted by a tax rebate scam and identity fraud victims from internet dating websites being reported at the rate of one every 3 hours, medical practices targeted by CEO fraud, HMRC and Apple gift card fraud, social media used to harvest fake charity donations, and 'migrant helpline' phishing emails leading to Ramnit malware which is a computer worm affecting windows users.

What is constant is the misuse of identity information but the ways that fraudsters abuse this data to acquire goods and services changes significantly. They are very good at using world events (such as the migrant crisis and other disasters) and special events (such as Valentine's Day or Christmas) to deceive people and persuade them to part with their personal data.

One of the newest types of identity related crimes is the online romance scam which came to light in 2008. There have been warnings that this type of fraud is reaching about half of the British population and efforts need to be made to raise awareness about this new MO. In this scam the fraudsters initiate a relationship with the victim through online dating sites. They then defraud them of large sums of money. In a study undertaken by Whitty and Buchanan (2012) it was revealed that despite the newness of this fraud 230,000 British citizens may have fallen victim. Victims receive a double hit, the loss of money and the loss of the relationship. Action Fraud believes that this crime is under reported and that there are many more victims.

To illustrate identity crime more clearly, two real-life examples of identity crime can be used. In 2014, Theophillus Madekurozwe stole letters from unlocked mailboxes at blocks of flats and the identities inside enabled him to obtain a series of credit cards with available credit of £113,000. He then used the bank cards to buy high value gift cards which funded a massive spending spree on designer goods including iPad tablets iMac laptops and high-end tech goods. He almost managed to escape because he spent the gift cards in stores where he had not obtained them. He was apprehended and jailed (Scheerhout, 2014).

In what was deemed UK's worst case of identity crime at the time, a British man had his passport stolen and then used with a different photograph to set up a communications company in the Isle of Man. The company was fined for breaching codes of practice and as the company was in the victim's name, it was he who was facing a £34,000 court order and unpaid VAT totalling more than £110,000. The prolonged battle against the tax authorities to clear his name fully took him three years (Winch, 2013).

Wall (2013a) in his study of this crime refers to "new forms of identity crime" stating that social networking media closes the gap between online and off-line identities and identifiers helping criminals to exploit these new forms of identities that didn't exist before. Social friendship identity, citizenship identity, financial identity, professional identity, organisational identity, sexual identity and geographic identity. Reputation is increasingly becoming more of a value, exploiting networks, one's identity and reputation within them.

2.7. Identity crime offenders and relevant literature

As Identity crime offending is remarkably diverse, it is unlikely that one single criminological theory will suffice to explain all aspects of the offenders' behaviour and motivation. So, to find the most suitable theory for each type of offence/offender/modus operandi, it is best to examine what theories may be most relevant. As Williams and McShane (2010:1) stated it is best to employ a theoretical perspective which is the product of a scientific approach which has been utilised to explain criminal behaviour. Notwithstanding this, there is very limited data available on offenders of identity crime. One of the few studies that was undertaken for the University of Wisconsin by Alison et al. (2005) determined that most offenders of identity crime were female (63%) and African American (69%) and nearly half were unemployed. It is also believed that identity criminals range from disgruntled teenagers experimenting with hacking tools to sophisticated organised crime rings targeting specific organisations or information (Gordan, 2006).

The diversity of identity criminals was further captured by another study undertaken by Copes and Vieraitis (2012:90, 92) where 59 identity crime offenders were interviewed, the majority of which had at least some college education. Their primary motivation for instigating these crimes was money, stating that identity crime can be richly and quickly rewarding, however, 11 of these offenders stated identity crime as being fun and exciting and 3 of them used it to hide from law enforcement.

As far as perceptions of risk are concerned, three different perceptions of risk were listed in this research by (ibid:95). Firstly, fraudsters believed that by relying on their skill they could

stay one step ahead of the law. Secondly, they saw their crimes as being easy and, finally, they did not have faith in the ability of police to catch them. These criminals used a number of strategies to obtain identity information, however, the most common method was to buy it (ibid:96-97). They all used more than one technique when cashing in on their identities, but the preferred strategy was to apply for credit cards (ibid:99).

In another study Copes et al. (2013) explore the various justifications and excuses used by identity thieves. The participants provided numerous accounts for their crimes, with denial of injury being the most common. They also discovered that the use of accounts varied by the type of lifestyles these offenders lived. Those seeking to live as conventional citizens call forth different accounts than those who have a criminal lifestyle. Additionally, conventional offenders made use of both excuses and justifications in their accounts of their crimes, but seemed to show a preference for excuses, especially when compared to the street offenders interviewed. “Those in groups were more likely to blame others than those who worked alone” (ibid).

Copes and Vieraitis (2012:66) in their study of convicted identity criminals cited three organisational systems that identity criminals use to carry out their crimes: loners, street-level identity theft (SLIT) rings and occupational teams. The loners have the least sophisticated form of organization and commit their crimes predominately on their own. This group represented 24% of the offenders interviewed by authors. The SLITs had a hierarchical structure although the structure is looser than other organised crime syndicates. Although some SLIT members were working in legitimate employment “the primary context in which they accomplished their crimes was the street’’. This group represented 57% of the total group. The occupational teams, who represented 18% of the group, were largely employed in legitimate jobs and used their work to commit identity crimes. The teams consisted of a ringleader, victim identity sources, runners, and credit verifiers. In most cases, these roles were filled by in-house personnel.

To illustrate the different types of offenders and groups it is best to look at some real examples of identity thieves. Kenneth Gibson was a 47-year-old Information Technology (IT) professional who between 2012 and 2017 stole thousands of employee and customer data from his work place (The Associated Press, 2018). Over time, he opened 8,000 unauthorised PayPal accounts with the stolen identities and opened credit accounts linked to those PayPal accounts, withdrawing money from them. He stole $3.5 million in total.

In 2001, Abraham Abdallah, a notorious identity criminal, accessed the bank accounts of 217 celebrities such as Steven Spielberg, Oprah Winfrey and Warren Buffet (Leyden, 2001). He stole $22 million from his victims. He committed his crimes by accessing the Internet using a public library computer and his excellent social skills to charm bank employees and others so that he could gather the information needed to access the accounts. Unlike Gibson, Abdullah was a trainee dishwasher and did not have access to his victims' personal and financial information through his employment.

One final example is an identity fraud ring, consisting of eight members, who stole children's identities (Identity force, 2018). They stole the social security numbers of children as young as 11 and opened bank accounts in their names. Through their crimes they stole $420,000.

Occupational identity criminals

The first to consider would be the literature surrounding occupational identity criminals. Being inside an organisation, public or private, usually offers the employee or contractor particular access to assets, including data and therein often increasingly valuable personal data which is the seed-corn of identity crime. This fact is not lost on potential identity thieves who if the opportunity presents itself with calculable and acceptable risks/reward levels may steal identity data. Therefore, an analysis of the theory and behaviour of the occupation-based criminal is relevant to this study. In this context, the most relevant theory to explain occupational identity related criminality is white-collar crime. The phrase white-collar crime was introduced to the sociological and criminological world by the seminal work of Edwin Sutherland (1940) who defined this crime as "crimes committed by persons of respectability and high social status in the course of their occupation" (Sutherland,1983:8). Dearden (2017) and Fuss and Hecker (2008) state that a typical profile of a white-collar criminal is defined as someone with high social status, considerable influence and access to resources and Wheeler et al (1982:642) define white-collar crime as "economic offences committed through the use of some combination of fraud, deception or collusion".

Sutherland's theory was received with criticism by some academics. The first criticism was the legal status of white-collar offences. As Sutherland's approach included acts that had been sanctioned through civil or administrative legal procedures, it provoked extensive criticism from legal scholars who argued only acts that are punishable by criminal law can be called crimes (Tappan,1947). The other point of contention was whether the offenders' social status should be a defining characteristic of white-collar crime. An example to illustrate this point is a top corporate executive and a typist who both have access to insider information

about their company's stock value increase, who then purchase the stock and commit insider trading (Benson and Simpson, 2015:9-11). Geis and Jesilow (1993) point out that some types of white-collar crime may be committed by secretaries or truck drivers, as well as by high-ranking officials or presidents within the same organisation.

Although Sutherland's original definition has been surrounded by controversy, the fundamental elements of his definition capture the nature of white-collar identity related crimes very well. One of these elements refers to the "violation of delegated or implied trust" by professionals. As has been discussed, the data entrusted to some of the identity thieves who hold legal employment with companies is heavily present. Sutherland's (1940) other assertion is that "the financial cost of white-collar crime is probably several times as great as the financial cost of all the crimes which are customarily regarded as the crime problem". In addition to the financial loss itself, insider identity crime has a significantly negative effect on an organisation's reputation and the loss of customer confidence resulting in loss of future sales which can be terminal for some companies. Sutherland's further assertion that agencies other than the criminal courts should be included in the fight against white-collar crime, as in the case of identity related crimes, is evidenced by the creation and the power of the ICO which issues fines rather than convictions when data has not being properly protected by organisations.

Even though Sutherland's (1940) definition was "possibly the most significant recent development in criminology" (Taft and England, 1964:199) it still created "confusion over the meaning of the term because he did not clearly specify the behaviour that constituted white-collar crime or the individuals or groups that could be considered white-collar criminals" (Robin, 1974). Susan Shapiro (1990) believed that, in order to combat the issue of defining white-collar crime, we should "collar the crime, not the criminal" and therefore shift the focus to the crime itself and not the criminal. Shover and Cullen (2008) elaborate further on the principal of white-collar crime by dividing the different paradigms into populist and patrician; populist, referring to the work of Sutherland, defines the characteristics of white-collar crime as the respectable states of its perpetrators. The patrician camp on the other hand emphasises the characteristics of the crime itself.

Another theory introduced by Seminal work of Sutherland (1947) which is relevant top this study is the differential association theory which was "one of the first articulation of the learning processes that contributed to understanding the commission of crime" (Yar and Steinmetz, 2019: 28-29). This was expanded and refined to social learning theory that emphasises crimes being committed when those acts have been positively reinforced (ibid;

Holt et al. 2018: 444-445).

Since Sutherland's white-collar crime definition, a number of criminologists have attempted to clarify and re-examine the generalisations that were made by Sutherland in his subsequent book published in 1949. One of these theories is introduced by Clinard and Quinney (1973) who were the first to focus on occupational criminal opportunity when they abandoned the concept of white-collar crime and categorised occupational crime into two groups: corporate crimes which are crimes committed for the benefit of an employing organisation and occupational crimes which are crimes committed in the course of occupation that directly benefit the offender.

Green (1997:17-19) took these theories and notions further by categorising occupational crime to four main types: organisational occupational crime which are crimes committed for the benefit of the employing organisation. State authority occupational crime consisting of crimes by officials through the exercise of their state- based authority. Professional occupational crime are crimes committed by professionals in their capacity as professionals and finally, individual occupational crime which are crimes by individuals as individuals.

Green (Ibid:16) believes that "the criterion of a legal occupation is necessary, because without it, occupational crime could conceivably include all crimes. A legal occupation is simply one that does not, itself, violate any laws. Thus, the term would exclude persons with occupations that are illegal to begin with such as organised criminals or bank robbers. Robin (1974) further describes occupational crime as "any act punishable by law that is committed through opportunity created in the course of an occupation that is legal".

Trahan (2011) made a distinction between white-collar criminals who commit financial crime for personal gain (occupational crime) and those who commit it for their employer (corporate crime). "Although occupational crime can be treated as distinctive because it is based on opportunities at the place of work, there is no single theory that can satisfactorily explain why all occupational criminals behave the way they do" (Green,1990:57). This is particularly true of identity related crimes. Benson and Simpson (2015) further examine occupational crime using three characteristics: the offender has lawful and legitimate access to the premises and systems where crime is committed, the offender is geographically separated from his victim and when criminal acts appear to be legitimate business.

Occupational crime covers all the instances where employees of different organisations either willingly or by the coercion of fraudsters have stolen data from their respective

employer to commit identity crime. It is certain that identity crime has an element of occupational crime. The assertion that part of identity related offenders/ offending is a type of white-collar crime is further supported by writers such as Sharp et al. (2004). Croall (1992: 271) in her examination of white-collar crime provides a list of characteristics associated with this type of crime most of which are applicable to identity related crimes.

A brief review of statistics from the Information Commissioner's Office (2018) reveals that in the first half of 2018 there have been 11 prosecutions (mostly professional individuals) but the punishments have been restricted to fines rather than custodial sentences. This illustrates another of the characteristics of white-collar crime, leniency towards offenders on the part of law enforcement agencies (Mann,1989) supported by the Identity Theft Resources Centre (2003:6) which reports that the treatment of offenders tends to be lenient. Identity theft is a high profit, low risk, and low penalty crime. As Green states (1990:65-66), being caught for stealing company property, such as data for use in identity fraud, may involve a minimal formal sanction (a short time in jail or a fine) or perhaps no formal sanction at all. However, the informal sanctions may be more severe for the thief including the loss of their job, failure to receive a recommendation for future employment, removal from the group of co-workers with whom social activities may have been a source of enjoyment, shame among family and friends and character defamation through other's gossip. In order to address the issues inherent in this area the recent GDPR rules that came into force on 25th of May 2018, impose the biggest fines levied upon businesses of up to €20 million (£17.6 million) or 4% of global annual turnover (whichever is higher) should organisations be found negligent by failing to protect personal and identity data. Previously, penalties imposed on companies that did not comply with the UK's Data Protection Act 1998 would be charged a maximum of £500,000 if they leaked data or failed to protect the data they hold against potential hacks.

The other relevant assertion made by Sutherland is the vulnerability of white-collar crime victims. When consumers have to share their identifying information with various organisations in order to access goods and services, they have very little (almost zero) control over what happens to that information, and the extent to which it is protected. When the stolen identity data is used illegally, the general belief of the organisations dealing with the individual victims (Action Fraud, 2018) is that the problem is not actually that of the victim, but rather it belongs to the business or organisation that has been defrauded. This has caused a lack of visibility for identity crime victims. The reaction of the organisations involved is to refund the victims and pretend that nothing has happened so that their reputations are not affected. It is for these reasons that the identity related criminals are

enjoying ‘relative immunity’ compared to other types of crime. White-collar offenders are often arrested much later in the investigative process than street criminals because of the complexity of this type of crime and the difficulty in identifying the victims (Braithwaite and Geise, 1982).

Identity related crimes have two parts to them as discussed in earlier chapters, the first part being the theft of the data and the second part being the misuse of the stolen data to commit fraud. Employees’ theft of consumer data to fuel identity fraud happens in three instances: when an employee steals data through their own greed, when outsiders (mainly organised gangs) persuade employees to steal personal data and finally when the employee or his/her family are threatened by the organised gangs to steal the data. Gottschalk (2017) said that white-collar criminals are not acting alone when committing financial crime whether they have external or internal help. This is applicable to identity related crimes as in some cases the insiders work with organised gangs or others in carrying out identity related crimes.

Gibbons (1973) discovered that occupational property theft was undertaken to sustain standards of living for which legitimate income was insufficient. Nettler’s (1974) argued that “desire and opportunity generate theft more frequently in these instances than does a financial difficulty”.

In one of the typologies provided by Punch (1996:56-57) he states that “employee deviance against the organization such as stealing is often viewed as being largely confined to lower levels.” ‘Private Justice’ is often applied in order to protect the reputation of the business. Passas (2009:153) for instance, argues that pressure to attain goals is constantly experienced by people in the upper social reaches, and that therefore “they are far from immune to pressures towards deviance”. Identity crime perpetrators, however, hold various positions within organizations. They range from being a director, consultant to general workers or independent traders.

Another theory that lends itself suitably to explaining crimes of employees is that of Burns and Stalker (1961) and his description of ‘organic’ and ‘mechanistic’ organisations. Mechanistic organisations operate in conditions of relative stability while organic organisations adapt swiftly to changing conditions. Both scenarios offer different risk and opportunity profiles. Punch (1996:2) argues that the culture of competition in organisations provides opportunities, motivations and rationalizations for rule-breakers.

Ruggiero (2015:23) goes on to explain that “as organisations become more complex, responsibilities are decentralized, such that their human components find themselves

inhabiting an increasingly opaque environment in which the goals to pursue and the modalities through which one is expected to pursue them become vague and negotiable." Ruggiero (ibid) further argues that the settings within which the elite operate are already normless, and further dilution of norms in the workplace encourages experimental conduct allowing for the arbitrary expression of practices.

SLITs (Street Level Identity Thieves) / career criminals

The SLITs are typified as having lengthy criminal records and being actively involved in street life. Even though some hold legitimate employment, their demographic profile is similar to street criminals. These groups use various methods to acquire identity information such as pickpocketing, going through mailboxes and using acquaintances in jobs with access to consumer data.

Wheeler et al. (1991) in their study of white-collar offenders discovered similar trends in terms of criminals prior offending. Their findings showed that 46% of credit fraudsters have prior convictions. Additionally, more than a quarter of those convicted of credit fraud, fake claims and mail fraud had prior felony convictions and a fifth of them spent substantial periods of time behind bars. The same pattern of offending was also evident in the Wheeler et al. (1982) study. They observed that in the case of credit fraud, false claims and mail fraud violators, four out of ten offenders had two or more prior arrests and three in ten had four or more prior arrests on their record.

Both types of offenders demonstrate the characteristics of career criminals. 'Criminal careers' is a relatively new concept introduced by the National Academy of Sciences' (NAS) Criminal Careers and Career Criminals (Blumstein et al, 1986). Neoclassical theory in criminology introduced the viewpoint that criminals had the motivation, will and cognitive capacities to choose to be a chronic, professional or career criminal (Cornish and Clarke, 1986; Edelstein, 2016).

Edelstein (2016) cites career criminality as a 'career of 'serial criminality' designed to gain material rewards, which can also provide the perpetrator with psychological, physical, social and other rewards. He then offers a new definition of 'career criminal' to distinguish it from other kinds of criminals such as 'professional criminals' and 'chronic offenders'. Secondly, he proposes to distinguish between different kinds of criminals by two criteria: professionalism and primary motive. Thirdly, the essay proposes to distinguish between two subcategories of professional criminals according to their primary motive. From this perspective, professional

criminals whose primary motive is pathological cannot be considered career criminals. On the other hand, those who act for material motives are career criminals.

As already cited, the largest number of identity criminals belonged to this SLIT group. Wolfgang et al. (1972) argued that a small percentage of criminals were responsible for most of the offences, and thus called for a focus on career criminals in order to bring a drop in crimes committed in society. Edelstein (2016) argues that “the career criminals are the rarest. The chances that we recognise them on the way home are minimal but they cause great damage in society.” Blumestein et al, (1986) goes further by identifying four key dimensions of career criminals: participation, frequency, seriousness and length. There has been a lot of criticism towards the criminal career paradigm such as Sampson and Laub (2016:323) who state that it “did not provide a coherent explanatory framework”. This assertion is supported by Gottfredson and Hirschi (1990) when they call the perspective atheoretical.

There are several different elements recognised as central to defining a professional career criminal. The four most prominent ones are: the different phases of the criminal career, including learning and specialization (Farrington, 1997). Others emphasize the connection between professional criminals and career criminals (Clinard & Quinney 1973). Others link careers and recidivism in crime (Blumstein et al, 1986; De Lisi, 2005); others take into account the motive of material gain in a criminal career (Davis, 2001). From the Copes and Vieraitis (2012:124) study it was evident that identity criminals, by developing a sense of professionalism and refining their skills in acquiring information, converting it to cash or goods, and avoiding arrest, increased their chances of being successful at crime. Also, as Eldestein (2016) stated, there are two conditions necessary to identify or label a criminal as a career criminal, that is material motives and professionalism and both of these were heavily present amongst identity thieves.

As Wheeler et al. (1991) argue, identity related criminals are not those upper-class or elite criminals ordinarily associated with white-collar crime. But neither are they similar to the street criminals who have received the bulk of criminological attention. For this reason, he calls for a re-evaluation of criminal justice policy with these offenders in mind.

The loners

Copes and Vieraitis (2012:66) third group of convicted identity crime offenders are the 'loner' which makes up 18% of the study. The loner can be represented by two potentially different identity crime actors. Those who commit the crime alone who could also be persistent career criminals, and those that commit this crime when an opportunity presents itself.

In this section the diversity of identity related criminals was stressed ranging from organised professional groups with professional jobs, to career criminals with lengthy criminal records active in street life and finally, those that commit the crime alone. The criminological theories that can be applied to this crime are equally diverse and range from Sutherland's (1983) white-collar crime theory of respectable individuals with high social status to Clinard and Quinney's (1973) occupational criminals and Green's (1977) categorisation of occupational crime. Wheeler et al. (1991), Blumstein et al. (1986) and Edelstein (2016) on the other hand focus on explaining career and serial criminality. Having examined the offenders of this crime in the next section I will then examine the literature on victims of this crime.

2.8. Victims of identity crimes

Very little is known about the victims of this type of crime but the scarce literature on the issue indicates that the victims of this crime are very different to victims of conventional crimes as they tend to be older and an equal number of men and women tend to fall victim to this crime (Golladay, 2017) The limited existing literature and data predominantly focuses on consumers and the impact that this type of crime has on them with some observers commenting that these crimes might have different impacts on populations (Goel, 2018). Pontell et al (2008:79) state that the victimisation of identity crime victims differs from that of many traditional forms of common and white-collar crime in that this crime is repetitive over time, the victim may or may not be aware of it while it is happening, and it continues to have harmful impacts during the period in which victims re-establish their financial identities. Although victims are not typically held responsible for the fraudulent charges that result from identity crime, the costs for victims far exceed the monetary losses of the crime. This crime costs consumers both time and money spent defending themselves. These costs include those for certified mail, photocopying, telephone calls, lost time at work, and lost vacation time. Victims of identity crime can also experience a range of emotional states that mirror post-traumatic stress disorder, including denial, anger, guilt, shame and embarrassment, fear and a feeling of being violated (Foley, 2003). Hemphill (2001) believes that the victims of identity crime are being victimised twice, first by the thief and second by the private sector. Because of the nature of identity crimes, the crime and victimisation can go undetected

therefore making it an invisible offence. The anonymous nature of the crime presents significant problems for police; as many as half of victims do not know how their personal information was obtained (Synovate, 2003).

Victims generally find out about their victimisation in one of three ways: They are at a critical point in their lives (e.g. applying for a job, mortgage or loan) and are denied something; they receive negative notification (e.g. discover fraudulent charges on their statements or are contacted by collection agencies); or they are notified through proactive business practices (Foley, 2003). Recent research suggests that more than 80% of victims discover the theft through a negative experience, not through proactive business practices (ibid). There is also a time-delay challenge associated with discovery (Harrell, 2015). Foley (2003) reported that slightly fewer than half of identity crime victims reported that they discovered the crime within 3 months, but one quarter did not find out about the theft until 2 years after the original use of the information. Synovate (2003), however, believes that the discovery length is related to the type of crime committed for example, credit card fraud is more likely to be discovered earlier than new accounts or other types of fraud. Another concept was introduced by Lacey et al. (2016) of victim-enabled identity theft, describing it as only being successful when the individual concerned participates in the compromise of their own identity information through an action they have been deceived into performing.

There is also little research conducted on the impact that this type of crime has on organisations. Financial services firms, operating in a complex social and economic environment, are exposed to several risks as a result of identity crime. Kerbsbach (2004:22) observes that financial firms are charged with the difficult challenge of increased responsibility to protect their customers, but they face greater pressure to defend their own bottom line. These financial service providers seem to be the only organisations acknowledged to be the sufferers or influencers of identity crime, but it should also be considered that there are other entities (such as public organisations and other private firms) that can equally be victims or facilitators of this type of crime. Therefore, this research will aim to provide a more holistic picture of victims and the ways and extent to which they are victimised and the organisations and resources available to victims to recover from identity crime. In doing so, it will also list the different organisations and institutions that are impacted by identity crime and the extent to which these organisations know their victims and whether the strategies employed to advise their customers are based on informed decisions. With so little information available publicly, it begs the questions, do they possess any understanding and knowledge about their victims and can the data available on victims be used to improve

defences against identity crime? Their services and support (if they have any) are directed at victims, so are they devised based on a thorough knowledge of the affected group?

Wall (2013a) presents a view which is more concerned about the victims by stating that new law is required to help victims of this crime. Furthermore, he asks for better management of public expectations through more public knowledge, better training for criminal justice agencies and clearer procedures.

2.9. Tackling the issue

An examination of the literature with respect to tackling and preventing identity crime highlights the directions that the academic influencers have taken. There are, however, two main emerging thought patterns which make a distinction between the technological and human elements when examining this area. Some, for example, have criticised the systems and their reliance on human beings spotting irregularities (Walton, 2005). Others have basically argued that these technologies which have been used to create and utilise identities are ill-matched to the economics and uses of identities (Camp, 2007:2). McNally and Newman (2009:21) express a more positive view recognising the vital role of technology both in providing opportunities for offenders and in providing techniques to prevent them from committing this crime. They highlight the weaknesses inherent in information systems and emphasise the fact that these systems need humans to manage them who themselves are prone to weaknesses, in addition to making mistakes, as major vulnerabilities. Furthermore, Newman (ibid:24) states that the emerging technologies and old technologies serve to provide signposts as to where or how identity thieves will strike next. Wall (2013b) is also of the belief that the same technology that is enabling identity crime can be used to provide the potential for regulation.

Pontel et al. (2008:79) and Vuckovic et al. (2018) call for public education campaigns to create individual awareness regarding the importance of securing personal data and responsible computer use. Pontel et al. (2008:79) at the same time, sees a need for better regulatory policy aimed at protecting information in public and proprietary databases that are not within individual control, in addition to Situational Crime Prevention (SCP) techniques that cover a much broader terrain than usual in order to be effective (ibid:81). The importance of individuals protecting their personal information is also supported by Newman (2004).

This view was rejected by Reyns and Henson (2016) who in their study of online victimisation discovered that online exposures, such as banking and purchasing, positively and significantly contributed to online identity theft. In addition, hacking and phishing, which both reflect the concept of online proximity, were found to have increased the likelihood of online identity theft. They also discovered that personal guardianship strategies to prevent identity theft victimisation seemed ineffective at reducing it.

Newman (2009) suggests that “criminal justice policy should be directed at 1) collecting information which informs us how these crimes are carried out 2) cataloguing opportunities made available to thieves (or likely to be invented by innovative thieves) through new technologies, business practices, and victim behaviour and 3) identifying significant players who can develop intervention that will reduce such opportunities”.

McNally (2008:50) states that although data enables us to develop a sense of identity crime, more detailed information needs to be collected about the “sequence of events involved at each stage and the interactions among various types of actors and props over time”. She (ibid:51) argues that identity crime can only be prevented one problem at a time, that there is a need for stopping and thinking before moving forward and a need for a universal map.

Newman (2009) agrees with Pontel et al. (2008:79) when he draws attention to the responsibility of businesses and individuals by calling for a campaign to convince them to put in place situational crime prevention measures and standard security procedures that typically harden targets, control access to information, and specially design products and services with the anticipation of how they could be exploited by identity thieves. This is presented as an on-going challenge requiring persistent and long-term commitment from businesses and individuals (Newman, 2009).

Cho and Lee (2016) argue that although the organisations or companies have made tremendous efforts by investing in security solutions to prevent information leakage and industrial system hacking, their practical effects are insufficient, and enhanced threats of both hacking and information leakage are also increasing consistently.

Cassim (2015) in his examination of identity crime and in his recommendations for preventing and addressing it provides a more holistic approach that would consist of raising awareness for both business (of their responsibility to protect employee and client records) and individuals and consumers about educating them to protect their personal information (offline and online). He emphasises forming alliances between different law enforcement

agencies and creating collaboration between governments and other service organisations to protect the personal information of private individuals and public bodies. He then focuses on providing assistance to victims of this crime by advising them of their rights and devising a plan to prevent or minimise the harm of identity theft when large identity databases have been breached. Abubakar et al (2016) broadly agree stating that identity theft cannot be solved by technology or law alone, it is a problem that needs a better strategy of managing complex networking systems where trust and privacy are not to be put at risk.

There have been suggestions (Newman, 2009:21; Archer et al, 2012; White and Fisher, 2008; Newman and McNally, 2010) to utilise situational crime prevention (SCP) techniques which are concerned with reducing criminal opportunities in tackling identity crime. As this research examines this crime from the perspective of the organisations tackling/ being impacted by it, SCP is one of the main central theories that will be used. Berg (2008) supports this view in her examination of identity theft through information technology by applying eight selected techniques of SCP methods to demonstrate ways it can be used positively in identity theft prevention. She states that situational crime prevention techniques are often used in organisational contexts but when it comes to computer–based incidents, individuals can also implement many of the measures and techniques. She further argues that government agencies and research institutions need to step in and ask victims some important questions that will not only find out how this crime has affected them, but also discover what behaviours and attitudes may have contributed to their victimisation. Prevention and education programs can then be focused on specific population groups and tailored to what they need to learn the most (ibid:165).

Willison (2008:171) on the other hand acknowledges the lack of theory in information system security literature but states that the “goals of IS security align themselves closely with those of SCP and each offer value and benefits to the other”. He calls for a need to address the problems posed by employee computer crime and a socio-technical approach to IS security (ibid:186).

Kirk (2014) brings the focus to strengthening the law enforcement response along with improving and strengthening systems, and at the same time changing habits and reducing complacency. The law enforcement response is difficult. In the UK it would be fair to say that there has been little law enforcement action. He continues that the government has woken up to this fact and has introduced measures and initiatives to change this shortcoming but despite these efforts, only 3 percent of cases involving cybercrime are reported to NFIB (National Fraud Intelligence Bureau) and from that very little investigation has been

undertaken by law enforcement. Graves and Sexton's (2016) emphasis is on sanctions in dealing with this crime by stipulating that the cost of lowering the amount of identity theft to some specified level can be reduced by substituting tougher sanctions for costly detection efforts. Soomro et al. (2016) raise a very important point by highlighting that in order for an effective functionality assessment of identity theft prevention measures, systems need to be assessed for their vulnerability. The lack of evaluation of identity theft prevention measures in mobile commerce resulted in implementation of these measures without knowing or testing their effectiveness. This was only possible after the event by an examination of the mobile commerce identity theft prevention strategies in UK by Shah et al (2019).

The above body of work highlights the academic recommendations for tackling this crime which covers a broad spectrum of topics ranging from technical approaches, SCP techniques and educational programs, but to what extent have these recommendations been utilised by the various organisations at the forefront of tackling this issue? And what challenges do these institutions face when implementing their strategies to fight this crime? Secondly, are SCPs the only methods or the only prominent methods that they are employing in their fight against identity crime? Additionally, in order to examine the methods, they are using to reduce this crime, it is imperative to look at how they perceive this crime.

2.9.1. Partnership approaches to tackle identity crime

In his observations of the developments in the last few decades, Tilley (2002), has categorized crime prevention into three overlapping periods. The first from 1970 to 1990 was a period in which crime prevention initiatives and activities were acknowledged as a valid and serious endeavour. The second period from 1985 to 2000 was the time that crime prevention knowledge gained institutional recognition, entered into mainstream practice and became a technical and professional affair. The last phase, from 1995 to 2010 was when the new initiatives became the responsibility of public, private and volunteer organisations instead of the sole responsibility of public institutions, the so-called 'top down' policy. It was at this phase that partnership and multi-agency initiatives gained more prominent and became heavily widespread.

When examining the crime prevention approaches taken by the public and private sector, the partnership approach between them also needs to be examined. The neo-liberal thinking that has been evident in other areas of crime prevention (Edwards and Hughes, 2009), needs to be analysed to calculate its effectiveness in the fight against identity crimes. "Partnerships, in all their guise place a high premium upon consensus, communication,

mutuality and the sharing of knowledge, and yet, the reality of competition, conflict and organisational autonomy remain essential characteristics of criminal justice." (Young, 1992:60). Garland (2001a:205) comments **"**in the complex differentiated world of late modernity effective, legitimate government must develop power and share the work of social control with local organisations and communities".

Partnerships are infrastructures they are not an extension of the traditional Criminal Justice System, it is strongly "oriented towards a set of objectives and priorities - prevention, security, harm-reduction, loss-reduction, fear-reduction that are quite different from the traditional goals of prosecution, punishment and 'criminal justice'" (ibid:17). There is a new commitment at local level that is called 'preventative partnership' (ibid). Partnerships can essentially be defined as collaborations between different stakeholders which consist of the Police, state and municipal agencies and private organisations and institutions (Frevel and Rogers, 2016).

In a study examining online retail organisations' knowledge sharing practices designed to prevent identity theft Shah et al. (2019) discovered that this process is based on individual staff members from information security and fraud prevention departments eager to share their knowledge as a community without any formal knowledge of sharing processes or any related training facilitating this exchange.

Crawford (1999:55) stated that the development of the partnership approach is bound up with the growth of both crime prevention and appeals to community, arguing that inter-agency partnerships are extensions of the concept of 'community' to organisations, an important and growing part of the map of British government. This was a trend that was also to include Europe, North America and the United Nations (United Nations, 1991).

In a stand-alone world of law enforcement, the often-anonymous nature of identity crime presents significant problems for the police. Moreover, most methods of identity crime are not amenable to police prevention measures: for instance, in computer-related identity theft, the offender may be in another part of the state, country, or even world. In addition, there is some anecdotal evidence to suggest an increase in cases in which individuals fraudulently allege identity theft to avoid paying bills, and the police must then distinguish between valid and fraudulent identity theft crimes (White and Fisher, 2008). Additionally, Wall (2013b) argues "identity as a driver for criminal activity is developing in new, and often unanticipated, ways. It raises questions about how to police new identity crimes as well as fundamental questions about who owns personal data and who is authorised to use it." Wall (ibid)

continues that his examination of the policing of identity crimes highlights two major issues in this area. One is that “the police are still operating in a space vacated by the private sector, who need to revisit and address the fundamentals of their identity based security systems” and this is a space which is “privately owned but publicly populated, to the point, for example, that victimised individuals still have no clear legal recourse to restore their economic reputation”.

Thus, one of the latest developments in the crime prevention world has been the introduction of multi-agency crime prevention partnerships. As well as other areas of crime control, the same approach has also been used in the fight against identity related crimes. The inherent nature of partnerships is about developing and maintaining networked relations between different organisations, however, in practice, these organisations do not meet each other on equal terms and end up having power differentials, with the police having greater power due to their control over resources and information (Crawford, 1998a:747).

It is stated that by looking at Crime and Disorder Reduction Partnerships more as multi-agency than inter-agency structures, we will be able to see, as Crawford (1998a) points out, that interdependence is not necessary, it merely becomes a case of seeing how different agencies can contribute to helping the police to meet their objectives (ibid:747).

Smith (2000, cited in Gilling, 2005) believes that what underpins a partnership approach is the ideology of unity. But he points out that the danger of this ideology is that it can lead to strategies of conflict avoidance, where power differentials between agencies and their different crime prevention programs, are left unchallenged. Conflict avoidance may be motivated by the need to preserve the impression of unity, but also by the felt need to preserve good relations at an interpersonal level; the ideology makes it important that individuals, as well as organisations are seen to get on (ibid:748). As Gilling (2005) states, where there is no structural dominance, the partnerships can turn into talking shops where active negotiations take place but hardly anything is decided or hardly any action is taken (ibid:748). Holdaway (1986) and Thomas (1994) (both cited in Gilling, 2005) see this difference as the result of different professional ideologies where some focus on community safety rather than crime reduction or situational instead of social crime prevention.

Gilling (2005), however, believes that in the new millennium there has been a growth in partnerships to the point that they have been institutionalised and moved away from just being an option. Additionally, the new practices of managerialism over professional discretion have helped this situation along with what Hughes and McLaughlin (2002) call

increasing risk management techniques.

As Wall (2013a) argues certain issues with regards to identity crime (such as the opposing opinions on the security and frequency of the issues) cannot be resolved but efforts and journalistic 'hype' can be made to "fill the information gap in identity crime".

There are two distinct aspects to tackling identity related crime. One aspect of that is the measures that the individual organisations are employing to tackle this problem and the other is the collective/partnership activities that have been developed over the last few decades to combine the individual efforts into collaborative approaches. It is evident from the literature above the significant role partnership approaches have had in the last few years in tackling different kinds of crimes. The research will examine how these ideas and approaches have been utilised to address identity related crimes and what kinds of partnerships have emerged as a result. It will also examine their effectiveness and the value that they are adding to the whole effort of tackling this issue.

3. Research Methodology

3.1. Research aims and objectives

This chapter will provide details of the methodology employed to carry out this research. It will commence by highlighting the gaps that exist within the current understanding of this crime from the perspective of the frontline professionals (public and private sector). These knowledge gaps manifest themselves in their perceptions of this crime, the definition of identity crime, their understanding of victims and offenders and techniques employed to tackle this issue. Finally, from the same perspective, the research will examine the partnerships that currently exist to deal with identity crime and their effectiveness. The methodology employed to carry out this research was qualitative data collected through interviews using open-ended questions with identity crime professionals as well as secondary documents accessed by the researcher through working with the Fraud Control unit of UK Payments. Demographics of the participants will be provided along with the data management and analysis approach that was used for this research. And finally, the valuable contribution to this study made by the researcher's work with the Fraud Control unit and the various professional industry conferences attended will be highlighted.

Criminological research covers a wide spectrum. It can focus on "the nature of the crime and its extent; the perpetrators of crime; the victims of crime; the institutions of criminal justice and their workings; punishment and penology; and the role of the state" (Jupp et al, 2000:16). In addition, research can have different purposes and types. It can be policy-related research, intervention-based research, theoretical research or critical research but these different types can also overlap (ibid:16). Jupp et al, (2000:14) believes that a "would be researcher needs to consider the following when formulating research problems and questions: the purpose of the research; the units of analysis (which can be the individual, the group or the social structure); end products for research; levels of specificity; levels of complexity; and the importance of meaning." He further emphasises the importance of clearly formulated research problems which are followed through in a consistent manner during the inquiry in order for the conclusion to be credible and plausible.

Constituting all of the above strands into one research project would be too wide a spectrum and therefore the focus of the research needs to be narrowed down. The review of the literature in the previous chapter highlighted some gaps that currently exist in the knowledge and understanding surrounding identity crimes in the UK.

The first of these gaps is emphasised by the challenges inherent in defining this crime which was highlighted by White and Fisher (2008) and Wall (2010a). The second is a lack of information, in the existing literature, which captures the views of those personnel that are on the front line of dealing with identity crime. So, it is important to ascertain how these organisations and employees actually define this crime. Do they all subscribe to the definitions that the Home Office has provided? If not, are disagreements about its definition impacting the work carried out to tackle it? In addition, in order to examine in context, the methods the respondents are using to reduce this crime, it is imperative to look at how they perceive this crime. The third lack of information concerns these practitioners' knowledge of their organisations' victims and offenders. The literature review highlighted contradictory views on the victims of this crime with Foley (2003) and Hemphil (2001) focusing on the plight of the victims while Lacey et al. (2016) seeing victims as participating in their victimisation. Many respondents' organisations are heavily involved in providing victim support services which begs the question as to whether these services have been devised based on a thorough knowledge of these victims. There is currently no research data available in this area. Whilst there is some academic literature focused on the offenders of this crime, mainly carried out by Copes and Vieraitis (2012), it is not known to what extent victim organisations/ institutions are aware of this research or if they conduct their own studies to understand better the perpetrators of identity crime.

The body of work examined in the literature review captured a number of academic recommendations for tackling identity crime such as utilising situational crime prevention techniques and educational programs (such as Pontel et al. (2008) and McNally and Newman (2009)), but it is not known to what extent these recommendations have been used by the various organisations at the forefront of tackling this issue. Additionally, are SCP strategies the only methods, or the only prominent methods, that these organisations are employing in their fight against this crime?

Partnership/multi-agency approaches have been heavily employed in the last few years to tackle crime issues, but there is hardly any evidence or data available about the partnerships/ multi-agency approaches in tackling identity related crimes.

Having given consideration to the above, the proposed research on identity crime is part theoretical and part intervention-based research and will focus on answering the following questions: firstly, the research develops a better understanding of institutions' perceptions and understanding of their offenders and victims. Secondly, it studies the risk assessment and decision-making processes utilized by government agencies and institutions to evaluate the

risks associated with identity fraud and the types of resources applied and key actions taken by government agencies and institutions to detect, prevent and mitigate identity crime. Thirdly, the research looks for the existing partnership/multiagency partnerships active in this area and will examine their effectiveness. And finally, the research captures the views of those fighting this crime on what needs to be done to tackle the issue.

3.2. Methodology

Gilbert (2005:14-15) argues that there are three major ingredients in social research: the construction of theory, the design of methods for gathering data and the collection of data. The first element, theory, is described as highlighting and explaining something that one would otherwise not see or would find puzzling (ibid:17). As there are hardly any data on the perception of major organisations (their representatives) about the phenomenon of identity crime the research will form theories. This last point focuses on crime prevention methods including the recent developments in partnership works. There are several studies conducted to gauge the effectiveness of such approaches in crime control and management. These studies and the theories highlighted therein will be utilised in examining the extent to which a partnership approach has been successful in tackling identity crime.

Gilbert's second major ingredient is the design of methods of gathering data which is described as the techniques and epistemological pre-suppositions which contribute to how information is identified and analysed in relation to a research problem (ibid). Jupp et al, (2000:4) further explains the importance of methods used in research in terms of their implications for the way in which problems are conceptualised and the type of explanations employed. This goes hand in hand with the importance of planning research which involves a process of decision making where the research problem provides the focus of the research and shapes the focus of the decisions that will be made throughout the research.

There are two major approaches when conducting a social research study: qualitative and quantitative research methods. It is believed that qualitative and quantitative research methods are not simply different ways of doing the same thing, instead they have different strengths and logics that are better used to address different questions and processes (Maxwell, 1996:17). For the purposes of this study, the qualitative method has been adopted for the specific strengths that it offers to this research. Of primary importance is the ability of qualitative techniques to assist in understanding the participants' perception of the phenomena under study, such as 'what is identity crime?' Equally, it has benefits in

understanding the particular context within which the participants act, and the influence that this context has on their actions, such as how the directors of organisations tackle this problem within their remit. Qualitative research is also valuable in identifying unanticipated phenomena, and as very little is known about identity crime, unexpected themes may emerge from this study. In addition, it has value in understanding the process by which events and actions take place, such as how identity crime is committed. And finally, qualitative research assists in developing causal explanations, such as what is causing identity crime and how customer identities are compromised (ibid:17-20).

Hammersley and Atkinson (1983:28) state that in a qualitative study "research design should be a reflexive process operating through every stage of a project". Maxwell (1996: 4) further emphasises this point by supporting the interactive model which is a process involving going back and forth between the different aspects of the design and in this process assessing the implications of purposes, theory, research questions, methods and validity. Therefore, the researcher will also adopt this approach throughout her study to ensure that the different aspects of the research design and methodology complement each other optimally.

Gilbert's last ingredient was the methods for gathering data. The conceptual framework for this research is triangulation of primary and secondary data. Triangulation can be defined simply as the use of different methods of research, sources of data or types of data to address the same research question (Jupp, 2001:308). Jupp (2001:72) further states that triangulation is the use of different types of data within one study to open up varying facets of the research and also to improve validity. For this research, primary data and documentary analysis will be used to complement each other. Porter (1994:70) also states that "It is less a case of checking a fact collected by one method, using another method than using one method and then justifying the results by another."

The technique that was employed to generate the majority of the primary data was semi-structured, face-to-face interviews lasting for approximately an hour each with the sampled population. Ackroyd and Hughes (1983:66) define interviews as: "Encounters between a researcher and a respondent in which the latter is asked a series of questions relevant to the subject of the research. The respondent's answers constitute the raw data analysed at a later point in time by the researcher."

Crow and Semmens (2008:119) state a number of research situations where semi-structured interviews are best applicable which are: where an in depth study of a phenomenon is required especially when a process or sequence of events is to be explored

or when ‘elites’ are to be interviewed or where the subject matter is of a sensitive nature. This was very much the nature of this study as the people that were interviewed hold high positions in their respective organisation in dealing with fraud (directors and heads of departments) and also the issue of identity crime is a very sensitive subject for these groups to discuss. A total of 28 interviews have been conducted for this project. Since not all of the sampled population (institutions and organisations) were based in Greater London, telephone interviews rather than face-to-face interviews were employed instead to gather the necessary information. The researcher ensured that the face-to-face interviews were held in a private setting so that the interview could be conducted without interruptions. The interviewees were told in advance about the length of the interviews. A recorder was taken to interviews to record the contents but permission was sought from the participants in advance of the sessions. Once the interview was finished the interview got transcribed as soon as possible while the discussions were fresh in my mind.

The interview questions were mostly open-ended questions resulting in mostly qualitative data. Extra vigilance was employed to ensure that the research questions were not too general, or too focused, as each of these approaches have a negative impact on the data generated (Maxwell, 1996:51). In addition, flexibility was used in terms of the questions posed as some research questions will not be fixed and often may have to undergo change as the project unfolds and as new dimensions open up (Jupp et al, 2000:15)

The basic questionnaire for all participants were the same and to preserve validity, questions were asked in the same order. However, within the overall sample, sub-groups exist which share the same profile or characteristics or function in the same industry sector, therefore certain questions were not irrelevant for some sub-groups and so they were replaced with questions more relevant to them. For example, some of the questions that were asked of a law enforcement agency differed from the questions posed to a private bank. In advance of the interviews adequate preparations and background research were conducted to ensure that the questions were relevant to the organisation. In addition, the participants were ensured of the confidentiality and anonymity of the research.

As the methodology for this research was of a qualitative nature and the interviews were semi-structured, it was the aim of the researcher to encourage the participants to share as much information as possible. Fresh leads for interviews with new participants or organisations were generated and followed up and acted upon.

As the issue of identity crime affects a large variety of private and public institutions, the chosen population consisted of three categories: public bodies (such as the Police, the Home Office, HM Revenue & Customs etc.), trade associations (such as the Association of British Insurers, British Bankers Association, retail associations etc) and private companies (such as banks, retailers etc). For the first two categories the sampling method was non-probability purposive sampling since there are specific organisations that the researcher was seeking to interview (Blaxter et al., 2002:162). But for the third category there were a large number of institutions that could/were approached. Therefore, probability sampling which is the random selection of participants (Gilbert, 2005:61) was adopted for this category.

To support the primary qualitative data, document analysis was also conducted on the numerous reports that are published in relation to identity crime or topics that would include identity crime by either government organisations or private institutions. This included reports or data from government agencies (e.g. the Home Office, CIFAS, Police, and SITO) reports and statistics. The following points were considered and adhered to when analysing such documents: authenticity, making sure that the documents were genuine and of an unquestionable origin, credibility, of the document ensuring that there were enough evidence to suggest that the document was free from error and distortion, representability, so that there was enough evidence for the document to be typical of its kind, and finally, meaning, was the document clear and comprehensible (Scott, 1990 cited at Newburn, 2007: 910). In addition to the above documents some participants also provided me with internal reports or with certain documents that they thought would be relevant to this research. They also provided the verbal permission to use these documents in my research.

Newburn (2007:911) in his examination of document analysis refers to a process of identifying themes and focusing upon the way in which things are written and the meanings that are conveyed. May (1993:146-7) takes this further by explaining that qualitative document analysis is different from quantitative document analysis which is simply calculating the frequencies with which something occurs arguing that it starts with the idea of a process or social context, and perceives the author of the text as a self-conscious actor looking to address an audience under particular circumstances, further stating that the task of the analyst becomes a ‘reading’ of the text in terms of its symbols.

In analysing documents Foucault (1984:103) states that when criticising the text, the task is not to bring out the work’s relationship with the author, nor is it about re-constructing the work through the text, a thought or experience, but rather it is about analysing the work through its architecture, “its intrinsic form, and the play of internal relationships.”

In my research I also consider observations collected at professional industry conferences and documents published by practitioners and academics.

3.3. Access

During the time of collecting data for this research I was working for UK Payments as a Fraud Project Manager. During my time with UK Payments I was initially responsible for running the plastic Card Present Fraud Priority Programme which is a project focusing on tackling the issue of cardholder data being compromised and then used to produce counterfeit cards. I was then promoted to manage the process of gathering and distributing monthly fraud figures from banks in addition to managing the Payment Industry Strategic Threat Assessment.

This position not only enabled me to develop a better understanding of the practical challenges facing the banking industry in this area but also facilitated the identification of other relevant stakeholders who are either affected by identity crime or play a significant role in tackling it. These contacts were developed in retail associations and governmental departments and will be used for the purposes of this research.

With regards to organisations within which I had no contacts, the formal approach of writing a letter outlining briefly the aims of the research and what the researcher hopes to achieve were employed (Newburn, 2007:935). It was also mentioned in the letter that anonymity and confidentiality would be adhered to in order to encourage the organisations' participation.

One obvious limitation of this study was the possibility that respondents will not share all or some of the necessary information with me. However, the likelihood of this was reduced because I was working in the industry and has established a solid reputation among interviewees and their organisations.

3.4. The demographics of the participants

The population for this study consisted of representatives from a wide range of organisations which can be divided into two main groups those that largely represent the public sector and those belonging to private industry. The information presented below will provide a reference for each interviewee and a brief description of their job title and responsibilities.

Public participants

R1	**Detective superintendent:** seconded to the Home Office working on in a multi-disciplinary team focused on identity related crime.
R3	**Director:** for a government organisation heavily impacted by this crime
R4	**Manager:** for one of the major organisation facilitating identity verification in the UK
R8	**Director:** for one of the major fraud fighting organisations in the UK
R9	**Director:** for one of the major fraud data sharing organisations in the UK
R10	**Law enforcement:** from Metropolitan Police with major responsibilities in tackling identity related crimes
R13	**Manager:** for one of the major crime fighting organisations in the UK
R20	**Law enforcement:** specialist in identity theft operations
R22	**Technical IT consultant :** specialising in identity related fraud and working with the UK law enforcement on this issue
R25	**Manager:** of identity fraud detection team within a major public organisation
R27	**Professor:** for an educational institution with responsibilities related to identity crime issues
R28	**Law Enforcement:** one of the directors for the City of London Police with responsibilities related to identity crime issue

Public sector participants

R2	**Revenue manager:** for one of the major transport organisation in the UK
R5	**Team leader:** for one of the major retail oil provider companies in the UK
R6	**Consultant:** specialising in data protection, working with major private and public organisations in helping them to protect their data better
R7	**Manager (trade association):** working with major security organisations in the UK
R11	**Head of development:** for one of the major financial service providers
R12	**Director:** for one of the major credit referencing agencies
R14	**Managing director (trade association):** for the trade association working with the major telecommunication companies in the UK
R15	**Consultant:** specialising in loss prevention, working with UK banks and financial service providers
R16	**Manager (trade association):** for a trade association working with UK banks and financial providers
R17	**Managing director:** a security and fraud consultant working with the major retailers in the UK
R18	**Managing director:** for a retailer with online and satellite TV retail business
R19	**Retail director:** for one of the major online goods providers
R21	**Director**: for one of the major credit referencing agencies
R23	**Director:** fraud communication director for a major UK bank
R24	**Security director:** for one of the UK's most prominent supermarkets
R26	**Director:** For a large retail business with online and satellite TV retail business

3.5. Data management and analysis

Because there were two different groups of respondents, one from the public sector and the other from the private sector, two separate analyses were carried out so that the findings could highlight the views within each group and also draw attention to any differences that may exist in points of view and approaches between them.

In qualitative data analysis Crow and Semmens (2008:176) argue that there are no “clear cut” and widely accepted rules and procedures instead there are a number of “broad guidelines”. They further state that qualitative data analysis starts almost as soon as the data collection begins, and this process continues throughout the research. Once some of the data were collected (approximately 10 interviews) I commenced on analysing it by first starting the coding process. Miles and Huberman (1994:56) define codes as labels or tags that are assigned to “units of meaning to the descriptive or inferential information compiled during a study”. In addition, they state that codes are “attached to chunks of varying sizes of words, phrases, and sentences or even whole paragraphs, connected or unconnected to a specific setting”. Newman (1997:422) on the other hand highlights that “coding data is the hard work of reducing mountains of raw data into manageable piles.

The coding process consisted of three stages: Open coding, axial coding and selective coding. Open coding is defined by Strauss and Corbin (1998:101) as the “analytic process through which concepts are identified and their properties and dimensions are discovered in data”. Axial coding which is the second stage is when the researcher takes the set of codes from which to develop themes and is defined by Newman (1997:424) as the pattern of thinking where links are developed between concepts or themes and doing so it may raise new questions. It can suggest dropping some themes or examining others in depth. “In addition, it reinforces the connections between evidence and concepts. As a researcher consolidates codes and locates evidence, he or she finds evidence in many places for core themes and builds a dense web of support in the qualitative data for them.... the connection between a theme and data is strengthened by multiple instances of empirical data.”

Selective coding, which is the final stage, involves re-reading the data in light of the themes that have been developed. I also used qualitative data analysis software NVivo to help with the coding process.

Throughout the process of this research, I also kept a memo of my thoughts and ideas. Glasser (1978:83-4) explains that keeping a memo helps the researcher to theorise and

write-up ideas about codes and their relationships as they strike the analyst during coding. These memos can be a sentence, a paragraph or a few pages enabling the researcher in developing “conceptual elaboration”.

Ultimately the research was expected to develop a better understanding of identity crime, how it is committed and the respondents’ institution’s perception of its victims and offenders. In addition, it was to help to identify the current detection, prevention and mitigation methods in use. Combating identity crime is mostly focused on situational crime prevention methods combined with management techniques such as customer authentication, ongoing account monitoring controls, fraud loss tracking and reporting, and training of personnel. Therefore, I expected to have these elements strongly present in the findings of the research. With this in mind, and with the results of one of the secondary data sources based on the effectiveness of partnership work (a research project that I conducted for my MSc dissertation), I then made recommendations on ways that institutions and organisations can employ the principles of working together in order to take the fight against this type of crime a step further. As Young (2005) states the aim of research is to foster an environment where the sharing of information is encouraged, “and learning lessons from others’ experience is used to good effect against the would-be fraudster”.

There were no ethical issues present with the proposed methodology for this study. All interviewees were assured that the data collected would be non-attributable to individuals or their organisations and that total confidentiality were to be maintained. In addition, since I was not requesting any sensitive data to be shared in the interviews, that helped with an increase of participation level.

3.6. Work experience

In addition to the first-hand data collected from the interviews and the secondary data and documents, I used the experience I gained from my employment within the banking industry. My role was with UK Payments Association (an organisation body set up by the UK Clearing Banks) working in the Fraud Control unit. Initially I was employed by UK Payments to manage the card present fraud (theft/fraud that occur when the card is presented in person) strategy which is one of the major elements of identity related crimes and it involved the responsibility for a number of work streams related to payment card present fraud. Working with the retail community to raise awareness about this crime and how vulnerable the chip and PIN devices are, was one of the major projects. It involved working with different retail groups such as supermarkets, fashion houses, train operators and the hospitality sector. To

raise awareness, workshops were held to discuss the issue with the representatives. The participants, who were responsible for this type of fraud in their organisations, were very keen to participate and to discuss any vulnerabilities that they may have in this area but made it clear that, making decisions and allocating budgets was the responsibility of the board of directors and was therefore, out of their hands. Following on from this theme, the two major obstacles faced in working on addressing these vulnerabilities was that firstly, security issues were not always on the top of the respondent's company agenda and secondly, as some of these organisations are very large, any changes would require a long time to implement. In order to generate support from the board, business cases needed to be presented to them which justified the expenditure to add the additional security measure. This justification needed to be expressed in both monetary and reputational terms.

The second part of the work stream was to collect information about the roll-out of DDA (Dynamic Data Authentication) cards which are more secure than the older version SDA (Static Data Authentication) which they replaced. Similar to the retail sector, the fraud practitioner community in this sector were very keen to utilise more secure products and systems but, once again, in order to succeed they had to justify internally, the costs associated with such measures. However, the association played a very central and critical role in accelerating the roll-out of these cards by collecting the data, enabling members to bench-mark their progress against industry averages and by promoting the benefits of upgrading to DDA swiftly to their wider membership.

A 'Crime-stoppers' campaign was also championed amongst the retail sector employees so that they could anonymously report anyone they suspected of being involved in chip and PIN fraud. However, the campaign was not as successful as forecasted and resulted in a lower number of inbound calls than predicted.

In this role I also worked with Insolvency Practitioners to ensure the security of PEDS (PIN entry devices) during the liquidation of retailers going out of business. It was evident from this experience that associations are very effective in promoting best practise changes in security procedures and processes within the retail and finance sector supporting this with the provision of technical knowledge, drivers for change, co-ordination and at times regulatory pressures. Fraud prevention is all about gathering audience feedback/input and generating 'buy-in' from anti-fraud professionals and front-line employees. Effective associations have a central role to play in developing partnerships (both within the sector and outside their sector) and maintaining a robust and functioning communication and data-sharing network.

Subsequently, I was promoted to manage the Management Information Strategy as well as manging the UK Payments Strategic Threat Assessment (STA) Project. The finance sector is the only sector that effectively and rigorously collects data on fraud which is used to calculate Impact Assessments, update the Event Horizon Map, and inform members so that the most pressing crimes can be categorised and prioritised.

In partnerships, proper and effective engagement with members is crucial in the successful running of the partnership. During the implementation of a project, the members are naturally in different stages of implementing the changes. This influences their level of participation and engagement but asking key individuals in organisations to champion the project ensures their commitment to the collaborative approach. Secondly, in most partnership projects, there are a number of people with different opinions and views, when a specific approach to deal with a specific vulnerability is recommended. One-to-one engagement with these individuals prior to the final decision-making process often ensures a positive response. Therefore, interpersonal skills and an understanding of the politics inside each member organisation is helpful to garner support.

Holding these two positions had several advantages for this research. As the job entailed a large amount of networking and engaging with different stakeholders and gatekeepers, several very useful contacts were made. There is a lot of reluctance by the practitioners of identity related crimes to engage with researchers but having met them personally in a business capacity, it made it easier to approach these people for interviews and also they were more likely to accept an interview request.

During this period, I not only had access to useful documentation but was also introduced to a number of useful sources. Additionally, as the financial sector is currently leading the field in the practices of fraud prevention, fraud monitoring and information management, having worked inside this sector has provided a bench mark for the researcher to evaluate, more knowledgeably, the efforts of other sectors in dealing with this crime. Furthermore, my role provided the opportunity to attend a number of closed membership and general conferences which have proved to be very useful to this study.

3.7. Conferences and seminars

I attended a variety of industry related conferences in banking, travel and retail fraud. The payment fraud conferences covered a wide range of issues related to payment fraud such as ATM fraud, Schemes (Visa and Mastercard) perspectives on current and developing trends

in fraud, legal issues surrounding payment fraud, and the latest technical software used by banks to help them tackle fraud. These conferences were very useful especially in the development of the second chapter on financial identity crimes. Key themes that emerged from discussions in these conferences included themes such as: different countries having different approaches to fraud prevention in a global crime market, the trend being towards a decreases in the number of fraud cases but increases in the value of each fraud case, fraudsters becoming more aggressive and intelligent, a need to engage with different stakeholders to drive fraud out, serious issues with jurisdiction across borders, identity related frauds being expensive and difficult to prosecute, identity crime foot soldiers being the ones that are caught whilst ring leaders largely evading capture and having local regulations for a global problem. And finally, limited amount of data being freely available on fraud detection methods and their effectiveness.

At the retail fraud conference, the importance of PCI DSS (Payment Card Industry Data Security Standards) for retailers was discussed. This standard was created to increase controls around cardholder data to reduce credit card fraud. Validation of compliance is carried out annually by an external Qualified Security Assessor (QSA) who creates a report on compliance for organisations (such as retailers) handling large volumes of transactions, or by Self-Assessment Questionnaire (SAQ) for companies handling smaller volumes. This is an important element in data protection as companies have been compromised when these standards were not thoroughly met (such as the TK Max data loss in 2007). Although the PCI DSS must be implemented by all entities that process, store or transmit cardholder data, formal validation of PCI DSS compliance is not mandatory for all entities. Currently, both Visa and MasterCard require merchants and service providers to be validated according to the PCI DSS. Smaller merchants and service providers are not required to explicitly validate compliance with each of the controls prescribed by the PCI DSS although these organisations must still implement all controls in order to maintain safe harbour and avoid potential liability in the event of fraud associated with theft of cardholder data. Issuing banks (the financial institutions that issue debit and credit cards to customers) are not required to go through PCI DSS validation although they still have to secure the sensitive data in a PCI DSS compliant manner. Acquiring banks (the banks that process payments for retailers) are required to comply with PCI DSS as well as to have their compliance validated by means of an audit. In the event of a security breach, any compromised entity which was not PCI DSS compliant at the time of breach will be subject to additional card scheme penalties, such as substantial monetary fines.

I was also a presenter in the Association of Train Operating Companies' (ATOC) conference. The aim of this conference was to raise awareness of the importance of protecting chip and PIN devices in this sector and to liaise with the participants in order to promote a better understanding of the processes in place to secure these devices. At the conference, I discovered that card not present fraud was the biggest issue for this sector and that the various train operating companies were losing vast amounts of money to this fraud.

Subsequently, through working with individual companies it was discovered that the chip and PIN devices were not protected properly by the different operators. Additionally, large numbers of credit and identity cards were found on trains (lost or forgotten) adequate measures were not in place to properly protect them. chip and PIN devices became very valuable to criminal gangs in 2008/9 who used to steal them, tamper with them and re-introduce them to the retail environment in order to capture the users' card data. Failure to adequately secure these devices increases the risk of them being stolen by fraud gangs. Some train operators were not even aware of the value of these machines to the wider identity crime fraudster community.

As part of UK Payments' efforts to tackle fraud, a yearly cyber-crime conference is held to provide a forum for the practitioners to share the latest developments and research. Two major points emerged from this conference: firstly, criminal websites selling payment card data employ sophisticated marketing strategies in order to attract potential buyers (such as pictures of expensive cars, holidays and homes), the strong implication being that the quality of the card data is so good that the purchaser will be able to buy these luxuries by fraudulently using their data. And secondly, despite extensive positive marketing, the anti-virus software currently widely available to individuals is only 50% effective in preventing successful cyber-attack breaches of systems and the software operating inside them.

3.8. Anticipated problems

Although limited academic research has been conducted on identity crime in the UK, there are sufficient accessible professional and commercial references which address identity crime to enable the proposed exploratory research to be carried out successfully. Several relevant documents have been retrieved from such sources as online journal databases, internet web sites, and local university libraries using a relatively small number of research keywords (e.g. identity theft, identity fraud, impersonation, white collar crime, bank fraud, financial service). In addition, there is a variety of reports published by government bodies in an attempt not only to tackle the issue but also to inform the practitioners and public of the

government's activities in tackling this issue. These reports will play a significant role in compiling this research.

Through business rapport with gatekeepers, I was in a key position to carry out the proposed research in the UK identity crime/fraud industry. However, I was aware that most organisations are seriously concerned about the public disclosure of confidential information, especially concerning the costs and extent of identity crime in their organisations. To eliminate this concern, I attempted not to obtain any figures on identity crime experienced by participating private or public institutions. Instead, the proposed research focused on examining how fraud management executives perceive the risk of identity fraud, how they define it, and the resources that they have, or intend to apply to detect, prevent or mitigate these risks in their organisations and to what extent, if any, they act with, or have considered the value of, a 'partnership approach'.

4. Identity crime from the public sector perspective

4. 1. Introduction

This chapter examines identity crime from the perspective of the government and the public sector. It commences by reviewing how identity crime has come to prominence and been recognised as a threat by government and the public sector, the extent of the problem and early attempts to tackle it in the UK.

There follows a review of the major public sector organisations that play an important role in tackling identity crime such as the National Fraud Authority (NFA), CIFAS (Credit Industry Fraud Avoidance System) and law enforcement agencies. The scope and activities of these organisations will be discussed in more detail in this chapter.

The impact of the sharp and continued rise in cyber-crime is reviewed next as it is a major factor in the commission of identity crime and a major challenge to practitioners (in both the public and private sectors) on the front line of identity crime prevention efforts. The latest public sector strategies employed to tackle this element of identity crime will be examined along with national and international efforts focussing on the EU and UNODC.

Finally, the responses to the research questionnaire provided by the public sector participants will be examined and discussed.

4.2. Acknowledging the existence and extent of identity crime in the United Kingdom.

The private sector made the first attempt to collectively start measuring this crime 29 years ago (R16). The public sector was slow to follow and only acknowledged this crime in 2002 when the Cabinet Office published a report examining the identity crime problem in the UK and estimated that it was costing £1.2bn (R24*).* Among other issues, the report advised the need for a multi-task force of public and private sector collaboration to tackle the harm caused by identity fraud to the UK economy (R24). This report was sent to the Home Office in 2003 and the Identity Fraud Steering Committee (IFSC) was set up to work with public and private sectors to “identify and implement cost effective measures to counter identity fraud” (New Estimate of Cost of Identity Fraud to the UK Economy, 2006-7).

In 2005, several MPs and Peers from both sides of Parliament, concerned with the prevalence of identity crime, established the All-Party Parliamentary Group (APPG on

Identity Fraud). In 2006 the APPG was asked by Andy Burnham MP, the then Home Office Minister to conduct an "investigation into identity fraud with a view to making recommendations to government of the immediate steps which can be taken to tackle this issue" (All Party Parliamentary Group, 2007). Fifty-three recommendations were made by the report with three key issues highlighted to address identity crime more effectively which included, better public awareness, a more accurate understanding of the scale of the problem, and the provision of more resources for law enforcement and the authorities to tackle identity crime. Despite these recommendations, little has been achieved by law enforcement agencies as there has been a lack of activity by government. In 2007 a total of £29m was allocated to implement the recommendations of this report, and finally in 2008 the National Fraud Authority was established to fight against identify fraud and fraud in general which was a major step forward (National Fraud Authority Business Plan 2010/11).

In addition to the formation of the NFA and following on from discussions between the UK Card Payments industry and the National Consumer Group, a specialised service called the Victims of Fraud Service was developed in 2008. The service is run by the three credit referencing agencies (Callcredit, Experian and Equifax) with the objective of assisting victims with support. This support includes providing advice to victims on how to protect themselves from further identity compromise such as signing up to CIFAS Protective Registration. The Victims of Fraud Service also specialises in handling credit report related issues on an individual case management basis on behalf of the victim contacting lenders on the victim's behalf, in order to restore the victim's credit history to its former state and finally, providing regular updates and advice to victims on the progress of amendments to the victim's credit report. Previously, it would have been the victim's responsibility to contact all the major banks or financial service providers which was a very stressful and time consuming task and in some cases the victims were completely oblivious as to what was happening to them and how their identifying information had been stolen and used. This was the first and a major step on behalf of the government and industry to acknowledge the pain caused by identity fraudsters to their victims and a positive move towards helping the victims to rectify the damage caused to their lives by this crime. However, despite this, these efforts have not been as effective as initially hoped as it seems that little has been achieved. So, one of the major aims of the efforts above was to provide victims with a single point of contact that could provide the support and assistance that they needed to resolve their issues. However, a report published in 2018 (Skidmore et al., 2018) indicates that the process for victims seeking advice, resolution or support is still confusing, with victims being passed around a multitude of services to secure the resolution they need.

In addition to the above, provisions were made in the Serious Crime Act 2007 to allow for the "targeted exchange of data between the public and private sector through an anti-fraud organisation to highlight potentially fraudulent applications for goods and services" (Document 8, R8). Further provisions were made in the Police and Justice Act 2006 allowing for the release of information on the recently deceased to the private sector to help prevent those identities from being used by criminals" (ibid). And the Identity and Passport service started to deploy a number of measures to increase the security of UK passports and to prevent fraudulent passport applications by conducting face-to-face interviews for first time for all adult passport applications (ibid). In order to provide awareness and guidance for the public and small businesses to keep their computers safe and conduct online business and transactions safely the Get Safe Online website was developed (ibid).

4.3. Extent of the problem and it's measurement

In dealing with any kind of crime or fraud it is imperative to discover the extent of the problem under examination. A brief study of recent media indicates identity crime to be one of the most modern and fastest-growing types of crime in the UK. However, the question is how accurate is this assertion? There are a number of organisations that publish data on losses due to identity fraud. Apart from the banking industry which is transparent with the amount of money that is lost to this type of crime, no other organisation (either public or private) seems to be publishing their figures independently. It is only after the exercise carried out by IFSC that the losses of other organisations have come to light.

As the literature review highlighted, currently the only source of data for identity related crimes is CIFAS (UK's Fraud Prevention Service) and although the data and sources captured by them are valid and reliable, they do not provide a holistic picture of identity crime in the UK. To address this issue, the Identity Fraud Steering Group in 2006 made an estimation of the losses suffered by the UK economy to this type of fraud. The estimated figure was £1.79 billion (Fraud Review, 2007) which was then reduced to £1.2 billion when the study was revised in 2007. This figure includes losses suffered by a large number of public and private organisations which are summarised below by type of organisation.

Organisation	**2006**	**2007**
Association of British Insurers	£22m	£31m
Audit Commission (losses to pensions schemes)	£15m	£36m
British Cheque Cashers Association	-	£0.4m
Building Societies' Association	£3.1m	-

CIFAS (representing the losses suffered by the retail sector)	£2.3m	£23.5m
Department for Constitutional Affairs	£29.9m & £5.9m	£50m (including police costs)
Department for Work and Pensions (benefit fraud)	£20m	-
Driver and Vehicle Licensing Agency (abuse of driving licenses for identity fraud)	£2.5m	£5.3m
Driving Standards Agency (estimates costs of ensuring that DSA is satisfied as to the identity of the candidates presenting for theory and practical tests)	£1.2m	£1.7m
Finance and Leasing Association (identity fraud arising from the provision of motor finance)	£14m	-
HM Revenue and Customs (referring to direct and indirect taxation)	£217.7m	£47.2m
Home office/Immigration and Nationality Directorate (cost of undertaking enforcement activity against individuals who may be involved in some form of identity theft or fraud, potentially document abuse)	£56.2m	£284.4m
Local Authorities	£28,564	-
Ministry of Justice (covering unpaid fines due to identity problems)	£35.8m	£39.7m
Money Laundering	£395m	-
Police Service	£1.73m	-
Telecommunications	£372m	£485m
UK Passport Service	£62.8m	-
UK Payments Association	£504.8m	£201.2m
Total	**£1.72bn**	**£1.253bn**

There are several differences between the 2006 and the 2007 identity fraud estimations. Some figures have increased and some decreased. This could be because some organisations or industries have not yet acquired a robust system of measuring this crime. The banking industry is the only sector that has dedicated resources to regularly collect, collate and publish data on the losses. In the 2006 figures, UK Payments included all identity fraud related categories such as Card Not Present fraud, whereas in the 2007 figures only Application fraud and Account Take over have been included. Some organisations have been omitted in the 2007 figures such as the Building Societies Association, Local Authorities, Money Laundering and Finance and Leasing Associations but, on the other hand, other organisations have been added such as the Department for Innovation,

Universities and Skills and the British Cheque Cashers Association. No explanation has been provided for these changes apart from the omission of Money Laundering figures which is the result of the members of IFSC arguing that this category does not have a direct link to incidences of identity crime.

The methodology used to collect this data considers three different costs associated with identity crime. These are: anticipation costs (costs associated with risk assessment, deterrence, prevention and identification/detection), reaction costs (investigation, recovery and restoration) and finally direct financial loses (net cost of detected identity fraud and estimated cost of undetected identity fraud) (Document 11, R15).

The latest report from the NFA recognises identity fraud as an enabler to other types of fraud, does not consider it as a fraud type on its own, and estimates the losses to be between £1.9 billion and £2.7 billion (when including the costs of responding to and dealing with this crime annually). This is only an estimate, however, and it is difficult to generate a more accurate picture of the losses suffered by the total UK economy. In addition, as this type of fraud and the methods of recording and reporting it are relatively new, there may be inaccuracies present in the data reported. The issue of the 'dark figure' of crime is also applicable in this area (where people do not report crime) therefore making it difficult to obtain a true picture of the problem. It is believed that not only do people not report crime but also some organisations feel reluctant to do so as well (Document 9, R15). Additionally, with some organisations, in some cases, if the identity fraud is part of a larger fraud it will not be recorded alone but as part of the larger crime (identity-fraud.org website)

In addition to the above figures, there are the costs of the social impact on victims (quantifying the cost in terms of rectifying the harm caused to them by identity crime). This was estimated as a staggering £6 million (based on an analysis by the Home office) (Document 8, R8).

The data from the NFA indicates that identity fraud losses have increased significantly in the last couple of years from £1.2 billion in 2007 to £2.7 billion in 2011. Two major opinions were identified from respondents with regards to the identity fraud figures. Firstly, it is believed that the current figures are not a true reflection of the extent of the problem. There are still large sums of money written off as bad debt and the identity crimes due to the creation of false identities never get included or even detected as identity crime. It is also believed that the lenders' ability to distinguish between bad debt and a fictitious identity has improved as they are starting to know their customers and their habits better. The increases in the figures of identity crime have also been due to the fact that more information is generated and more

and more analysis is conducted on the existing data. Finally, there are those who believe that "identity fraud has been going on for a considerable amount of time but it is its profile that has risen significantly" (R8).

There now follows a review of the public sector bodies engaged in combatting identity crime- the NFA (incorporating Action Fraud), CIFAS and the law enforcement agencies.

4.4. Formation of the National Fraud Authority (NFA)

As stated earlier, the NFA was established by the government in 2008 as an executive agency of the Attorney General's Office with four main strategic priorities and fifteen key projects, one of which was focused on identity crime because it was acknowledged that not only is the fraud landscape complex and the response to it fragmented but also that fraud in general is misunderstood and not always taken seriously (National Fraud Authority Business Plan 2010/11).Therefore, it was the NFA's responsibility not only to raise the profile of fraud amongst the public but also to bring unison in tackling fraud and to draw the efforts of industry together. The four stated strategies for this organisation were to build and share knowledge about fraud, tackle the most serious and harmful fraud threats, disrupt and punish more fraudsters while also improving support for their victims and finally, to improve the nation's long-term capability to prevent fraud.

In their 2010/2011 plan the NFA extended these strategies to include more elaborate aims (National Fraud Authority Business Plan 2010/11) which focused on improving information sharing between and within the public and private sectors. The clear objective was to prevent and detect more fraud as well as improving reporting of fraud to Action Fraud (established by the NFA) in order to harness the information collected to achieve better prevention of and enforcement against fraud. Additionally, this organisation was to build relationships, share good practice, deal with the gaps and overlaps, help to streamline the counter fraud community landscape and help the fraud prevention community become more cohesive, efficient and effective. Part of their program was also to improve the support and advice available to victims of fraud along with raising awareness amongst the public and the business community. The NFA was to provide a centre of expertise to raise the profile and priority of fraud, secure and target resources to counter fraud appropriately and to achieve better prevention and enforcement against fraud. A further objective was to ensure there was an appropriate balance in the criminal justice system between fraud prevention and disruption and the use of criminal justice powers and that the criminal and civil enforcement measures used against fraudsters were as effective as possible.

Identity crime, having been recognised as a key enabler of fraud in general, was to be prioritised and specific actions were to be taken to address it. The specific actions fell under strategy number six for this crime which included the NFA taking the lead on multi-agency work to crack down on identity crime. They were to devise and deliver a strategic threat assessment of the harms caused by identity crime, how identity fraud is perpetrated and the vulnerabilities of identity credentials. Additionally, they were to conduct an evaluation of methods of identity authentication, establish best practice and make recommendations to improve identity fraud prevention and detection. Disseminating best practice and ensuring vulnerabilities exploited by criminals were shared with the counter fraud community and working with both public and private sectors to improve public awareness of identity crime were other key responsibilities they were to drive forward. And finally, they were to improve and roll out the identity crime victims toolkit to all Victim Care units and partner agencies (National Fraud Authority Business Plan 2010/11).

Action Fraud was established in October 2009 by the NFA to provide a "simple and central point for individuals and small and medium sized businesses to report fraud" (ibid). The NFA believed that more than half of all fraud victims do not report the crime because of embarrassment. This service is focussed not only on recording the reported fraud but also providing victims with support (Fraud Focus, February 2010). The National Fraud Intelligence Bureau (NFIB) which was developed at the same time had the responsibility of combining the data collected by Action Fraud alongside data inputs from the public sector and industry as a whole collating and analysing this data and producing reports (National Fraud Authority Business Plan 2010/11). The news release from the NFA indicated that in the first year of Action Fraud 150,000 people contacted them to report fraud totalling £78m and although this total is not identity fraud specific, online shopping and application fraud (which are classed as identity fraud) are amongst the five most commonly reported frauds (Fraud Focus, October 2010). Action Fraud does not record and report identity crime separately, but they are getting that changed so that it will be in the future (R28). However, this has not happened yet. The NFA believed that the correct recording of identity related fraud would be influenced by the public's perception of the crime in that it is important enough to be reported. For example, when somebody calls the service to log a fraud on their credit card, if they call it card fraud it will be recorded as card fraud if they call it identity fraud it will be reported as identity fraud. Additionally, there is so much overlap between identity fraud and other types of fraud, such as mass marketing and phishing, that sometimes it seems almost impossible to have a clear-cut distinction (R28). In practice, Action Fraud has received a lot of criticism. An undercover investigation by The Times discovered that the call-

handlers working in this organisation insulted victims, were trained to mislead victims into thinking that their case would be investigated by the police (whereas these cases are never looked at) and finally, instead of supporting the victims, they were mocked and called 'morons' (Morgan et al, 2019). Furthermore, in 2013, 2,500 people's crime reports went missing inside Action Fraud due to an IT error. At this time, 85 call centre helpline staff were employed, albeit outsourced to the private sector contractor Concentrix. Lately £35 million of government funds were used to improve the helpline and website, however, only cases involving losses of over £100,000 are being passed to a human investigator, others being dismissed by computer algorithms as unworthy of investigation. In the year 2017/2018, of the 277,561 fraud cases reported to the police, only 8,313 cases resulted in charges being brought or summonses issued representing only a 3% success rate. Additionally, many people continue to report fraud to their local police forces and not Action Fraud (Skidmore et al., 2018).

To further highlight the issues related to the inefficiency of this service, in one instance more than 30 people reported a fraudster to Action Fraud after losing their savings to a bitcoin trader but despite a detailed report with names, contact details and evidence of the online transaction the organisation failed to act. (Gibbons, 2019).

In dealing with identity fraud, the NFA set up a task force with a task force board which oversaw a programme of work which was to be delivered by three subsidiary groups. There were also four key activities that the NFA was undertaking which had not been carried out previously. The first one, was the provision of a tool kit for victims of identity fraud. One of the gaps that the NFA noticed is in terms of victim support compared with other crimes. For example, victims of burglary receive support from the police by way of a visit from victim support who advices them on how to make their house safe and provide them with support, for fraud it is very different because in most cases the police is not interested (R8). The support which is still ongoing targets those that make phone calls or send emails to Action Fraud and report their victimisation. Once a report is made, the person contacting the centre will be asked whether they require further support and if the reply is in the affirmative they will be visited by a community representative to hand them the tool kit and answer their questions and concerns.

The second activity is related to the identity related materials confiscated by law enforcement agencies. Previously when the police disrupted an identity fraud factory or a website selling false identities, they would prosecute the people involved but as part of the operation they would have thousands of false identities and there were no clear plans to

examine or share that information. Therefore, one of the actions that the NFA took was to produce guidance to the police and banks and others on what they should do when they acquire this material, and communication channels were developed to share that material with other fraud partners (R8).

The NFA's third role was to represent the UK in international forums dealing with identity fraud. In addition, they were tasked with co-ordinating the UK approach to international engagement with these varied forums (R8).

And finally, the fourth area was to produce a UK strategic threat assessment. There is a lot of information and knowledge on identity fraud yet there has never been a co-ordinated approach to drawing all this data together in order to form a more coherent understanding of the issue. The NFA was clearly tasked to fill this gap. "There are lots of pockets of activity but very little of it has been co-ordinated" (R8).

Another of the key issues that the NFA addressed was to measure the monetary losses due to fraud. A measurement unit has been set up that has been producing an elaborate report on the fraud losses to the UK economy on an annual basis. Identity fraud is part of this exercise. For their first exercise, the NFA used the £1.2 billion figure calculated in 2006 but going forward, this figure will be re-visited on an annual basis. In order to complete such an exercise, the measurement unit has been relying on data from various organisations which have all been collaborative in providing information and assistance (R8).

The NFA's role was to focus the numerous amounts of activity that are currently being carried out by other organisations. In order to accomplish this objective a taskforce was set up with a specific time limit. The task force was run by its board which comprised of chairs of ACPO (Association of Chief Police Officers) Working Group on identity fraud and SOCA (Serious Organised Group Crime Agency) programme 17 and the IFCAG (Identity Fraud Consumer Awareness Group) plus HMRC and the City of London Police. The taskforce board oversees a program of work which is delivered by the 3 subsidiary groups (R8).

Unfortunately, the NFA's existence was short lived and it was dissolved in March 2014. Action Fraud was transferred to the City of London Police (who continued to work alongside the NFIB) and the strategic development of threat analysis was transferred to the National Crime Agency. The e-confidence campaign went to the Home office and responsibility for the development of the counter-fraud checking service was taken on by the Cabinet Office. The responsibility for managing the Annual Fraud Indicator was passed to non-governmental organisations (Experian, PKF Littlejohn and the University of Portsmouth's Centre for

Counter Fraud Studies) which includes a group of cross-sector fraud experts who regularly meet under a broad umbrella known as the United Kingdom Fraud Costs Measurement Committee (UKFCMC) to produce monetary losses (Fraud Indicator, 2016).

Additionally, single points of contacts (SPOCs) were created within each of the 43 police forces in order to receive and take action on identity crime related issues received from government agencies but looking at the report published on law enforcement activities in this arena, once again it is not certain if these SPOCs have been effective or have been utilised for the maximum benefit (R25).

4.5. CIFAS (UK's Fraud Prevention Service)

One of the other major players in the identity fraud and fraud in general arena is CIFAS which was established in 1988 by the major lenders in the UK consumer credit industry. CIFAS is a not-for-profit membership association representing the private and public sectors dedicated to the prevention of fraud, including staff fraud, and the identification of financial crime. Although arguments could be made to position the feedback from practitioners in this area under the 'private sector' chapter of this research, the not-for-profit, pastoral orientation of the organisation lends itself more readily to being grouped with the public sector research. Its influence is considerable, having over 360 Members spread across banking, credit cards, asset finance, retail credit, mail order, insurance, savings, telecommunications, factoring, share dealing and the public sector. Although at present CIFAS members are predominantly private sector organisations, public sector bodies may also share fraud data reciprocally through CIFAS to prevent fraud. CIFAS's role is to facilitate the sharing of information provided by its members to prevent further fraud (CIFAS website).

In addition to information sharing, CIFAS provides a service called the Protective Registration service which is a tool to assist individuals and organisations to combat identity crime. The service is run both for individuals and for organisations. CIFAS Protective Registration for individuals enables them to seek protection against possible impersonation attempts when they have good reason to believe that their details might be used by a fraudster. For example, there may have been a burglary or a violent crime where personal documents have been stolen. CIFAS member organisations are dealing with requests for credit or other services from someone who has taken out CIFAS Protective Registration will be alerted to the need for caution. During their routine checks, they will see a CIFAS warning flag marked 'Protective Registration' against the individual's name and personal details which indicate that he or she has been recorded on the CIFAS database for their protection.

As a result, CIFAS members will undertake additional checks to make sure that the applicant is genuine and not a fraudster trying to commit identity fraud. This offers reassurance that the identity of an individual (who has taken out Protective Registration because they are at heightened risk of identity crime) is protected against further fraudulent applications.

CIFAS Protective Registration for organisations, on the other hand, is devised to help them in protecting their consumers and employees from identity fraud if there has been a data security breach. When a laptop bearing customer details is stolen, or payroll or other information is intercepted, for example, a straightforward solution is available from CIFAS. The service is known as the CIFAS Bulk Protective Registration Service. It enables organisations to co-ordinate and to submit to the CIFAS database, as a batch, the details of all those individuals who require protection. The service allows those who are at risk of identity fraud to have a special CIFAS warning 'flag' placed on their credit reference agency file. Then when, for example, an application for credit or insurance is received by a CIFAS member (such as a bank, building society or insurance company), the member is alerted by the warning 'flag' to undertake additional verification checks to ascertain that the applicant is genuine, and not a fraudster trying to commit identity fraud. In addition to the above, CIFAS also publishes data on the extent of the issue on a regular basis and proactively participates in the Identity Fraud Consumer Awareness Group.

Law Enforcement

There are a number of law enforcement agencies taking an active role in fighting identity crime. These are the City of London Police, the Association of Chief Police Officers (ACPO), NCA (National Crime Agency) and DCPCU (Dedicated Cheque and Plastic Crime Unit). It should be noted that attempts were made to conduct interviews with law enforcement agencies- but these were unsuccessful- possibly because most of the data managed by these organisations is of an extremely confidential nature and its access is restricted even for academic purposes.

Currently, there is no single legislative definition of identity crime and thus no single law designed to address it. There are, however, a range of Acts criminalising offences which together provide appropriate tools to combat this crime. The Fraud Act of 2006 created a new offence of fraud which can be committed in three ways: by making a false representation (dishonestly, with intent to make a gain, cause loss or risk of loss to another), by failing to disclose information, and by abuse of position. It also established, in section 6, the crime of being in possession or in control of ‘articles for use in or in connection with any fraud’. Sections 25 and 26 of the Identity Cards Act 2006, since repealed, created new

criminal offences of being in possession or control of false identity documents, or apparatus or material for making false identity documents.

Wall (2013a) in his examination of laws relevant to identity related crime lists and examines other legislations that are successfully used to prosecute identity criminals. The Forgery and Counterfeiting Act 1981 contains two pieces of legislation relevant to identity crimes. The first is “using false instruments to induce prejudicial actions in others” (section 3) and the second is “using a copy of a false instrument” (section 4). Wall (2013a) further argues that in addition to the Acts above, there are others that can assist in the prosecution of identity crimes. These are: the Computer Misuse Act 1990 which covers unauthorised access, unauthorised access with intent to commit a crime and unauthorised access to change data and includes distributed denial of service attacks, the Theft Act 1968 (section 21(1)) and the Larceny Act 1916 (section 29 (1)(i) and 30) for covering cases of cyber-extortion or blackmail (using social media networks or not).

From the legal perspective, Wall (2013a), in summary, concludes believes that the law relating to individual identity crimes is recent and robust, yet does not reflect the terminology of identity crime which is confusing for regulators and does not assist new UK national fraud reporting systems. In addition, the law does not assist victims of identity fraud as well as it could.

4.6. Cyber security strategies

Cyberspace plays a very important role in facilitating identity crimes. As mentioned above, criminals easily harvest personal data using the internet and the results of the ensuing fraud often make news headlines so, cyber security is finally having the attention that it deserves. The opening paragraph of the UK cyber security report reads:

> “The future of the UK’s security and prosperity rests on digital foundations. The challenge of our generation is to build a flourishing digital society that is both resilient to cyber threats and equipped with the knowledge and capabilities required to maximise opportunities and manage risks.” (The UK Cyber Security Strategy, 2016)

In the report, it is acknowledged that cyber security is an area of relative immaturity when it comes to the measurement of outcomes and impacts (normally referred to as metrics). Absence of data is also acknowledged.

> "We will ensure that this strategy is founded upon a rigorous and comprehensive set of metrics against which we measure progress towards the outcomes we need to achieve." (The UK Cyber Security Strategy, 2016)

Additionally, a National Cyber Security Centre which is part of the intelligence agency GCHQ was established in October 2016 as part of a £1.9 bn five-year strategy. One hundred private sector employees were seconded to the centre to help identify threats. Chancellor Philip Hammond was quoted saying "government cannot protect business and the general public from the risks of cyber-attack on its own. It must be a team effort. It is only in this way that we can stay one step ahead of the scale and pace of the threat that we face."

The centre will be working on a voluntary basis with political parties and giving advice to high profile individuals, including MPs, on how to protect their sensitive data.

In November 2011, the government published the UK Cyber Security Strategy which focuses on all risks relating to internet use. By 2015, the government's aspiration was that the measures outlined in the strategy would mean the UK would be in a position where law enforcement is tackling cyber criminals, citizens know what to do to protect themselves, effective cyber security is seen as a positive for UK businesses, a thriving cyber security sector has been established, public services online are secure and resilient, and the threats to national infrastructure and national security have been confronted. Another Cyber Security Strategy was published to focus on the period 2018 to 2020. The national response in the report will be to Defend, Deter and Develop in the area of cyber security along with international action.

4.7. International and national efforts

Although this study is UK specific, identity crime is not limited by country borders and a brief look at the wider scope indicates that there have been major developments at international levels to address this dilemma. Identity criminals can cross more than one country or jurisdiction when committing this crime. In most cases, they are part of an organised gang or a transnationally operating group, hence the increased willingness and enthusiasm between governments and identity crime prevention practitioners to collaborate on international levels. The UK has teamed up with the USA, Canada and the European Commission to work collectively on this problem. Although the collaborations with the USA and Canada are on a discussion-only basis, information sharing co-operation with the EU is far more structured and focused with quarterly meetings to discuss various aspects of the issue (R8).

One of the first and foremost issues that the collaborations with the USA and Canada will look to examine is the lack of consistency in defining identity crime. This issue is on the EU Commission's agenda as well. The aim is to agree on a set of definitions that can be used across all the member states. The EU Commission has set up a specific group to take forward the issue of identity crime in 2007. On a more local level, although the Home Office provided a set of definitions on the identity theft website, it seems that the practitioners are not adhering to them in their day to day work environment. Other countries are also facing the same challenge. "There seems to be different opinions and different forums seem to have different names for it" (R8). This issue is challenging on a national level which will make it even harder to tackle on an international basis.

The majority of the discussions that have been held in these meetings have been focused on the following topics: the issue of cyber-crime and identity crime, identity infrastructure and identity management, discussions on a common approach to identity crime, the need for authorities to have an identity strategy and finally the cross channel and cross border nature of this crime.

Looking at these discussions on a more detailed basis provides useful insights. For example, with regards to cyber-crime, the UK is opting-in to the European Union directive 2013/40/EU on attacks against information systems to tackle cyber-crime. It is obvious that the international and cross-border nature of this element of identity crime is generating international concerns and efforts to tackle it. Although the UK has a National Cyber Security Strategy and an investigative unit to support that, PCeU (Police Central e-crime Unit) (Met Police), the move is a positive approach in bringing together unified legislation and common policies to fight against the crime and establish a cross-border European alert platform for internet-related offences, an EU cyber-crime training platform and co-ordinated member state projects (Document 1, R8).

The discussions held in the EU Commission meetings highlight several themes and suggestions that have been put forward to help tackle this issue. The first suggestion focuses on the need for a common definition as well as the establishment of central units both for citizens and organisations to report identity fraud and a unit or body where countries can verify data EU-wide. With freedom of movement for citizens a key concept, this would be of crucial value so that the identities of people moving to other countries in the EU can be checked. The second theme is the accurate and timely exchange of information for controlling and minimising the effects of identity theft and fraud. It is also acknowledged that there is a need for more analysis, study, training and expertise in cyber-crime and common

training packages for authorities and law enforcement, especially regarding the new technologies relating to biometrics. It is recognised that identity management has many dimensions and should be approached as an integrated whole with the need for multi-disciplinary teams as the nature of identity crime is multi-disciplinary and cross-border. Another key theme is to focus on leadership and political engagement and the need to enhance co-operation at national and international levels (harmonising concepts, rules, policies and procedures) - and finally, encouraging governments to use biometric systems to verify their citizens (Document 6, R8).

In the discussions held in these forums it has been noted that it is the authorities' responsibility to create a safe and secure identity infrastructure in order for their citizens to be able to exercise their rights fully, and sadly, the current identity infrastructures do not seem to be able to support this objective. There is a need for dynamic and integrated identity management approaches that manage the individual parts of the identity infrastructure as a coherent whole (ibid).

The above indicates a proactive approach in the European arena to this problem, however, when the remit and effectiveness of these efforts were examined two immediate concerns came to light. Firstly, the speed with which the discussion points are progressed. It is believed that actions are progressed very slowly in these forums. Secondly, the representatives from various European states come from different seniority levels, some very senior and some junior which impacts the priority given to identity management (R9).

Although the UK, compared to other EU members, is a more mature market and leads the fraud world in this area, the collaborations are perceived as positive steps in engaging with other countries and developing better working relationships with them to pursue the transnational aspect of identity crime.

Identity crime-related issues have also been an area of concern for the United Nations. In 2004 the United Nations Office on Drugs and Crime (UNODC) commissioned a discussion paper on identity crimes. The purpose of this paper was to "assist UNDOC in developing strategies and practical action for combating identity-related crime, improving communication between crime experts and victim experts, and identifying areas in need of further research. The outcome was a handbook consisting of 5 papers each focusing on one aspect of identity-related crime which was presented at the 4th meeting of the core group of experts on identity-related crime organised by UNODC on 18-22 January 2010. The first paper titled "Legal Approaches to Criminalize Identity Theft" (United Nations, 2010) focuses on three major aspects of the legal response to identity theft. The first part analyses the phenomenon

of the effects described as ‘identity theft’, examining the type of identity-related information the offenders aim for, as well as the methods used for the commission of the offences. The second part of this paper considers the existing approaches to defining identity theft by taking into account the results of the analysis related to the phenomenon as well as the existing definition (a typology of identity theft is developed.) The third part of the study provides an overview of arguments in favour and against the development of a specific approach to criminalise identity theft and highlights existing approaches. Additionally, it presented potential elements which are necessary for the development of a national approach on the basis of the results of the first and second part of the study.

The second paper focuses on Typology and criminalization approaches to identity-related crime: Compendium of examples of relevant legislation” (ibid) provides an inventory of countries’ national legal provisions” which are specific to identity-related crime with the ultimate objective of generating practical information which may be of interest for development of further studies or for production of technical assistance manuals and training. This particular guide came about as it was noted that several states were in the process of considering or establishing new criminal offences against identity-related crime, whilst others remained to be convinced that a new perspective on criminalization would be a sufficient improvement over existing offences such as fraud, forgery and impersonation. Therefore, it was recommended that UNODC take action to raise awareness of the legal issues at stake and the policy options available in this regard. This section was prepared to assist countries wishing to establish new criminal offences.

The third paper focuses on the victims of identity crime titles “Identity-related crime victim issues: A Discussion Paper” (ibid). This paper was produced to assist in developing strategies and practical action for combating identity related crime, improving communication between crime experts and victim experts and identifying areas in need of further research. The paper covers issues such as the range and types of identity-related crime victims, the legal bases for victim remediation, including an analysis of rights to identity reputation and privacy and finally, an inventory of state and private sector practices for victim support and remediation.

Public-private partnership practices are an important element of tackling crime which is an element covered by the fourth paper of this examination (ibid). “Identity Theft: An inventory of best practices on public-private partnerships to prevent economic fraud and identity-related crime” is the title of this chapter which lists an inventory of best practices. At all the meetings of UNODC, it was acknowledged that cooperation between the public and private

sector was essential in order to develop an accurate and complete picture of identity-related crime, as well as to adopt and implement both preventative and reactive measures against it. This predominantly covers the cyber aspect of this crime.

Finally, the handbook moves on to provide a practical guide to the international co-operation required to combat this crime (ibid). Because of the transnational dimension of identity-related crime, international co-operation is highly relevant for the success of many investigations. Due to significant differences between national and international investigations, the guide provides general principles of international co-operation to assist members with an overview of some of the most relevant case examples. Also, due to the complexity of the subject matter, the guide focuses on basic information and guidelines on how to best to deal with international co-operation requests in the field of identity-related crime.

Now that the UK has decided to leave the EU (the so-called Brexit), the question raised concerns the impact this will have on the UK's participation on the European level fighting this crime. Businesses have indicated concerns about the effects that Brexit will have on fraud in the UK, believing that with a potential lack of communication between the UK and the rest of Europe and an increase in trade with non-EU countries would make fraud in general harder to tackle. One of the major concerns amongst the cyber-security professionals was reduced information-sharing. However, the governments recently published White Paper on Brexit highlights its continued commitment to co-operation on cyber-security with European and global allies (HM Government, 2018). It is likely that after Brexit, the information-sharing arrangements agreed between governmental agencies will be replaced by bi-lateral and multi-lateral arrangements which would mirror the current agreements. Problems could arise, however, if the EU laws and regulations that protect businesses and individuals are not replaced by similar laws. One such regulation is the Network and Information Security Directive (NISD) (Directive, 2016) the first EU-wide rule on cyber security aimed at achieving a high common level of network and information security across the European Union.

Another concern is that there will be less cooperation between the UK's National Crime Agency (NCA) and Europol. Some experts believe this is unlikely because of the NCA's direct access to Britain's intelligence agency GCHQ and the indirect access to the NSA via GCHQ. For many, the belief is that the UK is too valuable to be excluded from co-operation around cyber-security and fraud prevention.

However, since the government will discuss and implement new agreements and procedures, including with the non-EU countries it will be trading with, this should help mitigate the potential increased threat. During the Obama presidency, for example, the UK and USA agreed to 'bolster efforts to enhance the cyber-security of critical infrastructure in both countries', and that agreement will likely continue and be enhanced after Brexit. By ensuring that new agreements and regulations are in place, the government can help reduce the threat of increased fraud from outside the European Union. Immigration and the skills gap are other major concerns in this area. However, it should be noted that as the cyber-security profession was already added to the UK skills shortage register in 2015, a key consideration has to be ensuring that any change in EU immigration, following the UK's departure from the EU, does not exacerbate the current skills crisis by closing off access to a key source of talent for UK technology businesses.

4.8. Responses from the public sector participants to key research questions

The previous section provided a comprehensive examination of efforts in the UK to acknowledge and address the issue with the introduction of NFA, attempts to measure this crime and introduction of cyber strategy which is a major element in the commission of this crime. To get a fuller picture of identity crimes within the public sector. I will examine the responses from the front-line identity crime prevention professionals. This will enable my research to establish the perception and experiences of these professionals and to capture their efforts in tackling this issue.

4.8.1. Perception of identity crime

Answers to the question on how identity crime is perceived inside their organisation cover a broad range of views and various terminologies are used to express those views held by the participants. Recurrent themes from respondents' perceptions of identity crime are of its size and scope, its complexity and its inherent danger/threat to society. One interviewee argues that this is a very difficult question to answer as identity related acts are not easy to understand (R1). Another participant perceives identity crime as high risk because of the ways an identity can be stolen and then used (R9). Another respondent (R10) sees that identity crime poses a huge risk because it can relate to anything whether it is an individual or a company or anything else across the spectrum (R10). Yet another interviewee sees this as a crime-type that comes up regularly in discussions and according to statistics it is a difficult and a prominent crime (R13). It is a serious threat to every man, woman and child in the country is how the third participant perceives identity crimes (R3) and a real and strong threat to us (R4). It is a key area and a priority (R8) and a big weakness (R22). It is rising and prevalent (R25 & R28) and a lot of effort is directed at it (R25) is how two other participants describe this crime. Some respondents shift the focus to society as a whole claiming that individuals throughout society have become very poor at protecting their identities (R3).

One of the respondents focuses on customers' (consumers') perception of this risk and states that because the customers do not understand how the technology works, their perception of the risk is much higher than the actual reality (R28). This is further emphasised by another participant who believes that there is a lack of awareness from the consumer perspective and also the business community (R22).

4.8.2. The various organisational levels with responsibility for identity crime

Respondents were asked at what seniority level identity crime was managed in their organisation. The representatives of the public sector indicate that within that sector, the issue of identity crime is dealt with at the highest level and there is a serious focus on addressing it effectively. The NCA has an identity crime specific project, ACPO has a portfolio to deal with this issue - all of which are at the highest level within these organisations (R1). But because the issue is so complex and 'cross-cutting' one government organisation alone cannot deal with it and therefore, several representatives from various organisations have to work together (R1).

In one organisation a team of 7 people work on the issue (R1). Another respondent states that they have fully qualified and educated staff (holding fraud investigation qualifications) working in their identity crime team (R4).

4.8.3. The nature of identity related crimes

Feedback on the nature of identity crime generated themes referring to its complexity, its role as a catalyst, and its organised and serious crime connections. Respondents expressed the fact that identity related crimes are of a complex nature and there is not a specific offence of identity theft in the UK (R1). This assertion was further supported by the statement that identity crime does not fit into one box and that every organisation affected by this crime deals with one aspect of it (R1). Specific identity-related crimes do not exist within certain organisations, and it is not investigated as identity theft or fraud, instead they are labelled benefit fraud or income fraud (R3). Identity-related offences were described as a crime type that enables other crime and criminality- especially the documents in a fraudulent name which are very valuable commodities for organised gangs. There is believed to be both an 'organised element' to identity crime and a 'volume element' (R10). The people committing this crime are linked to terrorism funding, human trafficking, public protection, serious assault and all the financial products that go alongside it (R10).

Organised crime gangs are believed to be behind attacks on one government organisation by using false identities or hijacked identities. The difference between a false identity and a hijacked identity in the first instance is somebody has made up a new identity and has managed to establish that with us, in the second, somebody has got enough information on an existing identity to take over that account and to come to us as though they were that

person (R3). One of the participants mentioned a case where IT professionals have been employed by criminals to do work for them believing that it was a genuine business (R28).

4.8.4. Current trends and MOs

One participant confirms that they had seen a decrease in identity fraud but they believe that this was due to criminals getting more money out of old identities rather than looking for new identities (R9). Another participant disagrees by stating that this fraud type has certainly increased over the last few years as there are more organised crime groups testing the water (R3). For another participant, 60% to 70% of their prosecutions for false IDs are foreign nationals. Therefore, there is an element of foreign nationals committing identity crime and attacks coming from outside the country by foreigners (R4). They have also seen an increase in people using EU passports such as French, Portuguese and Dutch (R4). Finally, stolen credit cards are also used to abuse the systems (R3) and another respondent focusses on a change of method stating that as the fraudsters cannot clone the new (credit/debit) cards they are trapping them (R22).

4.8.5. Impact of identity crime on organisations

Public sector organisations are both victims and facilitators of this crime. They are also impacted directly and indirectly (R28). Two respondents focus on the financial impact of this crime stating the way that they are affected is the huge amount of money that is spent to secure us against ID crime (R25) and that they spend a lot of money to ensure that customers' identities are safe (R28). Another respondent explains that organised groups directly affect all the systems of one of the participants using false or hijacked identities (R3). The other way that this organisation is impacted by this crime is that as they are a trusted organisation their identity is exploited to send others phishing scams (R3). Therefore, there are three ways that they are exploited: data theft, false identities and the identity of the organisation being stolen and misused (R3).

4.8.6. The definition of identity crime

Much feedback was provided to the state of play and challenges of this topic. There is significant disagreement between public sector participants on whether a finite legal definition of identity crime exists, whose responsibility is it to define it or whether indeed it is necessary for the effective functioning of their organisations. There is concern amongst some that the UK definition is not replicated by the EU or the USA, or even between the public and private sector (R25), whilst others seem happy that the definitions and

terminologies are sector specific and as used between them and their partners produce effective progress. Those respondents attesting to the lack of definition offer the following input-there is no formal definition (R10). A few years ago there was a debate at the European level as to whether a common legislation should be introduced which was rejected as members argued that domestic legislation should stay domestic but a common terminology should be agreed - but this was never done (R1). This lack of a formal definition is because there has never been a body that had the ownership for this issue (R1) but if we define it, the question is who would do it? (R1). A definition was put forward by the NFA but it was too broad, it could have been basically anything (R10). The disagreements tend to be what would constitute an identity- a name, address, date of birth? (R10). One of the prominent issues is whether to call it identity fraud or identity theft or identity crime. And there seems to be different opinions and different forums seem to have different names for it. As far as one participant is concerned there isn't an agreed definition and there seems to be quite a few of them floating about. (R8).

Those respondents who appear content that formal or informal definitions exist such that their work is not hindered provide answers as follows: The fraud Act which has made this as an absolute offence has provided guidelines for definition (R22), but the law is slow, especially in keeping up with the technological side of it (R22). There are commonly accepted terminologies, but nothing formally agreed (R1). However, some respondents believed that the terminologies within the identity crime arena are commonly accepted (R1 & R10). Definitions are very specific to each organisation (R4) and are in the context of each organisation's broader activities (R4). Another participant argues that definitions are context based in that they are created in the context of products or services that have been penetrated illegally by identity criminals. With another respondent stating that: "We spent a lot of time debating the issue whether we need an official definition of id fraud or whether we needed a crime made legal and we talked to ACPO, we consulted far and wide with the banking sector, what we found was that even though there was not a definition as such, there was enough legislation to actually function and where there wasn't we ensured that we updated the legislation" (R25). A lot of time has been spent debating the issue of whether we need an official definition of this crime. We found that even though there is not a definition, there is enough legislation and if there was not one, new legislation has been introduced to fill the gap (R25) but this lack of definition, in one participant's belief, has not affected the collective work on the issue (R25).

Views concerning the impact of a commonly accepted definition of identity crime between the UK and foreign governments produced the following feedback- In all areas related to this

crime we are the mature market (R9). To make matters worse the definitions in Europe are different and, in the USA, there are hundreds of pieces of legislation that have defined identity fraud (R25). There have been efforts on the international level (both EU and the wider international community) to solve the issue around definition and agree a unified definition to enable the efforts to go forward (R8). Another participant is more positive stating that not only are there definitions within the UK but that they are being shared all over Europe with other colleagues (R9). The challenge is believed to be how each organisation is reporting it and to bring in standardisation (R9).

4.8.7. The extent of the identity crime problem

Despite concerns about the methodologies used to measure the extent of the crime, the majority of the public sector respondents provided answers based on financial rather than social measures with estimates of the monetary impact varying widely. Most participants believe that organisations are finding that this crime is on the increase, especially over the last 3 years, with organised criminal groups testing different methods of identity fraud. The reason for this increase is due to people being much less careful about their identities (R3). One participant stated that identity theft is really difficult to measure as there are so many types of fraud (probably 5 or 6 types) that constitute identity theft that begs the question "how do you actually measure it?" (R28). The few efforts that were made to measure this fraud are considered reasonably inaccurate making it very difficult to get real handle on the figures (R1). This is made even more difficult by the fact that a lot of companies do not report it and just write it off as bad debt (R1). Another participant states that it would be very useful to have an accurate figure for this crime and although there are case studies and other information that is available and is of value, they are not the true picture (R1). A typical problem is highlighted by the same respondent stating that there is no central point of measurement and no central point of collection of intelligence. There are lots of IT systems, each police force has its own IT system, but they do not talk to each other (R1). Notwithstanding this background, two participants are prepared to put a monetary figure on the extent of identity crime one believing that the real number for identity related crimes is £7 billion and even that is a conservative number and that bringing identity related crimes to a halt would make a significant impact on the life of this country (R3). Another argues that the figure for this crime is £32 billion - but this is not comparing like with like (R8).

4.8.8. The public sector's knowledge of victims

Comments here range from respondents not having to deal with victims at all, being aware of the financial and non-financial impacts on victims, being critical of the victims' lack of

knowledge which leads to becoming victims and how difficult organisations find it to stay ahead of the fraudsters. As stated, one respondent replies that they do not work with victims simply because they do not have the resources and the number of stolen identities far exceeds the number of staff that they have (100k identities and only about 8 or 10 staff). But guidance and assistance are provided to those victims who get in touch (R10). Other respondents focus on how the impact of identity crime can be devastating on victims, impacting their ability to function in the financial services world and even more so, on a day-to-day basis such as not being able to pay their rent and bills (R9). Becoming victim to credit card/ATM fraud is another's focus especially linked to the lack of awareness of this crime by the public. There have been instances where fraudsters are changing the face of an ATM and are putting a fake one instead to steal identity data and there is a long queue of people waiting to use the tampered ATM (R22). However, one interviewee states that it is difficult to distinguish scammers from genuine victims as the scammers pretend to be victims in order to get into banks (R10). Another interviewee expresses the belief that due to the widespread impact of identity crime, 'the whole tax-paying population' is the victim (R3). On the non-financial side, two respondents report on the social impact caused by a severe form of victimisation - when the identities of the victims are used by paedophiles (R25) or the impact on parents when a dead child's identity stolen which can be even more traumatic (R9). Not all individuals have the expertise and knowledge about what to do if they become a victim of identity crime (R22). But one participant believes that there is enough support for the victims to help them deal with the issue. Action Fraud is believed to be the starting point, credit reference agencies to help restore their credit reputation and CIFAS for protective registration (R27). It is not only individuals who can become victims of identity crime. Both businesses/organisations may also become victims of identity crime (R25). It is difficult for businesses which fall victim to this crime to stay ahead of the fraudsters as the criminals are very persistent and are constantly discovering access routes to compromise the data held by the private or public sector (R22).

4.8.9. The knowledge of offenders amongst public sector respondents

Generally, law enforcement agencies are the best informed as they "have a very good understanding of the offenders due to the nature of their job since they will need to have all the data about a suspect" (R1). One participant state that they do not know much as this is a matter for the law enforcement (R2). However, most other organisations do not have information on offenders yet, on rare occasions, academics have been employed to undertake studies in this area (R9). There is a lot of anecdotal information (especially in the media), but is very difficult to determine how the identities have been stolen let alone

information on offenders (R9). One participant believes that there are a lot of Romanian organised groups that carry out the cash point identity crimes. The Bulgarians tend to cover the south of Europe and southern Ireland whilst Romanians operate mainly in northern Europe and Northern Ireland. There is a split across Europe with Bulgarians controlling the south side and Romanians the north. However, the petrol station identity thefts (criminals) are carried out almost exclusively by groups that are of Sri-Lankan origin and which are family run. There are also a few South African and Iranian groups (R22).

4.8.10. The public sector organisations' objectives regarding identity crime

There seems to be broad agreement amongst respondents from non-law enforcement public bodies on the key objectives at the strategic level. These government organisations work towards the following objectives identifying fraud, prosecuting it, stopping it from happening, learning from identity fraud committed and updating systems accordingly. Additionally, being a trusted and secure source of intelligence and information, having an identity fraud reduction focus, raising awareness by campaigns and finally conducting research to feed into investigation and protection (R3, R4, R8 & R25). The objective for law enforcement agencies is to design risk management tools to prioritise that for the highest risk categories, arrests are made and the individuals are prosecuted but for medium risk a disruption based strategy is used such as revoking someone's license, revoking their insurance, cancelling enhanced disclosure certificates enabling them to work in certain jobs and in this way the risks are reduced or minimised and finally, implementing a prevention strategy which is working with partners to reduce the risks of people becoming victims of this crime (R10).

4.8.11. How objectives are set in the public sector organisations

Responses were provided on the governmental process, non-government public bodies and law enforcement agencies. At the government level Ministers become aware of the issues through discussion in Parliament or through the relevant people who work in this area. Civil servants then present the opportunities to Ministers to work on those issues and Ministers say yes or no (R1). But when the next Minister or government comes to power they may not agree with the work and may change or stop it. It is stated that the Home Office is consistent in that it has Civil Servants who stay behind each of the governments who continue on-going programs at work that go beyond each government. But once the government changes the new minister may not agree with the previous government's work plan and may decide to change it as different governments have different agendas - so one government may have a project on identity crimes, the other may stop it or cancel it (R1).

Other public sector organisations have a broad of task force to oversee the production of a threat assessment. That threat assessment is put forward to members of working groups for agreement then that threat assessment will be taken as the position of the organisation and will be used to prioritise and for actions (R8).

For law enforcement agencies, the priorities are set according to the level of risk any given problem presents. Certain things are obviously higher risk, and they have a risk management tool enabling them to identify the higher risk (R10).

4.8.12. The objective-setting process

The objectives for some government organisations are set by Ministers (R1) others have Steering Groups with Chair and Deputy Chair who would agree on issues based on evidence that would then be reported to Ministers (R25). And finally, one respondent states that it is set by government centrally, taking into account the learning and advice of the respective organisations (R3).

4.8.13. Public sector identity crime detection methods

Responses here indicated a basic IT systems approach supplemented by ad hoc victim input. Two respondents state both manual and software detection systems are used. Some methods have been there for a very long time - but new detection methods are developed as problems arise and patterns can be identified (R3 & R25). A dedicated risk and intelligence service that monitor different patterns of behaviour and different patterns of application looking at number of forms/application from certain parts of the country (looking for unusual increases in the number of applications) (R3) number of changes to an account, looking to see if the changes are credible (R3). The potential victim input usually arrives by telephone - what generally detects fraud is when somebody phones to ask why his/her account has been changed, stating that they have not made the changes so that highlights an issue (R3). Once a problem is identified, interested parties are identified and brought together and the resources are allocated to form a single point of responsibility (R3).

4.8.14. Identity crime prevention and mitigation methods employed

Contributions were made mainly by respondents from law enforcement agencies which operate 3 streams of work. The first one focuses on a database containing information on counterfeit and false documents (R10). The second work stream is an enforcement team that acts upon the intelligence obtained from the database (R10). And finally, maintaining relationships with the specialist printing industry suppliers. The fraudsters, in order to create

counterfeit documents, need specialist printing equipment and in most cases, pay cash for them. It is easy to identify when a genuine business makes the purchase or a fraudster's does. The printing industry suppliers are given the criteria that would make a purchase suspicious. Then the necessary checks are made to see if there is intelligence and information to corroborate their suspicions into actually "yes this printer was going into a printing factory" or actually "we have got a fully-fledged id factory there" (R10). Similar processes are being examined to have the same processes in place with the companies in the second-hand market such as E-bay and Gumtree. Efforts have been made in the last 4 years to try and get new legislation through to make it a new offence to knowingly sell specialist printing equipment (R10). Sharing data with government and non-government organisations is another way of tackling this crime (R10). For one respondent, the tactical responses are focused around the IT systems, working with other agencies to control or restrict the enablers of identity fraud, prevention messages, mitigating efforts which are about reducing the harm to the victim and repairing one's account (R20). For another participant preventing this crime is about devising new initiatives to tackle it, spending millions of pounds to create a system whereby you properly collate intelligence and assess intelligence and share it for prevention and create targets to go and arrest and enforce and re-create the cycle again (R1). A further focus on crime prevention methods is the cost of creating and maintaining them - tackling this crime is a risk-based approach prioritising according to the budget (R1).

4.8.15. Organisations which operate within partnerships

Respondents report that 8 years ago there was very little cross government action dealing with identity fraud but that changed with the introduction of identity cards when the Home Office established the Identity Fraud Steering Committee. Public and government organisations, such as the Home Office, IPS and others work with the following organisations: DVLA, HMBO, HMRC, DWP, Various police forces, Other small organisations, CIFAS, FFA UK, UK Payments, Charities commission, UK Border agency, Home Office Operation , Game masters Licensing, UKPI, DWP, HMOP, Met Police, SOCA, FSA, Royal Mail, DVLA, National Crime Agency (NCA), IPS, HMRC, IFSC, Home Office, Academia, City of London Police, CML, Finance and Leasing Association, ACPO, Police forces, Banks, Retailers, Building societies, Utility providers, MOPS, Other credit reference agencies, Trade associations, Identity consumer awareness group (IFCAG) and finally Identity steering committee group (IFSC).

Law enforcement work with the following organisations: government and non-government agencies, financial institutions, DBS, NFIB, HMR, DVLA and IPS.

4.8.16. The context within which these organisations collaborate

The responses indicate that the various co-operations are driven by regular communication on the dissemination of information and as a response to changing or developing trends. In partnerships, members work with different organisations for different reasons such as working on shared responsibilities and problems but on a strategic level the efforts are focused on governance, tactical and intelligence (R3). What falls out of committee meetings dictates what the partnerships will work on and with whom (R4) which will be about intelligence sharing and establishing trends (R4), intelligence sharing on organized crime and prevention methodologies (R13). Law enforcement agencies work on intelligence sharing and identifying trends, document verification (R10) data sharing (R20 & R28), and finally, personnel training (R10).

4.8.17. Responses on the effectiveness of these collaborations

Feedback highlights the lack of consensus on this issue with those professing their effectiveness often continuing by criticising shortcomings and problems that need to be addressed to improve effectiveness. The role of data processing and the challenges of data sharing is internal to the public sector. On a strategic level, these collaborations are believed to be quite effective working through some of the policy issues and making sure that each of the organisations has an understanding of the other (R1). The more challenging part is the tactical operation level. In the nice cosy environment of policy and strategy it is easy to get the right people around the table and in on conversations. In the day-to-day dirty world of actually getting the job done, it isn't quite so clear cut (R1). Partnerships are effective in bringing the right people together, but the challenge is to join up operationally (R1). It is believed that some parts work better than others (R3) and that when there is a shared problem the co-operation is more effective (R3). However, when it is not exactly the same, different organisations will have different systems and the systems may not match together (R3). Sometimes there are barriers in getting information backwards and forwards and there are difficulties in trying to understand what each party wants out of the partnership (R3).

One participant argues that partnerships have been extremely successful especially in relation to deceased persons' data when that information was made available by the General Register Office to the private sector to help them with fraud. Secondly, when the Serious Crime Act was introduced this enabled the public sector to have legal gateways to share

fraud data with the private sector through designated fraud organisations (R9). Another participant believes that it has been effective in curbing the growth of identity fraud (R12) and yet another states that the partnerships are very good at talking back to little audiences. People tend to follow an audience so taking the whole idea of fraud and identity fraud to so many different arenas has been helpful (R13).

Four respondents' comment on data sharing among partnerships stating that partnerships work well but there is a much wider issue about data sharing because of the Data Protection Act. Additionally, criticisms have been made on the partnerships not being proactive - it can seem as if there are lots of activities going on, but very little actually changes - the old phrase 'talking shop' is being used to explain the lack of achievement by partnerships (R8).

One public sector respondent highlighted the role of private sector companies and their activities in identity verification, stating that a sub-group needs to be set up with the private sector just to look at the issue of verification on how that can be taken forward. There are a lot of commercial companies that are now active in the field of identity verification, offering verification services of various standards. For example, all the credit rating agencies provide document checking services, some of them incredibly sophisticated and some of them fairly basic. The solution probably lies in the commercial sector itself that the market will dictate how this is taken forward. As these commercial companies compete with each other, they will come up with new ways of verifying staff and new services. So, a sub-group mainly made up of private sector would be beneficial (R8). The private sector is criticised for not doing as much as they should even though they can and that is, because for them, fraud is part of their normal day-to-day activities and a small part (R25). Notwithstanding this view, other respondents state that the private sector is believed to be more proactive in sharing data because the private sector is believed to have other (profit generating) priorities. However, austerity has made them more proactive since they are trying to save money (R10) some better than others (R20). One public sector respondent states that, regarding data sharing, public organisations are not able to do so as freely as the private sector as they are heavily bound by the Data Protection Act. Attempts have been made to introduce legislation in this area in order to make it easier to exchange data and information with the other organisations (R25).

4.8.18. International collaborations

Respondents offer views on partnering with the USA/Canada and the EU which, whilst approving of efforts, are mainly critical of results. There are international efforts to work collectively on the issue, such as working with the USA and Canada, but in order for that to

be successful there needs to be an agreed definition so that the parties know what will be covered in the collaborative exercises and what the scope of the work will cover. The definitions need to be agreed by all the member states (R8).

Within the European Commission, the UK market is looked upon as the mature market in the arena of identity crimes (R8). The EU commission has also set up a group to take forward the issue of identity crime. But it is believed that firstly the progress with such forums is slow and that the representatives of these forums are very mixed in their seniority. Some send high level government officials, some send police officers, and the others send "whoever was available" (R8). This makes collaborative decision-making and agreeing to proposed work difficult as some of the attendees are not in a senior enough position to agree or disagree and have to seek advice from higher authorities and therefore cause more delays in agreeing to actions (R8). In summary, one respondent's feedback distils the essence of views about partnerships which is that "International cooperation is a dream and national cooperation is a nightmare" (R22).

4.8.19. Tackling identity crime

A number of themes on what additional actions need to be taken to combat identity crime in the public sector emerged from the answers provided by the participants. Of prime focus are, more funding, the prioritisation of projects, attention to the most vulnerable groups in society and some techniques which should be employed to tackle identity crime. One respondent commented that there is a lack of money available to direct to this area. The government is struggling with this issue, so it has to be given priority in terms of risk to society and fiscal losses (R1). In addition, from the government perspective, this issue doesn't sit with any current issues so new initiatives need to be developed and large sums of money are needed to create a system whereby intelligence is collected and collated and assessed and enforced and the same cycle is created again (R1). Continuing, the respondent adds that new initiatives need be devised and introduced constantly and there needs to be an acknowledgment (and taken into consideration when devising strategies to tackle this crime) that no single, simple solution exists for this problem (R1). Another respondent states that "it is a balancing act" (R10) whilst another observes that developing solutions takes time and implementing secure methods across large organisations is expensive and time consuming (R2). Focusing on complexity, one participant comments that doing something about a specific vulnerability sooner and quicker is needed, but this is challenging within big organizations, especially considering that the customer service teams within the big organisations are more focused on customers and avoiding too much inconvenience and

restrictions (R10). Focusing on the vulnerable sectors of society, one respondent advocates the shift in priorities to the vulnerable sectors and argues that attempts need to be made to recognize the most vulnerable sector and to widen partnership work and raising awareness (R25). Agreement comes from another respondent who believes that the way forward is to agree a program of actions so that once the most harmful things are highlighted, they can be dealt with (R8). Two participants agree on a shift of focus in tackling identity crime, one stating previously the focus was on money laundering and anti-money laundering in order to maintain the City of London as the world leader in financial services but that has changed (R9) and that there is a lot of work being done at the moment and that identity fraud has a much bigger profile now with it assisting the funding of the 9/11 and 7/7 attacks (R9) and that bodies such as IFSEC do a good job but its remit needs to be wider (R25). Another respondent focuses on tactics stating criticism is made about the lack of understanding about the subtle differences between prevention and disruption in the current attempts with tackling this issue (R10) and that, in an ideal world, the priority tactic would be horizon-scanning, something that has been proposed by a lot of people (R10).

Prominent issues, weaknesses and concerns

Respondents were asked to comment on their concerns on the state of the identity crime prevention landscape and offered a number of views covering the profile of identity crime which their feedback included cyber-crime, basic identity documentation, the speed and flexibility of identity criminals and the need to improve international co-operation. On the profile of identity crime prevention, two respondents state that the biggest challenge in this area is that all organisations have an interest in identity yet it is not a priority for anybody (R1) and that it is only recently that this issue has received enough attention to get its own MP (R20). On cyber-crime, three respondents offer views stating that identity crime, along with cyber-crime, are huge emerging issues (R4), that traditionally burglary used to be the most intrusive crime but that is changing because identity crime is more personal (R10) and that “the cyber issue is the second biggest challenge that exists in this area as fraud has moved to the internet and online and the internet is allowing criminals to sell and purchase identities without visibility” (R3). There still is a lack of proper understanding about the impact of cyber-crime. The criminals do not have the restrictions that normal people have on this medium as they have access to large amounts of money and technical expertise and that way we are always playing catch up. The way business is conducted in cyberspace needs a fundamental change (R3). One respondent highlights that cyber-crime is an international issue therefore collaboration with International colleagues is a must (R1) whilst another respondent highlights that this crime has become “global but we still have county police

forces. We are a global community with global fraudsters and yet we do not have the same global law enforcement to tackle the issues, even getting permission to go to France on the Eurostar that takes a mountain of paperwork." (R3). Referring to the weaknesses in current identity documentation two respondents state that there are only two identity documents in the UK, the birth certificate and the death certificate, which makes the birth certificate the only official identity document during one's lifetime in the UK. However, there is a myriad of other documentation that is being used for identification such as bills, passport, driving license and professional body identifications (SIA security badges). A possible weakness is that none of these documents were designed for identification purposes (R10). Additionally, a lot of money is spent on creating security features for these documents, but no one actually knows what these security features are (R10). Making sure that people in positions of managing the checking of identities can differentiate between genuine and false identities and therefore being more confident of the decision -making process at application stage is vital (R10). Biometrics is believed to have its own weaknesses in the sense that it could increase violent attacks against individuals and the false reading that could happen, for example, if it is a voice-recognition, if the person has a cold it could not recognise their voice (R22).

Awareness-raising and education

Respondents comment generously on the role of and need for improved education for the general public. Educating them about what their identity really is vital (R10). There is a reliance on the public's personal security practices rather than giving them something completely secure (R22). Prevention messages need to be stepped up, but this will be quite challenging because as soon as an area is focused on, the fraudsters move to something else such as the fraudsters' latest move to social media (R1). One participant believes that there is still a great deal of work that needs to be done to educate the public about protecting their identity information, such as on computers. There is still a need for educating people about the threat of phishing emails as people are still falling for such scams (R3). People need to make sure that the website they are visiting is the right one and it is a well-known one and to get advice before spending money (R13). More work also needs to be done to change people's perception about this crime. One, we need to start accepting that this crime is more intrusive than burglary (R10) and two, to change the romantic view of people about this crime which is just a guy sitting behind his computer. This crime involves terrorism, attempted murder and arson amongst other crimes (R9). However, there are behavioural and cultural problems to consider. Many respondents believe that identity crime is a cultural issue because individuals like to obtain goods and services quickly and without fuss and this

attitude and behavior creates the weaknesses exploited by criminals (R10). A balancing act between security and ease/speed is needed. There is too much weight on ease and speed at the moment (R10). People are greedy and reckless with their money and therefore, more efforts need to be directed at changing people's approach in that, if it is too good to be true, then it is not true (R13). Public awareness and education is crucial and teaching people how the scams work is very important (R22). For example, one effective method that was employed in Denmark was to feature scams on a "soap opera" on national television. This showed the public how the scam worked and educated them (R22). Individuals also fear revealing that they have fallen victim to this crime in case they lose credibility in their community. The same thing applies to brands, businesses and the market (R22). On protecting the credibility of organizations and private businesses, one respondent laments that marketing takes over fraud awareness-raising with leaflets (R9).

Law enforcement agencies

Public sector respondents provided several insights into the role and performance of law enforcement agencies highlighting their lack of resources, lack of reaction speed, lack of knowledge and lack of adaptability. At the moment, hundreds of thousands of new crimes are being committed in this area but actually no form or manner of how to investigate them exists (R10). It is not something that law enforcement could manage (R10). One respondent believes that questions need to be raised about how many of these cases are investigated with the limited resources that law enforcement has available to them (R3). A single identity fraud case is less likely to be investigated by police in a department that has tens of thousands of cases (R3). Ideally every case should be investigated but due to lack of funds that is not possible (R3). One respondent comments that this is an issue that is still not easy for law enforcement to understand and get their head round (R20), another noting that identity crime doesn't feature anywhere in the high-level plans which is the correct thing as it cannot be treated as seriously as a murder, rape or not even a road death (R1). This respondent continues stating that the law enforcement agencies do not have the technical expertise to understand identity related crime. This crime type is not as straightforward as, for example theft or burglary. Additionally, the legislation is not as clear as it should be, there are some grey areas and this falls between "some of the cracks of policing" (R1). Conversely one of the participants explained how effective it had been to demonstrate to the jury and the judge in court, the technology that fraudsters use to commit identity fraud (R22). One of the difficulties that exists in prosecuting complicated identity crime cases, is that when the technical expert is put in the stand, he/she can only answer the questions that the prosecutor asks and cannot go on to explain what has happened (R22). In one of the court cases, a

barrister actually asked, what is “a google”. The jurors tend to have more technical knowledge than the legal team (R22). The same participant continues talking about the police IT team not being knowledgeable enough to deal with the IT issues, that most police forces do not have computer forensics, technology is moving too fast for the law to keep up with and that technical expertise needs to be developed within law enforcement (agencies) rather than just brought in (R22). Another respondent concedes that criminals are moving very quickly from one offence to the other, for example, the offender could be selling drugs on Monday, but he realises that the risk is too great for dealing drugs, so he changes to doing identity theft and fraud on Tuesday where the risk is lower but the resources of law enforcement cannot move themselves and their priorities this quickly (R10). One respondent claims there is a political issue related to identity crime and that is the fact that law enforcement is reluctant to tackle this crime as if they start to record and report it, it will raise the published crime rate (R10) whilst another argues that the police treat theft in a way that it is depriving people from their property, yet identity theft is only considered an enabling crime (R1). Indeed, some participants believe that there is no need for a new identity fraud offence in UK (R1 & R3) or that only legislating against the theft of identities once the thieves have misused such information is the correct way to proceed (R10). Despite the shortcomings and issues with the enforcement of this crime, some successful partnerships have taken place between the police and other organisations. One respondents refers to a successful project where they collaborated with the police on the national fraud prevention week called “Operation Snow Trigger” where each individual force were provided with their top 15 addresses that had been used for identity fraud. So, then the right messages got out. It is believed that the public love doors kicked by police, but the message that came out of the exercise was that it is not just identity fraud alone. It is the start of a journey. It allows people to see instances of people being arrested and being put through prosecution, who were involved in drugs, terrorism, passport factories, credit card fraud rape, arson, attempted murder. It is evident from the text above how important it is for the public to see that law enforcement is actually dealing with this issue (R9).

Data-sharing and authentication of identity

Respondents offered comments on these areas lamenting a lack of a central database and the lack of participation by all organisations in effective data sharing. There are still organisations that choose not to share data but the issue, and the need for a better process to share data, has been discussed at length in various working groups. There is a serious need for a central database to deal with identity crime (R4). In addition, people need to be more active in data-sharing and not to have to jump through a myriad of hoops to enable that

to happen (R4). The single biggest impact in this area would be an effective coordination of intelligence rather than the current fragmented activities (R1). The same criminals attack different organisations which makes sharing information so much more important. The single impact needed in this area must come from an effective co-ordination of intelligence rather than the fragmented approach that exists at the moment (R3). The importance of authentication of source (feeder) documents was also stressed with one respondent stating "It is almost like let's rush the application through and deal with the issue afterwards" instead of actually dealing with the issue at the first stage because if it is dealt with afterwards it would be a spider web. If you get a bank account, you can have this, and you can have that, and you can have the other, so you have several breeder documents that go into it. You have a big spider web of things that now you need to shoot down and deal with whereas, if the first time you go and use a document to apply for a bank account you shoot that down, and I can make a bank account absolutely useless to you, then I have no problem (R10)

4.9. Discussion

Identity related crimes, in common with most crimes, are influenced by politics. One government may introduce a measure but there will be no guarantees that the next government will continue the work. It is more important to be seen to make efforts to tackle this issue than actually tackle it. This is having devastating effects on a crime type that not only impacts everyone in society, but also has a negative impact on the integrity of the whole system. There is a conflict between what the government perceives and what it is prepared to do to address the issue. The perception of this crime is that it is a priority, but the actions and efforts do not match that perception. This lack of taking responsibility was evident from the formation and the subsequent dissolution of the NFA and the political climb-down surrounding the aborted attempt to introduce identity cards. Considering that this crime is an enabler of other crime types such as terrorism, human trafficking, drug-trafficking and others, it is surprising that the government is not taking more of an active role in this arena similar to that of cyber-crime as these crimes have the potential to heavily impact the healthy functioning of our society.

Identity is a very diverse concept which makes identity crime a very complex issue. Different organisations label it differently which in turn is making defining it and measuring it accurately very difficult. This is a full-spectrum crime in that it has a volume element as well as single-attempt high-value loss element to it. It is opportunistic as well as highly organised with links to serious organised crime. So why is it that government is addressing other

serious crimes and not identity crimes? Despite this lack of ownership, some participants stated that a lot of effort and money is spent by government to tackle this issue and others argue that more money needs to be diverted to this area. Additionally, the lack of ownership of identity-related crime by government is believed to be the reason for the lack of a formal and widely accepted definition.

The lack of proper understanding about this crime is impacting how it is perceived, especially by consumers. Their perception of the risk is much higher than the actual victimisation figures, a theme that also emerged in the National Statistics Survey (2012) and in Jordan et al. (2018) which has already been highlighted in the literature review of this research. There are disagreements between the practitioners as to the severity of this crime because solid, reliable data do not exist. The data that have been quoted by interviewees have huge discrepancies in them. To add to the confusion is the fact that each organisation is experiencing this crime differently, one may have large numbers of attempts made by identity criminals against their services but another one may see fewer attempts (but larger value crimes) committed against them. As was highlighted earlier, some people are not reporting to Action Fraud and reporting to the police instead who do not have the mechanisms to capture and include it in the bigger picture for this crime. There are also those victims that do not report it at all. Therefore, the assertion that the number currently being stated as the amount of losses is incorrect would appear to be accurate.

Generally, the plight of victims is acknowledged by most participants. One even goes further by stating that there is enough support for the victims, which as stated earlier, is not the case. Looking after victims or developing a better understanding of them is not on the agenda of these organisations at all. They believe there are far more important issues on which to focus. Huge gaps still exist in adequately addressing the issues related to victim support. Despite the heavy presence of needs for education and awareness-raising the organisations in charge of delivering those measures are outsourced and not effectively run. This finding emphasises the point made by Wall (2013a) that argues a new law to help victims is required.

The knowledge of the public sector regarding the offenders is very poor at best and contradictory at worst. One participant argues that law enforcement has the knowledge but this is not a priority for them and so they tend to refer the identity crime cases to Action Fraud, so how could they have developed this knowledge? There are, however, very small units such as the DCPCU or the small unit within the Metropolitan police (Amberhill project) who do have some knowledge about the identity criminal fraternity, but this is not

representative of law enforcement in general. And since their focus is mainly on the organised crime element of this (as they tend to work on cases with very high losses) they may not have the full picture regarding the nature of the volume-crime identity criminals. What is disturbing is that some participants look at media to get their information on offenders. Some, however, recognise the diversity of offenders in this area across a spectrum spanning entirely opportunistic criminals to organised gangs. The attention of these public organisations is mainly focused on the broad range of non-offender-based crime-prevention strategies.

The efforts employed are risk-based approaches mostly aligning themselves with the SCP theories. In the literature review, Newman (2009), Archer et al. (2012) and White and Fisher ‘s (2008) views highlight the importance of SCP and suggest the application of these techniques to the fight against identity crime. The data indicates that the public sector professionals are well aware of the value this theory presents and are already using it widely. Data and intelligence sharing are themes that have strongly emerged in the efforts to tackle this issue. The current data-sharing practices mostly focus on MOs and new trends. They also align with the deter, defend and develop pillars of the Cyber Security Strategy.

All major public sector organisations impacted by this crime participate in partnership/multi-agency activities. Data-sharing is the most prevalent activity within the partnerships in which the public sector participates.

The NFA’s basis was to build on the partnerships that already existed and provide direction for them. Information-sharing has become such a vital part of preventing identity crime that Action Fraud was established to collect the data. Now with NFA disbanded, the risk is that the aggregate of this crime (as it currently includes so many different crime forms) will not have the necessary visibility that it requires.

Most participants believe that these collaborative efforts have been effective and add value to the general efforts in tackling it. However, criticisms have been directed at the lack of achievement by one participant and that when these partnerships are examined it seems that lots of activities are happening but not much is achieved, (mirroring Gilling’s (2005) argument of calling some of these efforts ‘talking shops’). Strategically, these partnerships are believed to work well, this could be because at such high levels there is more mutual ‘consensus’. It is at the operational level that problems arise. To make these partnerships more effective, shared expectations need to be developed and one of the issues that need to be addressed is the restrictions that currently exist with the public sector sharing data with

each other and the private sector. This is evidenced by the data that CIFAS handles as their membership mostly consists of the private sector and not the public sector.

Tackling this issue has three hierarchies: local, national, and international. There are partnerships at all levels discussing and working to tackle this issue. Different countries have different approaches to identity crime prevention, therefore, it makes it even more challenging for partnerships on an international level to work together adding the fact that different countries also have different laws. Additionally, this is a global crime issue, but local regulations are used to fight it further making the fight an uneven war (Fraud conference attended in 2010).

In summary, from the perspective of public sector professionals, there is a lack of ownership and real determination to apply adequate resources to tackling identity crime. As a result there is no clear definition of this crime which would aid meaningful data analysis, clear up the perceptions of it reported among respondents, lead to a better understanding of victims and their treatment and enable a better understanding of the range of identity crime offenders to aid law enforcement agencies. The value of SCP theories and methodologies was broadly acknowledged by the respondents but, in the absence of the NFA, the desire to seek effective data generated a move to seeking partnerships and collaborations (local, national and international) upon which there are mixed views amongst respondents on their efficiency and effectiveness.

5. Identity crime from the perspective of the private sector

As stated earlier, this study aims to provide an understanding of identity crime related issues from the perspective of both public and private sectors. Having captured the perceptions and efforts to tackle this issue from the public sector in the earlier chapter, I will now examine this issue from the viewpoint of the private sector's front-line professionals. This will enable this thesis to make comparisons between the two and highlight any differences and similarities. To do so, this chapter is split into two main sections. The first focusses on identity related crimes from the perspective of the finance sector whilst the second consists of the responses to the interview questions by the respondents from the rest of the private sector.

5.1. Identity crime from the finance sector perspective

5.2. Introduction

The finance industry suffers the most at the hands of identity criminals which is why it is important for this study to examine it in more detail. As highlighted earlier, through employment in the UK Payments Association, I had access to valuable (and not available to the public) information and observations that helped significantly in shaping this chapter. Additionally, this sector is the only industry that systematically collects data on the losses incurred by identity crime and which has established orderly and organised methods in collaboratively working on this issue.

To commence, different types of financial identity crime will be examined which will include counterfeit payment card fraud, remote purchase fraud, lost/stolen card fraud, card identity theft and finally mail-non receipt payment card fraud. This examination will include the monetary losses generated by these types of fraud over the last 20 years and the specific measures developed by the finance community to address them. As there are other non-card related fraud which contain elements of identity crime such as cheque fraud, online and mobile banking, telephone banking fraud and money mules, these will also be discussed.

The UK payment infrastructure is a complex web of institutions and players all working together to deliver the services and products that have become such a fundamental part of everyday life. Key entities will be listed and discussed briefly including schemes, issuing and acquiring banks, FFA, DCPCU, data processors, merchants, vendors and credit reference agencies. Vulnerability within any of these entities would cause compromise in this cycle.

The chapter will then progress to highlight the significance of media and academia in the efforts to tackle identity crime within the finance sector. Emerging criminal methods will be examined next followed by the increasingly frequent data compromises that have occurred not just with the finance sector but also other industries and government organisations.

The compromises caused by internal staff play an important role in the arena of identity related crimes. This is an issue at which the finance sector (and others) is constantly deploying significant resources to identify and combat.

The chapter then examines the major vulnerabilities present within the finance sector, such as data authentication, which presents huge challenges along with KYC (Knowing Your Customer). Online services, customer vulnerability, staff recruitment and documentation are recognised as other vulnerabilities inherent within this sector.

Organisations in the finance sector use several strategies in their efforts to tackle identity crime, chiefly information management, communication, situational crime prevention techniques and data sharing. However, when examining the SCP techniques employed by this sector, it was discovered that rarely did its organisations avail themselves of the full range of these techniques and put them into action, thus recommendations have been provided to those organisations to enable them to address this oversight.

5.3. Identity crime and the finance sector

The UK's financial sector is the industry that has been most affected by identity crime. One of the key reasons behind choosing this sector for this research project was because it collects and transparently (to some extent) shares data on the amount of money lost to fraud and also shares some of the techniques that it uses to tackle it. A plethora of information can be found on fraud issues on the leading websites of the financial sector. No other sector (insurance, telecoms or even retail) publish such data or give identity fraud and fraud in general such prominence. The monetary losses that this industry suffers runs into hundreds of millions of pounds each year. This is not surprising since the products and services offered are very attractive to the criminal world. Fraudsters understand the effort/risk/reward dynamics of cracking the security measures put in place by this sector to steal information, including identity data, that they can then use to either acquire financial services, or other services, for free or to commit identity fraud. These efforts are made more effective by the weaknesses and vulnerabilities that exist in the financial systems and products under attack.

In terms of fraud figures, the financial industry is the only sector that publishes data independently on a regular basis with professionalism and rigour. This data is voluntarily offered monthly to the Fraud Control Unit of UK Payments Association by its members (that consist of UK banks and financial institutions). They then use this data to produce various reports which are circulated to their banking members. Bench-marks and thresholds are also driven from this data to help members set their goals and objectives. This data is then published twice a year to communicate to the rest of the country the amount of losses that are incurred by the payment industry. These figures, however, only represent the fraud that has been reported by bank customers or discovered by banks themselves and do not include those frauds that have not been reported and those that are written-off as bad debt. Part of this data is also included in the national identity fraud figures.

Plastic card and identity crime were included in the British Crime Survey results as a one-off exercise in 2005/06 (Hoare and Wood, 2007). Although this research is outdated it produced interesting results. An analysis of the findings of this BCS undertaken by Jacqueline Hoare and Charlotte Wood brings to light very interesting results. They emphasise that the result of their study should not be treated as the full picture of these crimes because not all identity fraud types were covered in the BCS and they were only able to conduct this research because a supplementary module on plastic and identity crime was provided, for the first time, within the 2005/06 edition.

The findings indicate that eighty-three percent of all adults had used a plastic card in the last 12 months, with 35 to 64-year olds being the highest users. Four percent of card users had been a victim of card fraud in the last 12 months. Fifty percent of card users said they were fairly or very worried about being a victim of card fraud, a level that is higher than any other crime type. Men aged between 35 to 44 were more likely to be victims and women aged between 25 to 34 were more likely to be worried about being a victim. Victims were more likely to be worried about payment card fraud than non-victims, two percent of adults were victims of identity fraud and one percent had their card details used without their permission. Only one percent had their passport, and two percent their driving licence, lost or stolen.

As Hoare and Wood (2007) explain, the BCS this study did not aim to provide an estimate of the extent of fraud within its main crime count. These incidents, which involve the theft of a plastic card for example, are included within the count of the appropriate offence category, such as robbery, however, subsequent fraudulent use of stolen cards is not currently included within the main crime count. Unlike this one-off exercise, the finance sector has

been providing figures on financial identity related crimes which will be examined in detail in the section below.

5.4. Different types of financial identity crime

Financial Fraud Action UK (FFA) is the part of UK Payments which is responsible for leading the collective fight against fraud on behalf of the UK payments industry. FFA categorizes identity related payment fraud into 5 different types each of which will be examined closely: counterfeit card fraud (including ATM fraud), remote purchase fraud, lost/stolen card fraud, card identity theft and mail non-receipt card fraud. The FFA's publication, Fraud the facts, is the source for all of the graphs for the financial section.

In addition to the FFA categories of identity related crime, there exists a range of other fraud types which contain an element of identity fraud ranging from face-to-face fraud, cheque fraud, internet, remote and mobile telephone banking fraud and the use of money mules. These too will be briefly examined.

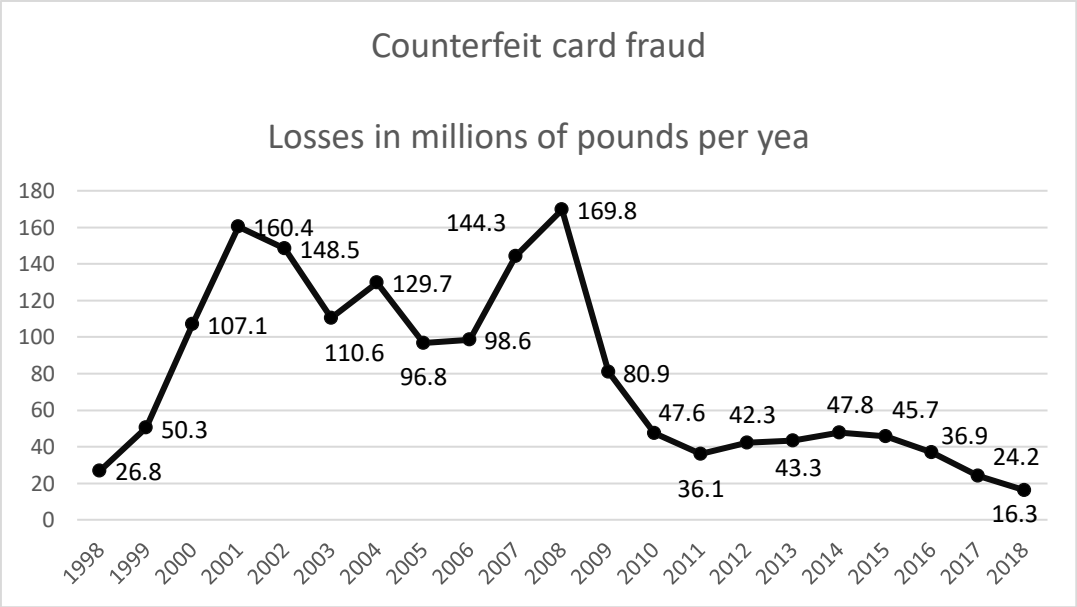
The way that fraud is reported and recorded in the financial sector is either 'gross' or 'net', gross referring to total fraud losses while net references fraud losses minus any recoveries or charge backs (Document 12, R15). When examining the literature provided by banks and financial service providers, references are made to card identity theft which indicate that they consider card fraud as a type of identity theft or fraud whereas, in discourse, they only consider application fraud and account take over as identity theft or fraud. This is a very confusing picture for the general public (Document 1, R15).

The total number of financial fraud cases in 2018 totalled 84,624. The industry believes that they have prevented £1.66 billion of losses in that same year. The security processes employed by banks decrease dramatically where the crime is less susceptible to direct bank intervention, such as scams directly targeting the customer.

5.4.1. Counterfeit card fraud (Card Present)

The FFA explains that Counterfeit card (CP) fraud occurs when a fake card is created by fraudsters using compromised details from the magnetic stripe of a genuine card (Fraud the facts, 2009 &2019). Following on from the introduction of EMV (which is a global standard for credit and debit payment cards based on chip card technology taking its name from the card schemes Europay, MasterCard, and Visa - the original card schemes that developed it) the payment industry has progressed a long way in tackling Card Present fraud and bringing the situation under control. As can be seen from the data below, there have been two

massive rises in CP fraud in the last few years but each time the problem was contained effectively to reduce losses.



The two rises and falls in the amount of CP losses can be explained by what had been happening at the time. The rise in fraud in 2000-01 was due to the magnetic stripe on the reverse of the card being compromised. The financial industry, in order to tackle this problem, introduced chip and PIN which effectively reduced fraud but in 2008 the losses increased again which was due to chip and PIN devices being compromised at a number of retailers. The industry responded to these compromises by working closely with retailers, the chip and PIN device vendors and updating the cards themselves, not to mention the DCPCU's (Dedicated Card and Payment Crime Unit) efforts to tackle the organised criminal gangs behind these attacks. Among other valuable strategies employed was a Crimestoppers 'whistleblower' project which firstly, provided anonymity via the provision of their secure line for retail staff to report any suspicious activity and secondly, raised awareness of this crime amongst the retail community.

The introduction of chip cards was a major infrastructure change to the industry costing them a staggering £1.1 billion. It was a joint effort between Europay, MasterCard and Visa to ensure security and global inter-operability so that Visa and MasterCard cards could continue to be accepted everywhere (across borders). The EMV standards define the interaction at the physical, electrical, data and application levels between chip cards and chip card processing devices for financial transactions.

Security measures can be applied at every stage of the card payment cycle and on every single payment device. For example, there are three different types of chip cards: SDA, DDA and CDA. SDA refers to Static Data Authentication and DDA stands for Dynamic Data Authentication. As SDA cards use static data, they have a number of vulnerabilities. DDA cards are far more secure than the SDA which is why the card industry started migrating to them. This decision was made in the light of the huge losses in 2008 and 2009. The SEPA (Single Euro Payments Area) in line with Visa and Mastercard mandated that European banks upgrade to DDA when issuing cards from 2011. This roll out was completed by 2015.

CDA (Combined Dynamic Authentication) is the advanced alternative to DDA and is the most secure of all three of the card protection authentication systems but at the moment none of the UK card issuers are using this technology and, from a business perspective, do not yet see the need to switch to this more costly but more secure option.

Prior to the introduction of chip and PIN, the FFA worked with retailers providing them with guidance on ways to spot counterfeit cards, providing them with advice on what to do if they encountered one. The cards could be false cards manufactured from scratch or they could be legitimate stolen cards which have had their magnetic stripes and security features altered (Document 15, R15). Cards that do not look authentic might be made of any material with correct dimensions and a magnetic stripe. They may or may not have details embossed on them. As they do not look authentic, they can only be used to target retailers who are in collusion with the fraudster, or in unattended terminals and cash machines. The banking industry introduced several measures to help tackle these issues. One of these was the introduction of Hot-Card-Files which is a list of stolen cards. If cards are stolen, they can still be used for under-floor-limit transactions (whose value does not exceed a nominal sum of approximately thirty pounds). Stolen and counterfeit cards can be used for under-floor transactions (ibid). The other useful technique was code 10 which is used to handle the situation where a counterfeit or stolen card has been retained. If a shop assistant became suspicious of a card, they would call the issuing bank for an authorisation code. If the bank replied with a code 10, the shop assistant would decline the transaction and retain the card. A rewards program is used by the banking industry to pay out £50 when a card is retained, and a fraudulent transaction is prevented. Over £16 million in rewards were paid in 2016. The introduction of chip and PIN reduced magnetic stripe fraud in the UK but has not achieved much in reducing this type of fraud abroad. Although most European countries have migrated to chipped cards, until recently, only IC (magstripe) cards and POS (Point of Sale) systems were used which is why the UK fraudsters were stealing the data on the magnetic stripe and then using it in Europe. Equally, because chip and PIN is used here,

foreign issued cards are exported here and misused in UK retailers. To enforce the uptake of chip and PIN amongst UK retailers the finance sector and banks introduced a shift of liabilities from 1st January 2005. After this date, any retailer not using a chip and PIN terminal in their store was to become liable for the cost of a fraudulent transaction.

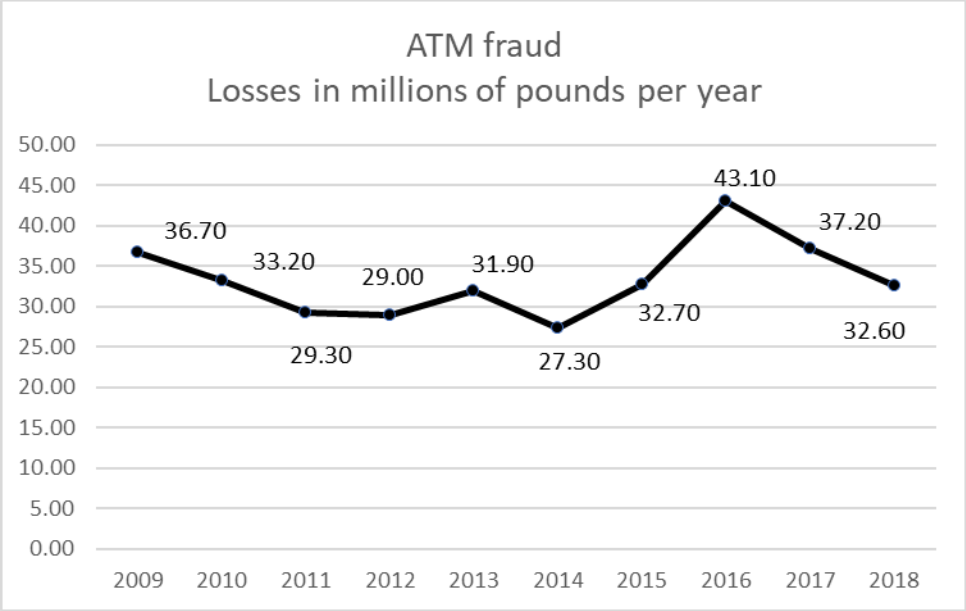
Card data is a very valuable asset to fraudsters. They can use it themselves or sell it to interested parties who can misuse it. Protecting this data is very important to the financial sector. A compromise would not only result in financial loss but the prolongation of these attacks and compromises may result in erosion of public confidence in payment cards and potentially reduction in card usage. Additionally, these attacks make it more challenging to promote a positive UK industry view on threats and security with opinion formers and government on public policy issues.

The payment infrastructure is complex with several players. The vulnerabilities in cards, the transaction process and environment such as PEDs (Chip and PIN Entry devices) provide fraudsters with perfect opportunities to break into the system and misuse it. This is further exacerbated by the technical, human and financial resources that some of these criminals have at their disposal.

Since 2008, Counterfeit card fraud losses have fallen from their previous highs, possibly due to the increased roll-out of chip technology around the world, and the successful strategies employed to address it.

ATM (Automated Teller Machines) Fraud

The following graph shows the level of fraud at cash machines in the UK on either stolen cards or where a card account has been taken over by a fraudster. In all cases, the fraudster would need to have access to the genuine PIN and the card (Fraud the facts, 2009 &2019).



The ATM network (cash machine) in the UK is run by LINK. All the ATM machines in the UK are connected to LINK and all the banks that issue credit or debit cards to their customers are LINK members. Equally, any bank or business that wishes to operate a machine needs to become a member of LINK. There are currently 64,500 ATM machines in the UK with 100 million LINK-enabled cards in circulation.

According to LINK, for whom security is a top priority, there are no 'magical' solutions to guarantee the100% protection of ATMs at the moment. There is currently no central body to impose deployment of security measures by ATM providers. However, some industry practitioners believe this would not be effective since, in the short term, it might help reduce the number of ATM attacks but in the longer term it would increase the number of attacks directed at these machines (Document 14, R11).

Although the ATM deployer has the responsibility for the security and safeguarding of the machines and the area surrounding them, the ATM networks decide on the level of security required. Additionally, whilst the insurers, card schemes and the card issuers also have strong influence on the level of security employed for the protection of the ATM machines themselves, it is the deployers who are responsible for the security and safe-guarding of the area surrounding the machines (ibid).

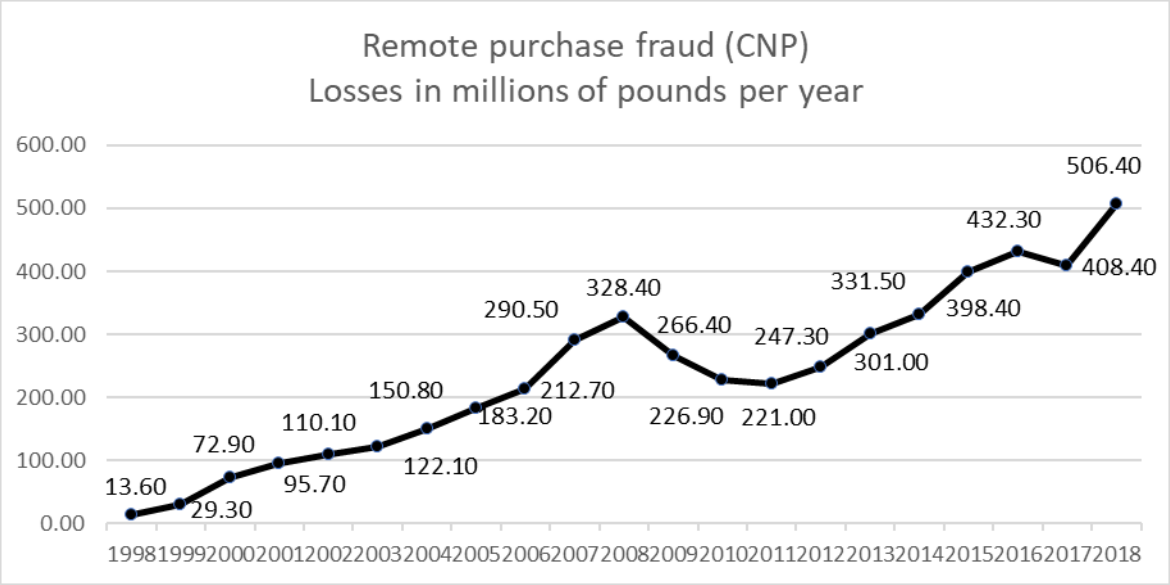
One belief is that ATM fraud is committed by transnational criminal organisations using sophisticated material both for physical and primarily for logical attacks (ibid).

There are three types of ATM crimes; attack against the ATM network (such as card skimming and card trapping), attacks against the ATM owner (such as physical attacks

against the ATM machine) and finally attacks on the people who are using the machines to either recover their card or their money. Not all these attacks would be classified as identity related crimes but those that do are skimming which involves copying the data on the magnetic stripe when a card is used at an ATM machine (which is achieved by inserting small card readers near the Card Reader Input Slot), Fake ATMs, and attacks that threaten the ATM networks (some examples are 'the Lebanese loop', point of sale compromise, mass compromise, hardware overlay, and phoney ATMs.

5.4.2. Remote Purchase fraud

The banking sector uses the term Remote Purchase (RP) fraud for those crimes that are committed using stolen card data on the internet, phone and mail order (Fraud the facts, 2009 &2019). The losses due to this type of fraud have been consistently increasing which is in line with general crime trends associated with the use of the internet.



There are several methods that fraudsters employ to commit RP fraud. Malware, for example, remains a popular method used by fraudsters to obtain customers' details, and is sometimes used in combination with phishing emails or smishing text messages in which fraudsters impersonate trusted brands such as online retailers. Malware includes computer viruses that can be installed on a computer without the user's knowledge, typically by clicking on a link in an unsolicited email, or by downloading infected software. Malware is capable of inserting bogus web pages, logging keystrokes and performing unauthorised actions on a victim's computer, in an attempt to capture passwords, financial information or other personal details.

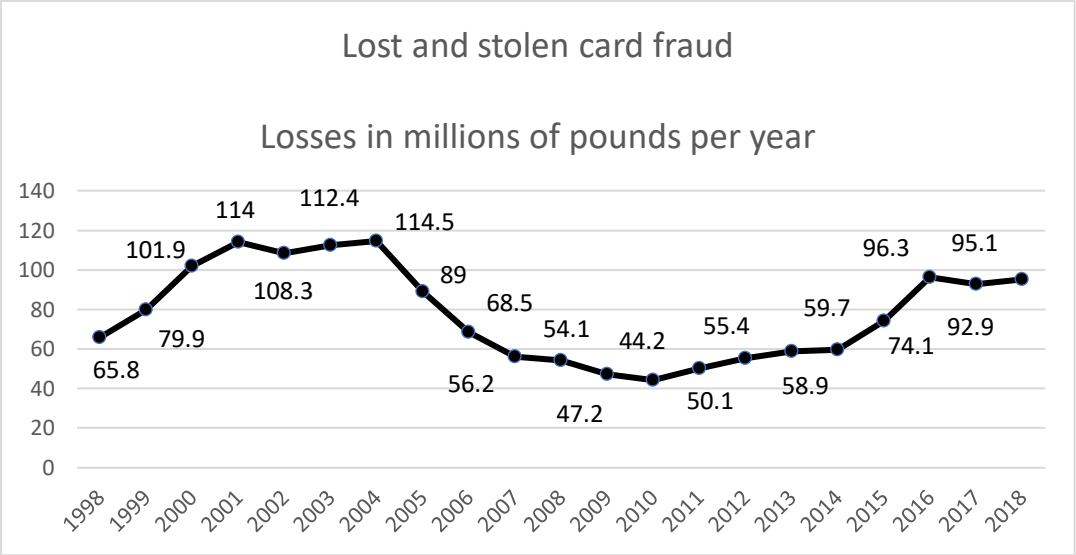
Crimeware is another tool that fraudsters use which is a sub-class of the broader category of malware referring generally to unwanted software that performs malicious and illegal actions on a user's computer. These actions are intended to yield financial benefits to the distributor of the software (Jacobson and Ramzan, 2008:1-2). Crimeware attacks often span multiple countries and are commonly perpetrated by organised criminals. Because crimeware is designed with financial gain in mind, the perpetrators often treat their malicious activities as a full-time job rather than as a hobby (Jacobson and Ramzan, 2008:4). Crimeware propagation techniques can be classified into two broad categories: social engineering (such as attachments and piggy backing) and security exploits (such as internet worms, web browser vulnerabilities and hacking) (Jacobson and Ramzan, 2008:3).

There are several ways that financial organisations and online-retailers can protect themselves against RP fraud. Initially, merchants have risk monitoring systems that help them to flag suspicious transactions - once a suspicious transaction is flagged, they then carry out a manual review on such orders (Document 16, work experience 2008).

The key advice provided to e-merchants by schemes is that no one tool is a silver bullet and that a wide range of tools needs to be employed to help tackle fraud. The average is about 4 tools (ibid). Transactions across national borders raise the red flag higher, as international transactions represent nearly half of all credit card chargebacks (a demand by a credit card provider for a retailer to make good the loss on a fraudulent or disputed transaction). A surprisingly short list of nations highlights which states s produces the most fraudulent transactions.

5.4.3. Lost and stolen card fraud

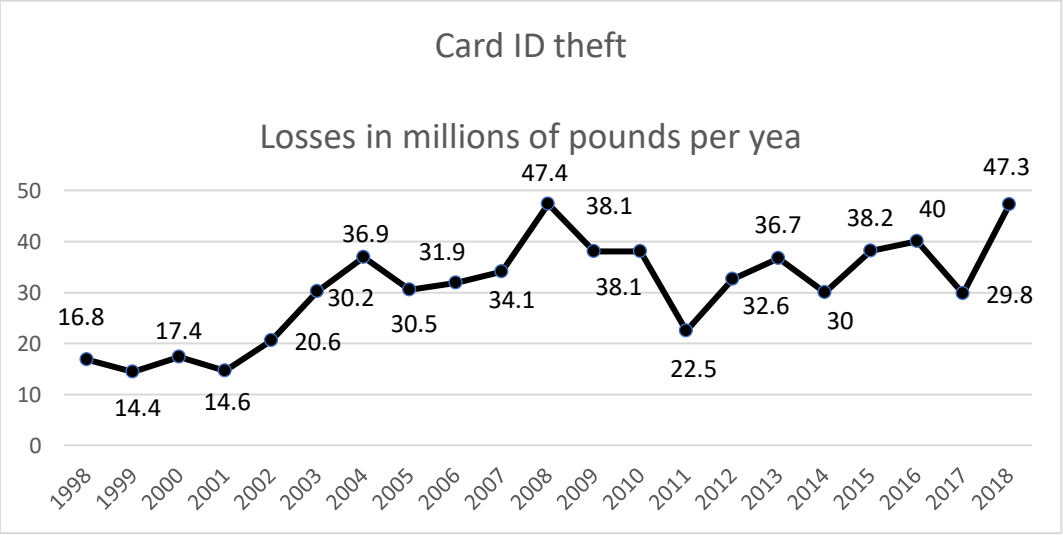
According to UK Payments, this category covers fraud on cards that have been reported lost or stolen by the cardholder (Fraud the facts, 2009, 2019). These lost and stolen cards could be used in shops that do not have chip and PIN equipment, or they could potentially be used to commit fraud via a telephone, internet or mail order transaction. The introduction of chip and PIN helped to reduce this fraud type significantly. Additional measures include IT systems that track customer accounts for unusual spending patterns and the Hot Card Files generated and circulated within the banking industry.



Lost and stolen card fraud seems to have been increasing consistently in the last few years. This is an area that the banking industry needs to monitor seriously.

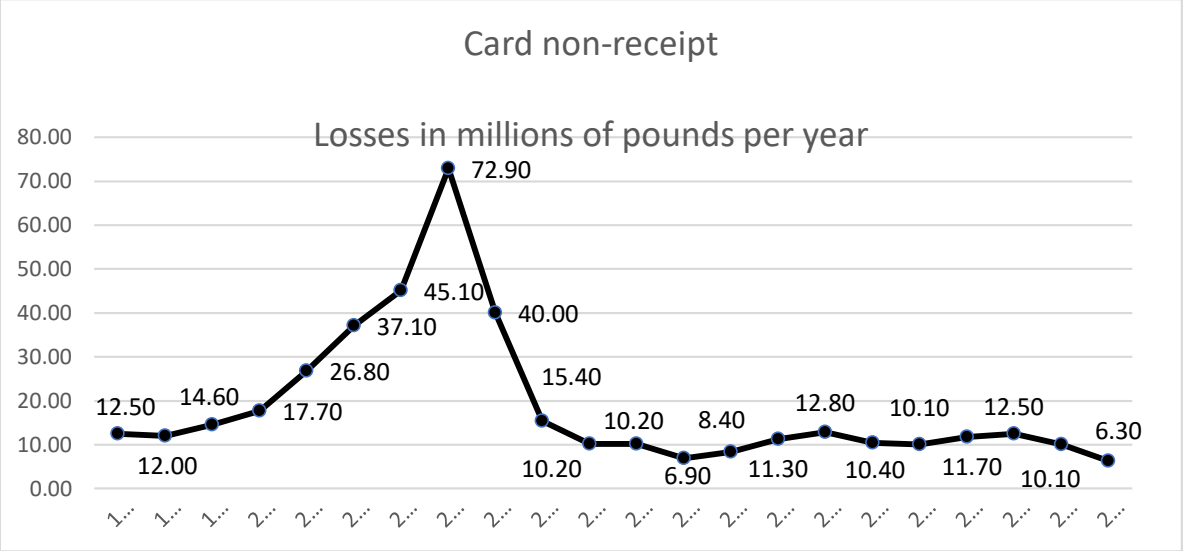
5.4.4. Card identity theft

The financial sector has two categories of card identity fraud, application fraud and account takeover (Fraud the facts, 2009, 2019). Application fraud occurs when fraudsters use stolen or fake documents to open an account in someone else's name and account takeover is when the fraudsters use another person's credit or debit card account, first by gathering information about that person, then contacting their bank or credit card issuer whilst pretending to be that person. The fraudster then arranges for the funds to be transferred out of the account or will change the address on the account and ask for new or replacement cards to be sent to the new address.



5.4.5. Card mail non-receipt fraud

This type of fraud happens when payment cards are stolen whilst in transit from the card issuing companies to their cardholder (Fraud the facts, 2009, 2019). It is believed that properties with communal letterboxes, such as flats and student halls of residence and people who do not arrange to have their mail redirected when they change address are all vulnerable to this type of fraud.



A number of strategies have been used by the finance industry to combat this fraud such as working in collaboration with the Royal Mail and other organisations that deliver the cards, identification of hot spots and use of secure couriers in high-risk postcodes or the delivery of

the card to the local bank branch. The banking industry believes that the peak of this crime which occurred in 2004 was due to more cards being issued as a result of the introduction of chip and PIN cards, therefore, more cards were being intercepted. Since the 2004 peak, the trend has settled down to a much lower range assisted by the fact that PIN numbers were sent separately from the cards.

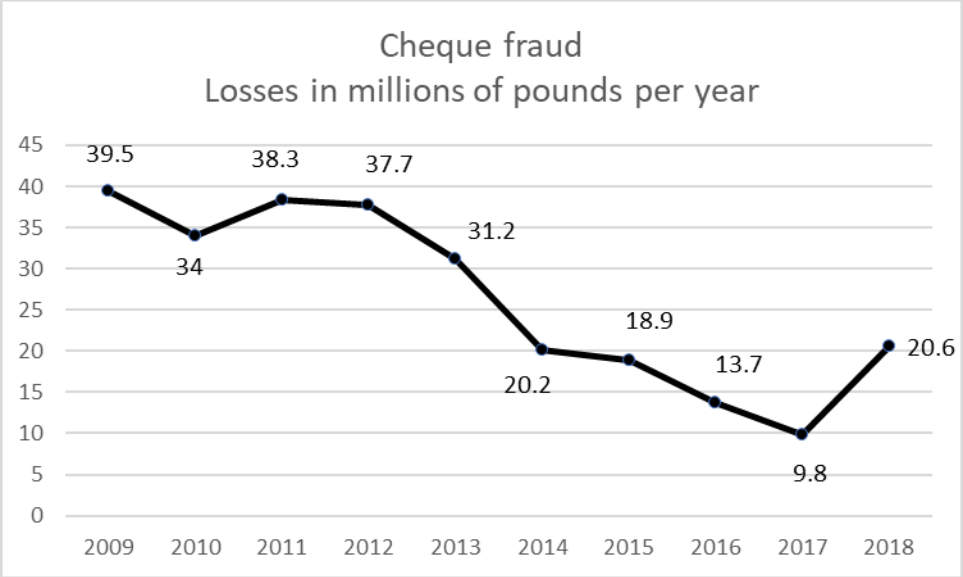
5.4.6. Retail face-to-face fraud

In addition to the above, the FFA also captures fraud that has occurred in the face-to-face retail environment (Fraud the facts, 2009, 2019). The majority of this fraud is undertaken using cards obtained through more basic techniques, with fraudsters finding ways of stealing both the card and PIN in order to carry out fraudulent transactions in shops. This includes criminals targeting cards and PINs through distraction thefts and entrapment devices at ATMs combined with shoulder surfing or PIN pad cameras. Criminals also use methods to dupe victims into handing over their cards on their own doorsteps.

5.4.7. Cheque fraud

There are three different types of cheque fraud which can all be categorised as identity crime (Fraud the facts, 2009, 2019): Counterfeit check fraud: these are cheques that are manufactured or printed on non-bank paper to look like a genuine cheque and are drawn by a fraudster on genuine accounts held by the victim at their bank. Forged cheque fraud: a genuine cheque stolen from a customer and used by a fraudster with a forged signature. Fraudulently altered cheques: a genuine cheque that has been made out by the genuine

customer, but a fraudster has altered the cheque in some way before it is paid in e.g. by altering the beneficiary's name or the amount of the cheque paid.



In the last couple of years, the FFA started capturing the amount of cheque fraud prevented. A total of £198.2 million was prevented by banks monitoring systems in 2016, a 51% reduction in 2015. These activities and the general demise of cheque usage have seen the amount of losses due to this fraud decreasing. Despite these efforts and a further reduction in 2017, in 2018 there has been an increase in this type of fraud.

5.4.8. Internet/e-commerce fraud

In addition to Card-Not-Present figures the FFA provides quantitative data on internet/e-commerce fraud (Fraud the facts, 2019). These cover fraud losses on card transactions made online and are included within the overall remote purchase (card-not-present) fraud losses described in the previous section. An estimated £393.4 million of e-commerce fraud took place on cards in 2018, accounting for 59 per cent of all card fraud and 78 per cent of total remote purchase fraud.

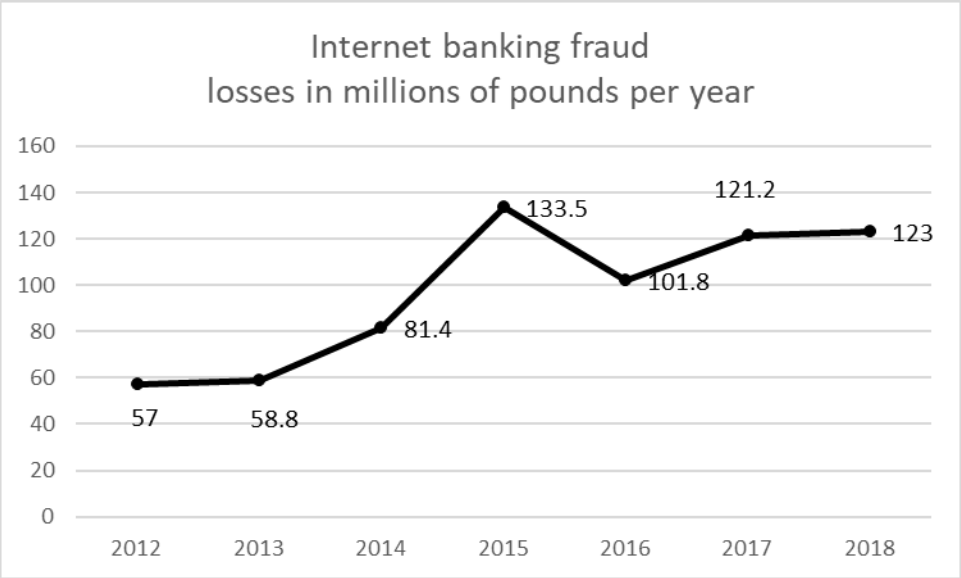
Data compromise, including through data hacks at third parties such as retailers, is a major driver of these fraud losses, with criminals using the stolen card details to make purchases online. Several high-profile data breaches occurred during 2018, with significant brands affected, alongside a number of lower-level incidents. The data stolen from a breach can be used for months or even years after the incident. Criminals also use the publicity around data breaches as an opportunity to trick people into revealing financial information.

Total e-commerce sales on sites based in the UK during 2018 was £251 billion, meaning that for every £100 spent online at UK merchants only 10.5p was fraudulent. For online merchants based overseas, 25p for every £100 was fraudulent.

5.4.9. Remote banking fraud

Remote banking fraud losses are organised into three categories: internet banking, telephone banking and mobile banking (Fraud the facts, 2019). It occurs when a criminal gains access to an individual's bank account through one of the three remote banking channels and makes an unauthorised transfer of money from the account.

Remote banking fraud totalled £152.9 million in 2018, two per cent lower than in 2017. The number of cases of remote banking fraud fell by eight per cent to 31,797. A total of £317.7 million of attempted remote banking fraud was stopped by bank security systems during 2018. This is equivalent to £6.75 in every £10 of fraud attempted being prevented. In addition, 15 per cent (£22.2 million) of the losses across all remote banking channels was recovered after the incident.



5.4.10. Mobile banking fraud

This type of fraud covers fraudulent payments made from a customer's bank account specifically using a mobile banking app (Fraud the facts, 2019). This data has only been collected since 2015. In that year, total losses were £2.8million but by 2016 they were £5.7 million a rise of 104%. The figures for this fraud have been increasing regularly year by year. In 2017 they stood at £6.5m and in 2018 £7.9m. Mobile payment systems are still a new technology and, as yet, the industry is not fully aware of the risks and areas that could be

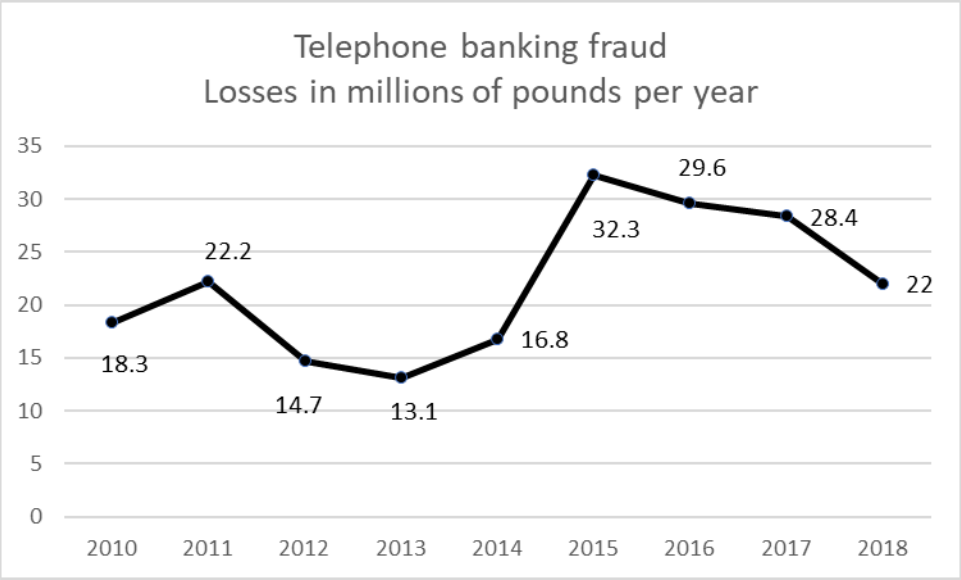
exploited by criminals. It is also not entirely clear where the ownership/responsibility lies in the event of a mobile banking app-driven compromise. Is it the consumer, the phone network or the bank's internal computer system security?

There are constant threats of malware to mobile payment networks and apps are becoming increasingly vulnerable to criminal exploitation. There are more questions than answers when it comes to mobile networks such as the extent to which the mobile user's use password protection on their phones and customer awareness of the vulnerabilities inherent in the devices that they habitually use.

Contactless payment, where the cardholder is able to pay for items up to a limit (typically £30) by simply placing the card within 5 cm of the device being used by the retailer to capture the funds (without recourse to the cardholder having to enter a PIN) is another emerging technology which has been embraced by the financial industry and consumers in the last couple of years. Fraud on contactless and mobile devices remains low with £6.9million of losses during 2016 compared to spending of £25.2 billion over the same year. However, these two areas need to be kept under surveillance as identity criminals are sure to target them at some point.

5.4.11. Telephone banking fraud

This type of fraud covers fraudulent payments made from a customer's bank account using telephone banking (Fraud the facts, 2019).



5.4.12. Money mules

It is believed that most fraudsters behind online banking scams are located overseas, so they need an accomplice with a UK bank account to act as a money mule or money transfer agent, to launder the stolen funds (Fraud the facts, 2019). Some mules are recruited under false pretences, after applying for a job as a payment processing agent in the belief that they will be working for a legitimate company. After being recruited by the fraudsters, money mules receive funds into their accounts. They then withdraw the money and send it overseas using a wire transfer service, minus a percentage commission payment. Money mules are recruited by a variety of methods, including spam emails, adverts on genuine recruitment websites or newspapers, and approaches to people with their CVs displayed online.

Although the prospect of making easy money may appear attractive, after a successful prosecution, any commission payments will be recovered as they are the proceeds of fraud, and money mules may become embroiled in a police investigation. Money mules are the easiest part of the chain to track down.

According to CIFAS (2019), over the nine months up until September 2019, there was a 25% increase in money-muling activity amongst those aged 41-50, and a 26% rise among those aged 51-60 with a total of 32,468 incidents recorded. However, previous data from 2016 indicated that in the first nine months a total of 67, 223 incidents were recorded. This shows a significant decrease in number of cases recorded across the two periods.

The above captures the different types of products and services that the financial service providers offer to their customers. There is a large range and no aspect of these products and services are immune to attacks and infiltration by criminals. Therefore, efforts need to be made to make sure that all of them are secure.

5.5. The Complex UK Payment Infrastructure

When examined closely, the financial industry is made up of a very complex web of entities to make the whole system work and make financial transactions possible. This web consists of, the issuing banks, the acquiring banks, data processors, merchants, vendors, schemes and finally the ATM network. These organisations rely not only on the effective functioning of their systems but also, for credibility, on the public perception that these systems are functioning. As such, their communications, information management and relationships play an important part of the infrastructure. All of this contributes to both making the industry a

safe environment and also, in some cases, adds to the vulnerabilities that are created in handling consumer data.

Schemes

To understand the complexity of the whole payment structure, it is best to look at how the whole system works. The most fundamental part of it is the schemes: Visa and MasterCard and American Express. They are the owners of the payment scheme and for any bank or financial institution to issue or acquire financial transactions, they must become a member of these schemes and adhere to their regulations. They do not issue any cards themselves but rather license their payment brands to issuing and acquiring banks.

The schemes also actively work to tackle identity fraud issues by providing good practice guides to their members, inventing secure methods of payments and hosting various fraud related meetings and conferences to address the issues. The members of the schemes are required to report fraud to them within a certain time frame (Document 12, R15).

The best practice advice provided to banks by schemes acknowledges the different operating environments and processes and procedures that each financial institution deals with but there is a requirement for the banks to report all their fraudulent transactions to the schemes within a defined timeframe (ibid).

Issuing and acquiring banks

The Online Business Dictionary (2012) defines issuing banks as:

> "The buyer's or importer's bank which establishes (opens) a letter of credit (L/C) in favour of a beneficiary (seller or exporter), forwards it to an advising bank for delivery to the beneficiary, and commits itself to honour demand drafts drawn by the beneficiary against the amount specified in the L/C. Also called the opening bank."

We, as customers, know the issuing banks as those that issue us with debit, credit or charge cards and in doing so collect and hold our identifying information and also any history related to the usage of the card and since in the modern world less and less cash is used, this history is rather extensive.

Acquiring banks on the other hand deal mostly with the retailers that accept the payment cards according to the online Business Dictionary the acquiring banks are (ibid):

> "Banks which process a merchant's credit card sales, and credits them to the merchant's account."

These businesses collect, and in some cases, hold on to various payment related information on customers. This data is collected at the merchants' terminals and sent to the acquiring banks.

One of the major challenges that the Issuing and Acquiring financial institutions face is their customers' attitudes, experiences and behaviours towards identity crime related issues. When customers fall victim to such crimes, it has a negative impact on the way they perceive their bank's ability to effectively protect their data. This then has an effect on the reputation of the issuing bank. However, the banks can use this opportunity to collect feedback from victims and use that not only to provide better victim support and experience but also to use the knowledge to enhance detection, mitigation and prevention strategies. They can use the input collected from customers and victims to provide a platform for improving processes/ good practices and card holder communications and advice.

Financial Fraud Action UK (FFA)

FFA is responsible for leading the collective fight against financial fraud on behalf of the UK payments industry. Their membership includes banks, credit, debit and charge card issuers and card payment acquirers in the UK. They provide a forum for members to work together on non-competitive issues relating to financial fraud. FFA's primary function is to facilitate collaborative activity between industry participants and with other partner organisations also committed to fighting fraud.

Dedicated Card and Payment Crime Unit (DCPCU)

DCPCU is a special police unit comprising of police officers drawn from the City of London and Metropolitan police forces. The unit is fully sponsored by the banking industry and supported by bank investigators and case support staff who have an ongoing brief to help stamp out organised payment card and cheque fraud across the UK.

Data processors

There are a large number of third parties who facilitate or contribute to making the payment transactions happen. These entities are employed by banks or retailers to help with different parts of the payment process such as collection, preparation, input of data, processing of data and output. Similar to the banks, the data processors come into contact with large

amounts of card data which they process and may store and, therefore, have the risk of data being compromised at any stage of this process or from storage.

PCI (Payment Card Industry) compliance has been introduced by the schemes to ensure that the entire end-to-end transaction processes are safe and secure and that all parties involved in the process are aware of the rules and regulations regarding the protection of data. The range of security requirements stipulated includes: PA DSS (Payment Application Data Security Standard), covering the payment application, PCI POS and PED covering the security of the point of sale device and PCI EPP covering ATMs and the encryption of pin entry devices/pads (PEDs).

It is believed that there still is a 'low appreciation' of the PCI DSS requirements among merchants. Data processing and storage is usually outsourced to a third party and in some cases the third party then outsources that to another, leaving the merchant unaware as to who is, in fact, processing the data on their behalf. This is the result of 'naive senior managers' who are not IT savvy and who do not have a full understanding of the risks associated with data storage and processing (Card world, April 2009).

Some of the companies that have experienced compromises such as (Hartland) were actually passed as being PCI DSS compliant but if someone inside the organisation has changed something of which the audit department is unaware, that can change the whole dynamics of things (ibid).

The extent to which merchants comply with PCI DSS and to what degree this compliance will protect them against threats is not known. The organised attacks that have been recorded over the last few years indicate that the criminal gangs have the capability to infiltrate systems. They operate similar to the common business models, try, test and learn from their mistakes. Additionally, the merchants seem to have more of a reactive response rather than a proactive one.

The liability of complying and protecting merchant data lies with the acquiring bank (merchant bank) but there is a reliance on behalf of the banks and financial service providers for the third parties to treat the data in a secure manner.

The cost for an investigation of a compromise is estimated at £30,000 as well as the penalties that are in place by Schemes for such incidents, in addition to all the time and labour costs employed by organisations to remedy the problem. Investigations are not always straight-forward and, in some cases, they still do not find the answers that are sought (ibid).

There is also a vast growing business with fast pay service providers. This area of finance is not regulated, therefore, how the data collected by these companies is used is unknown.

Merchants and vendors

Merchants are the retailers that have the infrastructure to accept card payments which can either be face to face card acceptance or can be online. Merchants vary from hotels to shops, bars or restaurants, air travel agencies and indeed any establishment where payments are made by customers.

Vendors, in the banking industry, are those companies that develop the devices or software utilised to make payments happen. Typical examples are those companies that manufacture Pin Entry Devices or those that make the actual cards. There are also those that provide the necessary software for certain types of payments. Both merchants and vendors have their own forums within which members can discuss and collaborate on non-competitive fraud issues. From the above analysis of systems and players, it is clear that there are a lot of organisations and interplay between them that make the card payment business happen. In addition, the industry is constantly innovating and adding to the different products and services offered to merchants, vendors and end customers and in this environment of rapid change it is not surprising that criminals are finding it easy to infiltrate these systems.

Credit reference agencies

The credit reference agencies play a prominent role in the arena of identity crime in addition to providing credit reports to consumers and fraud victim support. This role has traditionally been as the credit risk and information providers to credit risk decisions and decision makers (R20). These fraud solutions have been perceived as a ‘major business development opportunity’ for credit reference agencies and are provided to consumers, businesses and government agencies as well as law enforcement bodies (R20). The products are risk based and involve identity verification and authentication. These solutions not only assist in tackling identity fraud but also help in combating money laundering (R11). These services and products include solutions on authentication to prevent identity fraud, products to detect any discrepancies in applications and comparing the data with information provided on previous applications and highlighting if they do not match. Also, looking for matches against other applications to highlight possible fraud, recording where fraud has happened, whether an application has been declined or accepted, examining mortgage brokers and whether they have been involved in fraudulent mortgage applications, basically building intelligence. Solutions also exist for companies that have suffered a data breach. The credit reference

agencies would offer a discounted version of their credit expert service to such companies to be offered to their customers. They also advise companies on ways they can help their affected customers to protect themselves. Finally, they provide credit reports on business to business so that when businesses want to trade with other businesses to identify where there may be fraud in trade credit relationships (R11). This service also helps companies to prevent trading with fictitious companies.

In addition to the above, the data that credit reference agencies generate enables other organisations that primarily verify data for businesses and government agencies to exchange information (R11). The source of the data for the credit reference agencies comes from public sources (such as the electoral roll, court judgments, bankruptcies and so on) and the data from lenders (such as accounts) (R11).

5.6. Media and academia

The media plays an important role in the whole arena of financial crime and is centred around three different objectives which are: broadcasting news, forming opinions and raising awareness and finally putting pressure on banks and financial institutions.

With respect to identity crimes, the media has been very effective in bringing to light the concerns and issues inherent in this area. Numerous cases have been reported and presented in the last few years highlighting the inconvenience and troubles caused by this crime to its victims.

Equally, academia has been very influential in criticising the banks' processes and procedures, drawing largely negative attention to them. A very prominent example is the University of Cambridge Computer Laboratory which regularly develops reports on the security engineering of the payment systems for their Spring Conference. Some of the papers published are "Chip and PIN is Broken" (Murdock et al, 2010) and "Risk and Privacy Implications of Consumer Payment Innovation" (Anderson, 2013) . In an examination of the technology (3D Secure) used by the two schemes, Visa and MasterCard, to reduce online fraud, Murdoch and Anderson (2010) critically asses the vulnerabilities of these two authentication methods. Verified by Visa and SecureCode by MasterCard are now deployed by online retailers in order to tackle the soaring losses of online payment card fraud. The way that these systems work is that when a customer attempts to make an online purchase, a pop-up window appears asking him/her for their password. If the password entered is correct the customer will be directed to the purchase window to complete the transaction. In this study Murdoch and Anderson highlight 7 vulnerabilities that exist with these two

methods. They start by arguing that by operating with only a single sign-in method, these systems breach ‘many established security rules’. The first vulnerability identified by Murdoch and Anderson is that the log-in process confuses the user (hiding security cues) as the method used for verifying the customer uses a pop-up window with no address bar, making it hard for customers to establish whether the pop-up window originated from a secure network. ‘Activation during shopping’ is their next concern arguing that when customers use this for the first time, it is required that they are verified. To do so, some security questions are asked (such as date of birth) which fraudsters may have intercepted and copied to capture identity data. Poor password choice by customers is another issue highlighted, along with shifting the liability to customers. Banks are gradually shifting the liability for identity and payment card fraud to customers as they are unlikely to object to the terms and conditions offered by them and passwords do not currently have the statutory rights of a signature.

Mutual authentication and inconsistent authentication methods are the other concerns. They believe that customers are made to verify a memorable phrase which could be a poor choice and also, vulnerable to a man-in-the-middle attack. Resetting passwords are relatively easy, and also, as only part of the password is required, customers may choose easy passwords which would be open to compromise. And finally, they criticise the privacy of 3D secure stating that it requires that a description of the transaction be sent to the Issuer which places question marks on the privacy of this system, especially if third party providers are used.

Murdoch and Anderson (2010) suggest a transaction authentication similar to the CAP calculators and emphasise the incentives and regulators’ intervention to fight the consumer corner. Once one of these papers is published, the banking industry responds by publishing press releases as a counter-measure. A better relationship formed between these two sides could work to the advantage of both parties. The banks will have access to expertise and the research skills of academia, and the academics would have access to information for their research.

Media interest and criticism, and the critical examination of the finance systems by the Murdock team forces the representatives of the financial institutions to respond with press releases to address the concerns raised. I witnessed this first-hand from the work experience that I undertook within the finance sector. Colloquially speaking, these criticisms are effective in keeping the financial institutions on their toes.

5.7. Data compromise within the finance sector (mass data compromise)

Data compromise is the unauthorised extraction and manipulation of personal and banking data from public/private sector systems that has the potential to be used for fraudulent purposes. It mostly happens at merchant sites or third-party sites with vulnerable networks.

The issuing banks are warned early by such incidents either through their customers or through their own fraud detection tools. When such incidents take place, the issuing banks minimise the harm caused to their customers by monitoring the affected accounts and issuing replacement cards. Following such events, the schemes provide each issuer with a list of their cardholder accounts that have either been compromised or are perceived to be at risk. It is the responsibility of the issuers to manage such risks by 1) blocking the accounts 2) reissuing the cards which is not the most suitable option due to the high costs of such a response and the inconvenience that it causes to the customers and finally 3) placing the accounts on 'watch lists' for close monitoring (Document 12, R15).

Data compromises have become frequent occurrences in the last few years. One of the biggest financial sector compromises took place on January 2009. Heartland Payment Systems, which processes payroll and credit card payments for more than 250,000 businesses, reported that their consumer credit card and payment card transaction data were exposed (Document 15, R15). The data that was compromised was track 1 and 2 data stored on the magnetic stripe on the back of the cards. It was believed that the intruders broke into Heartland's systems via the internet as early as May 2008 and installed malicious software to steal card data carried on the company's networks. The malware was hidden so well that it eluded two different teams of forensic investigators brought in to find it after fraud alerts sounded at both Visa and Mastercard. By the time it was discovered, the malware had already been deactivated. More than 100 million card numbers were stolen by fraudsters. Apparently, the company had not implemented, or was not using, all of the security controls required by PCI standards.

This was not a one-off incident and since then data compromise has been a regular occurrence. Some of the most recent compromises are: Tesco bank (Broadie, 2016) with 40,000 accounts compromised, Wonga (Osborne, 2017) 245,000 accounts, CEX (Tuffcub, 2017) 2 million accounts, and most recently British Airways (Bishop, 2018) with 380,000 transaction records stolen in just two weeks. These are large cases of such compromises; smaller scale attacks are even more frequent but are seldom reported.

5.8. Internal staff fraud

Internal staff fraud is a major issue for the finance sector as well as the other sectors impacted by identity related issues. There are 3 types of insider threats that affect the financial sector (and other organisations): staff specifically placed in their employment by criminals to commit crime (planting insiders), staff coerced by fraud gangs to assist in committing crime with threats of physical, financial or reputational damage and insiders who commit crimes while employed due to other reasons.

The basis of committing fraud while in employment contains either an element of organised crime or an element of opportunism linked to personal gain and it seems that with both, issuers and retailers operate a variety of different arrest policies.

Employee theft/fraud is a growing concern for organisations of all types and sizes. However, large companies operating in key industries such as finance and insurance are the prime targets for organised criminals. Insider fraud can originate in a number of areas from within an organisation, and from different types of people. While many of those responsible are individual opportunists, there is also a significant organised crime element. The fraud gangs either place staff in positions where they have access to data or attempt to bully or bribe existing employees to give up sensitive data that can be used for identity related crime offences. Threats of violence or blackmail by the gangs are not limited just to the employed individuals. Employees' family members have also been targeted. The financial sector is vulnerable to this type of criminality as they use employees who are often young, impressionable and low paid individuals. These high-risk personnel are deemed most likely to turn into 'staff fraudsters' and the fraud gangs target this lower end of the employment pyramid (Document 13, R8).

Collating meaningful data on insider theft/ fraud is a significant problem. There is no consistent data definition of insider fraud and no regular collection of data. There is no regulated body that collates insider fraud data or insists on cases being reported to the police, and many organisations decide not to instigate criminal proceedings given the heavier burden of proof required to secure a conviction and a desire to avoid damage to its reputation, which could, in turn, affect trading and/or share price (ibid).

There have, however, been a number of small-scale research projects conducted by various organisations. The City of London Police, in 2008, through their research in this area revealed that 35 percent of its work now involved some insider element, compared with ten percent in the late 1990s. While it is difficult to quantify in monetary and non-monetary terms,

insider theft/ fraud represents a clear danger to all UK organisations. In similar research, one of the UK banks profiled the cases of insider theft/ fraud it discovered between January 2005 to April 2006 to identify high risk areas. Although there was little difference between the sexes, just over half of employees (51%) dismissed had been with the bank for less than a year and a quarter between one and two years. Almost four in every five employees (78%) dismissed were under the age of 30. Twenty percent were under 20, 36% aged 21-25 and 22% aged 26-30. Only 4% of those dismissed were more than 41 years old. CIFAS, in its research on this issue, focused on the organisations which experienced insider fraud and discovered that only 2 out of 127 claimed they did not experience insider fraud. Additionally, the data revealed that over 60 percent of respondents reported that the theft/ frauds they had uncovered involved collusion with people outside the company.

In another study, one of the retail banks that sought Experian's help, revealed that the main type of insider fraud occurred at the branch level, where employees had been able to access and steal from customer accounts. The bank had a specialist department to investigate all employee fraud, irrespective of the monetary value, and it was the policy of this particular bank to prosecute all frauds as a criminal offence where the evidence was sufficient to do so. The average loss per insider fraud case was £40,000 and the bank had insurance in place for losses in excess of £5,000.

"It is not unusual for telephone conversations to be recorded and the computer system monitors employees at all times. Those new to the business world are often unaware of the controls in place and are easy to detect once frauds start to emerge. The criminal gangs know this and seek new employees in the first few months before they become aware of the audit controls in place. Subsequently, they also ensure they keep their distance in the eventuality that the frauds will be detected" (Document 13, R8).

The statement above clearly indicates a need for the establishment and implementation of training programs for new employees which emphasis the security measures regarding internal theft/ fraud so that they can be made aware of the focus on this activity, the zero tolerance company policy and the determination to prosecute offenders right from the beginning of their employment.

Therefore, it is the responsibility of companies to take it upon themselves to protect their assets and reputation by assessing the risks to their business and introducing robust anti-fraud policies and protections that cover every eventuality. The best place to stop insider fraud is at the recruitment stage. The process should start during the employee's induction and continue through ongoing staff monitoring. Also, the ability to share information (on the

offender) when something does go wrong in order to prevent the same person re-offending elsewhere (Document 13, R8). Organisations should identify the key roles and highest risk areas for the most intense scrutiny, enhance recruitment processes; strengthen security controls, and put in place trusted whistle-blowing procedures (ibid).

“Most companies are reliant on criminal records alone to check for unsuitable employees. The main problem here is that relying on criminal record checks alone can still result in fraudsters being employed as it fails to pick up on discrepancies and inconsistencies in other areas on the CV. The overwhelming majority of individuals picked up for committing insider fraud do not have previous criminal records, and many organisations do not pursue a criminal conviction of fraudsters they have dismissed due to the greater burden of proof required. Additionally, organisations relying on this method alone often run criminal record checks on applications for positions that don’t necessarily need them. For many, a simple verification that the CV is a true and accurate indication of their backgrounds would suffice. Monitoring and assessments and checks can be performed when staff are promoted or moved to more sensitive area.”

Although financial losses from fraud are damaging, the potential harm that an internal data compromise can do to any organisation’s reputation is significant, especially when that data is of a personal or financial nature. It is best that the organisations take a very public stance on the tools they have available to them to monitor and detect inappropriate activities (ibid).

Future threats of internal fraud

Greater access and use of portable company devices and personal IT such as laptops, tablets and smartphones are leading to an increased risk of possible data compromise. In addition to internal systems and devices, the widespread use of unregulated instant messaging systems contained as applications on employees’ smart-phones (for example, Whatsapp) which also contain cameras to snapshot data are presenting a new and growing problem for data security professionals. Employees are also increasingly taking advantage of flexible working environments from home or outside of their office which increases the chances that people close by could access or oversee sensitive or personal information. In the challenging financial climate, some organisations have been unable or unwilling to increase staff benefits meaning that pay and bonuses have stagnated or reduced, resulting in increased staff feelings of resentment and indifference towards their employer. Organisations recognise that this could be a trigger for criminal activity by employees who feel that they deserve more or are being overlooked for possible progression. Reliable data to support these assertions are, unfortunately, unavailable.

5.9. Major vulnerabilities

The financial sector identifies a number of vulnerabilities and challenges in tackling this crime. The first is emerging methods**.** As mentioned previously, fraudsters are very inventive and proactive in the methodologies they employ to commit identity crime and the finance sector is constantly discovering new MOs. In one MO for example, up-market restaurants were targeted by identity fraudsters who would call the restaurant pretending to be from the acquiring bank and inform the restaurant that all the chip and PIN machines for the area are corrupted and that they will be out of action for 2 hours. The fraudsters then advise the restaurant that, during this period, all transactions must be carried out by telephone and they were then given an 0800 number to contact and a reference to quote. When the restaurants called and used the reference number, the customer was called to the phone and asked personal security questions that would enable the criminals to take over their account.

Goodman (2015) describes a scam when fraudsters manipulate the user's smart-phone screen with a spoofed caller identity. They spoof the number of an account they want to access and then contact the bank. Once the bank's telephone system identifies an in-coming call from a customer's phone number, it is easier for the fraudster to obtain more personal information to access the account holder's data and money. This can also be carried out in reverse, calling a customer and pretending to be from their respective bank. The same technique is used to deceive consumers pretending that the call is coming from the government saying that they owe unpaid taxes (ibid:217).

Goodman illustrates another technique called 'rootkit' where criminals install malware on the victim's mobile phone. This malware gives the fraudsters control over all the features of the device, including its touch screen and number pad so that when the owner of the compromised phone tries to call the bank, the call is actually re-directed (ibid).

Contactless technology is now being rolled out in the UK and around the world for 'BioMetric passports' and travel and payment cards. However, the inadequacy of the security systems supporting contactless transactions facilitate access to the information on these devices to unauthorised people. With chip and PIN or magnetic stripe, the owner makes a conscious decision to authorise the reading of information by physically handing over the card to the user of the PED device. Contactless uses a short-range wireless link from a reader to activate a chip which can then be interrogated to provide information stored on it. The problem is that readers are easily available for purchase by anyone and the security codes

that protect the information have already been hacked. In some cases, details have been published on several websites for some time.

Authentication is another vulnerability. Static data which is still used in some instances to authenticate customers remains a major vulnerability. Such data can easily be accessed from a number of sources such as 192.com, Companies House, Facebook (Document 15, R15).

Despite the existing measures, criminals are managing to break through the identity and verification systems. The mission, in many organisations, to make the customer experience as easy as possible often means a reduced focus on security. Increased credit limits and the ease with which consumers can obtain loans or new cards are the other reasons this area presents major vulnerabilities. To facilitate this crime and to avoid detection, criminals must have secondary accounts in the names of third parties to which they transfer the stolen funds (known as mule accounts).

Over the last few years online activities have come to dominate our lives. Most financial products and services are now being accessed online, such as apps for bank account access. Criminals have, therefore, shifted their focus to this arena as, in some respects (for example, data sent over open networks rather than closed), it is easier to infiltrate than the old-fashioned systems. Therefore, the increased use of online services will present major challenges to the finance sector in identifying and addressing the vulnerabilities which will present themselves.

In general, the public are very careless about their financial details and payment cards believing that, if they are victimised by identity criminals, the banks will pay for it. That attitude needs to change as protection against this crime is everyone's responsibility, not just that of businesses. Additionally, consumers often lack the technical information to protect their personal computers and other devices effectively, specifically, not removing all their personal data from these devices prior to scrapping them when upgrading to a new machine. The UK is increasingly a multi-ethnic, multi-cultural society with varying levels of comprehension of the English language. Despite this backdrop, fraud prevention messages are delivered almost exclusively in English, leaving large sections of the community arguably less prepared and thus more vulnerable to identity crime. In addition, and awareness-raising needs to be targeted at the older generation as technology is moving rapidly bringing changes which may see them ill-equipped to understand and act appropriately to secure their devices and themselves from becoming victims to identity fraudsters.

All major banks and financial institutions are aware of the risks that staff dishonesty can present but, to what extent they have defensive policies and procedures in this area, is not clear. There are three foci to this: awareness and acknowledgement of the importance of staff dishonesty, policies and procedures developed to address it and effective application of such policies. Banks often use specialist staff recruitment agencies, but it is not known how these agencies are vetted and selected by the banks and how these agencies vet and select staff for the banks. There are CRB/DBS (Disclosure and Barring Service) backlogs as priority is given to checks which are focused on the protection of minors. This gives rise to a number of vulnerabilities which include insufficient pre-employment vetting/background checks and generally detailed vetting of staff. For example, in call-centres which often suffer from high staff turnover, there is frequently urgency to replace staff which leads to the abandonment of full vetting procedures as speed replaces quality and security as the driver for hiring employees. Generally, employment agency recruiters have inadequate checks in place and therefore expose their clients to the vulnerabilities that exist in this area. The call centres tend to operate over multiple locations and therefore, when recruiting staff, varying standards exist and, even if a common policy exists, the success in execution of the policies may differ in various locations.

Most banks have offshore call centres. It is not known how well the staff are vetted in these countries. There are different legal implications on overseas staff. Since banks operate in different countries, it is possible that the staff in other countries abuse their position and misuse the data to which they have access.

And finally, one of the major vulnerabilities sis the risk that different documentations present. The global mobility of the workforce produces its own unique challenges as many UK organisations lack the ability to detect false identity documentation presented by foreign nationals. As identity criminals have recognised this vulnerability and are becoming increasingly sophisticated, this problem is growing.

5.10. Tackling identity related crime in the financial sector

This section will examine the processes and methods that the finance sector uses to combat identity crime related issues.

Information management

The financial sector has the most robust fraud reporting system in place, developed and overseen by the FFA, the loss figures are captured and released to the general public twice

a year, providing a reliable source of data for fraud losses in this industry. The FFA also collates and circulates data regularly on fraud trends to its members.

Managing data or 'Management Information', which is the term used by the banking industry and the financial institutions, is a very important factor in monitoring, detecting and preventing fraud. The data provides a benchmark for the members to compare their status and progress on a range of key performance indicators and is also used for the UK Payment Threat Assessment. This data enables the banking industry to observe changes in various types of fraud and, therefore, to help them direct their resources to the most pressing fraud issues. Key data that are collected comprise: the amount and frequency of losses, location and merchant types, average loss per account, average loss per payment card, incidence rate, average fraud run time (date of first to date of last transaction), fraud write-offs, detection rate, fraud by sector type, fraud by place of misuse, cross border fraud and cross border fraud by sector.

Communication and awareness-raising

Communication plays an important role in tackling identity crimes. Consumers seem to have lost their trust and faith in the system in tackling this issue. Sixty one percent believe that criminals are at least one step ahead of the industry (Visa Global Security Summit Summary Report, 2011).

There are a number of ways that communication can play an effective role in this area. Firstly, the trust in the system needs to be restored and maintained by the banks and the financial services companies. The expectation of consumers' needs to be managed. In the real word no one expects that the police can completely eliminate crimes such as burglary or assault. The general public have accepted that these crimes exist. What is important however, is that banks assure their consumers that they are in control of the problem, and that they are doing everything within their power to minimise the impact of such crimes.

Communication, however, needs to be developed on the basis of research so that it can be focused and directed. It is not clear as to whether any communication on the part of the financial organisations or the government is based on any research. Equally, there is no evidence to suggest that any evaluation research has been conducted to examine the effectiveness of any marketing or awareness-raising activities. Communication needs to be informed, structured and targeted.

There are three elements to communication: informative awareness-raising and targeted attitude impacting and educational. Informative awareness-raising can be used to make

consumers aware of the latest trends used by criminals to commit this crime and to assure them that the industry is doing its best to tackle the issue. It is also useful for the industry to acknowledge the pain and discomfort caused by this crime to its victims and to sympathise with them. Targeted attitude impacting will focus on changing the dispositions that consumers have already formed. It is not known what the consumer perception is of their duties and responsibilities regarding the protection of their financial identifying information, however, it is clear there is resistance to accept responsibility.

Educational communication is designed to focus on changing consumer behaviour, but to reach this stage, the first two stages need to have been completed successfully. Consumers should be made aware of the risks and the methods that criminals are using, they need to feel responsible (although to a degree) in protecting their own identity information. Once they accept this, the education messages can be developed to help them to change their behaviour and make them protect their identifying assets better. Customers can be encouraged to be more vigilant. Assessments could be devised to understand the effectiveness of the communication in altering customer behaviour and attitude. Otherwise, the messages sent to customers may not necessarily have been effectively received, thereby failing in their objective of impacting and changing their behaviour.

5.11. Crime Prevention Methods currently utilised by the finance sector and the underlying criminological theories

An examination of the measures and practices utilised by the finance sector (Appendix 2) indicates that from the 136 methods used to tackle financial identity related crimes 46% are situational crime prevention techniques, 12% intelligence/data mining, 12% proactive approaches, 10% data sharing, 4% regulatory, 4% training, 3% educational/behavioural changes, 2% risk management, 2% guidelines, 0.7% incident management and 0.7% law enforcement. This information was obtained from my work experience at the UK Payment's Financial Fraud control unit.

Situational crime prevention techniques, rather than focusing on the root causes of crime or the social and psychological disposition of the offender, focus on the environment in which crime occurs. The theories that underpin SCP are rational choice theory, routine activity theory and crime pattern theory. In a study undertaken by Eck and Guerett (2012) to examine the effectiveness of SCP a hierarchical approach of classifying the most effective technique was used. It was discovered that in 70% of the 149 studies included in the review, only seven of the twenty-five situational crime prevention techniques were used. The

techniques used are very sector-specific so each sector would adopt the most relevant technique depending on the nature of their business. However, it was discovered that in the studies mentioned, CCTV was the most used technique and the least effective one illustrating that the tendency is to use off-the-shelf situational crime prevention techniques rather than those tailored to the specific problem at hand.

As cited earlier, of the 136 crime prevention techniques used by the finance sector, 62 are SCP techniques. Target hardening (increase the effort) is the technique that is use the most (29) followed by surveillance (increase the risk) which is used in 13 different aspects of preventing financial identity fraud. Other techniques in order of frequency of usage are access control (Increase the effort) 7, controlling tools (increase the effort) 6, set rules (remove excuses) 3, and in equal measure of 1 deflect offenders (increase the effort), reduce temptation/ arousal (reduce provocations), natural surveillance (increase the risk) and deny benefits (reduce rewards).

SCP techniques have offered an effective crime reduction strategy to the financial community based on empirical evidence and its evaluation. However, there are instances where the effectiveness of these techniques has been short-lived because criminals were able to circumvent the defences, as the data on fraud pre and post the introduction of chip and PIN cards testifies.

Because of the transnational nature of identity crime (especially the data breach and identity theft element), situational crime prevention techniques, which aim to reduce the opportunities for crime in the immediate environment, provide a more expedient approach/ method to reducing crime incidents.

SCP techniques, however, have not been free of criticism. Wortley (2010) in his examination of SCP techniques highlighted a number of criticisms directed at this approach. The first claims that SCP "lacks the vigour, complexity and sophistication for other criminological theories" and that it is no more than just "common sense". It does not explain why crime happens and is a simplistic response to a complex social problem. SCP ignores root causes of crime, such as poverty, inequality, racial, sexual and religious discrimination, in shaping its theoretical framework and therefore it "attacks symptoms and not underlying, systemic cause."

The third criticism is that SCP will simply displace crime but not fully prevent it. Wortley (2010) believes that there is a superficial logic to this criticism. He argues that "empirically it

has been found that displacement often does not occur, and where it does, it is invariably less than the amount of crime prevented."

From a social and ethical perspective, the criticisms have been that SCP disproportionately targets the poor and disadvantaged (but it is now increasingly being applied to other crimes such as computer-generated fraud) and that this approach allows organisations to shift the blame for identity and data theft to the victim as they expect the victims to take precautions to protect themselves.

SCP techniques are often cited as invasive and oppressive and might contribute to the creation of a fortress society. However, Wortley (2010) argues that "many situational techniques actually involve "softening the environment and bringing communities together" such as Neighbourhood Watch schemes. Generally-speaking, the finance sector, notwithstanding its charitable campaigns to support 'good causes' and locally targeted community initiatives, regards tackling the root causes of all crime as the responsibility of the government and the public sector.

5.12. Discussion

The banking industry has effectively utilised some aspects of SCP theories in managing financial identity crime. The two most used theories are 'increasing the effort' and 'increasing the risks' but the other aspects of these theories such as 'reducing the rewards', 'reducing provocation' and 'removing excuses' have been left almost untouched. Below are some recommendations on how these theories can be employed in the fight against financial identity related crimes.

Increased effort

Controlling access needs to be biometric rather than password based as the latter is becoming increasingly outdated and vulnerable to compromise. No data (particularly small data storage units or laptops) should be allowed to leave the company premises. Ideally, from a security perspective, the use of personal smart-phones would be restricted or banned in sensitive, data-rich environments.

Far tougher exit screening for those employees who have access to consumer data, is needed to make the offender work much harder to steal the data. Targets need to be concealed with an end-to-end solution and targets need to be removed by not storing consumer data anywhere or under any circumstances.

Offenders need to be defected by designing tests for those employees who work with data and specifically designing education for those employees who work with consumer data. And finally, controlling tools/weapons is needed on specific tools that facilitate production of devices to commit financial crime (such as certain electronics like PEDs and cards).

Increase risk

Extending guardianship by increasing the role of the police and their responsibility in dealing with identity related financial crime would be a way of increasing the risk to commit this fraud. The appointment of board level data protection directors who could be an IT specialist or just a resource dedicated to overseeing secure handling of data and preventing compromises is needed to ensure companies have a dedicated resource in this area.

Within organisations there needs to be a system where every time someone searches for data the system will record it and flag it (reducing anonymity). It is best that all employees are well-informed about these measures, so they are aware of the increased risk of being apprehended. This will have an impact on averting internal staff data theft and improve processes inside the organisation so that, in case of a breach, the company can track the source of the compromise. And finally, regular surveillance of employee social media accounts accessed (potentially inappropriately) in the workplace for signs of collusion with fraudsters (strengthen formal surveillance).

Reduce the rewards

A system needs to be employed where all stolen identities are flagged making them less valuable to fraudsters (identify property). It is well known that the identity data stolen by various organised groups end up on the internet for sale. The banking industry should exploit the use of this strategy (notifying the potential data buyers that the names are flagged) to disrupt such operations on the internet (disrupting the market).

Data needs to be made useless for hackers and criminals by employing better authentication/encryption processes (denying benefits). This is the most challenging aspect to the finance industry. This is an industry wide issue/challenge. The first line of defence needs to be focused on researching the best authentication methods available and employing them. Experts should be consulted so that improvements can be made to the available solutions to make them more effective. The measures then need to be implemented quickly. Fraudsters target those organisations that have the weakest systems, so if an effective solution is adopted, it should be implemented industry wide not just by a few organisations so that there will be no weak link in the chain to be targeted by fraudsters.

The industry is well acquainted with implementing and working to standards. Standards could be developed in authentication to assist in the process, establishing the benefits of these defences so that they can be used in business cases presented to non-fraud prevention decision makers within these institutions.

Reduce provocations

Reducing frustration and stress may be effective in minimising employee data theft caused by stress. If employees are stressed or under pressure it may drive them towards stealing data or it may make it easier for organised gangs to convince an employee to participate.

Avoiding disputes could be another effective way to reduce internal fraud. A disgruntled employee may commit fraud as revenge against his/her employer. Such disputes should be resolved amicably. Good clear human resources policies covering grievance procedures, escalation procedures and fair internal tribunals (with independent parties outside the organisation) would help in such circumstances.

Important information which is inadequately guarded increases temptation (reducing temptation and arousal), ensuring that there are systems in place both in computing and procedures to offset such arousals. This could be considered in three different stages: accessing data, use of that data and removal of that data. Imposing time limits for the access and use of data would assist in increasing risk and reducing temptation.

Neutralising peer pressure could have a positive impact in reducing provocations. It needs to be widely publicised to the entire staff when a colleague has been apprehended and/or arrested for stealing data. This will produce a positive impact on deterring those who might consider crime under pressure from colleagues or criminals.

Remove excuses

Setting rules is crucial for helping to tackle the insider element of identity related crimes. All organisations, small and large, need to have rules in place governing processes and staff behavior when handling financial and identity data. Any such rules need to be openly and frequently communicated to staff (posting instructions).

Messages, electronic or hard copy, can be introduced in a number of situations and places such as at ATMs or screen prompts before the final stage of an online transaction or on staff noticeboards (alerting consciousness) to remove excuses along with controlling drugs and alcohol. Controlling drugs and alcohol could have an impact when dealing with employees under the influence of alcohol or drugs who may be tempted to steal data. Some may even

do this to feed an addiction. At the beginning of the employment stage, tests could be carried out to make sure that the person being employed is free of such addictions, and vigilance from line management and Human Resources should be continuous. Offering anonymous counselling to staff affected by drugs or alcohol may also be beneficial.

In practical terms an effective crime prevention program needs to go far beyond situational crime prevention theories. As can be seen from the above, current holistic crime prevention practices include data sharing, intelligence, awareness raising, training and education. Regulation and guidelines also play an important role. In order to have an effective strategy, all of these elements need to be present as one alone may not provide the satisfactory result that the organisations expect.

It is evident that financial identity crimes cannot be fully eliminated but they can be reduced, disrupted or displaced by effective prevention and mitigation programs. An effective program should include strategy in intelligence, prevention (such as utilisation of SCPS), authentication, detection, reporting and information management, regulatory policy and finally communication policy. The respective organisations should also have the necessary resources and funds to implement the strategies in addition to a dedicated team that can carry out the necessary work. Commitment from all involved - such as different departments and stakeholders is also imperative for effective implementation and continuation of crime prevention programmes.

Strategies need to be both long term and short term with different outcomes. Short term strategies can focus on imminent threats and to ease or relieve the losses of specific fraud types which are causing big losses. Once such issues are under control, long term crime prevention strategies also need to be put in place to effectively manage such on-going and new perceived threats.

Liability shifts represent an important factor in fraud reduction. It is a strategy that payment card brands have been using to drive the EMV migration for merchants to upgrade their payment infrastructure. The liability of a chargeback from a credit card ultimately rests with the Issuer but only in the event that the card issuer has inferior or matching technological defences to the merchant. For the issuer, that technology is represented by EMV chip cards and for the merchants by EMV-ready terminals. In case of a technology tie, the fraud liability remains with issuer. An ownership plan needs to be developed when tackling identity related crime and businesses are to be held accountable for the parts that they own. As society is moving more and more towards mobile technologies and payment systems, a better outline of ownership is necessary to help understand and manage liability shifts.

Within the banking industry, fraud is relatively a non-competitive area - that is to say, the banks do not see having a better fraud prevention system than their peers as a competitive advantage. At the FFA's forums, members discuss and collaborate on various projects and work to combat financial fraud. Benchmarking and performance monitoring could be an effective way of making sure that each partner is controlling their issues. Once established in the UK, this could be extended internationally if foreign banking/finance associations were prepared to co-operate and introduce identical methods.

There are other effective tools to include in a holistic fraud prevention program such as an alert system that can inform all financial institutions of the latest fraudsters' MOs. Equally, the setup of an effective alert system for customers of each bank or financial institution would be extremely useful. The only alert system in place, at the moment, belongs to Action Fraud but the extent to which the general public make use of it is not known. Incident impact assessment and management is another effective tool to reduce the impact that certain harmful frauds have on consumers. The impact of the fraud on the consumer is logged and analysed and support strategies improved as a result.

Examination of financial identity crime and the finance sector's response to it give weight to the fact that, in many cases, identity fraud can be effectively controlled. For example, situational crime prevention methods were employed to reduce the instances of counterfeit payment card crime between 2001 and 2008. The responses from anti-fraud practitioners in this research highlights a desire to tackle the problem of identity crime at grass roots level but they often lack effective support from their senior officials, for whom it is not a top priority. There was also a significant indication from respondents that situational crime prevention on its own is not enough and that other methods, such as information-sharing and regulatory pressure also need to be included in the overall strategy.

The finance sector and their approach to handling this data can be used as reference point for other sectors. The framework that they use is very effective, especially in collectively dealing with the issue. The researcher through her work experience observed what a central role the finance association's fraud control unit played in helping the member banks to deal with the issue. The data was regularly (monthly) collected, collated and reports were produced using this data. This information was then fed into the UK Payments Threat Assessment enabling this industry to prioritise the most pressing fraud issues on which to focus. The forums that focused on payment crime issues met regularly (bi-monthly) with clear agendas. Actions were then driven from the discussions held in these forums and the

Threat Assessment along with the allocation of adequate funds to help drive the necessary action and projects forward.

The banking sector, in many respects, is the market leader in dealing with fraud, whether it is in measuring it or in their efforts in preventing or tackling it. Although it was established among participants that identity crime prevention was not an area of commercial competition between them (the need for data sharing in order to understand and predict and hence better defend being greater) there still appear to be issues with openness on the part of some participants and the level of contribution they were prepared to make to the research questions and objectives.

The payment industry has a clear definition of different fraud categories. They measure, report, and make decisions based on informed and factual data. They have built up relationships and partnership channels and infrastructures and platforms have been developed for communications so as soon as the need arises these channels are used to either develop strategies together or to share and implement the strategies that have been developed by Financial Fraud Action UK to address the fraud issues. This sector is the only one in the UK that has successfully achieved this structure. Other industries could copy the same infrastructure to achieve the same level of transparency. However, the complex financial transaction layout and the busy and multi-layered infrastructure is criticised as a contributor to the vulnerabilities that exist in this area.

In the next section, in order to provide a complete picture of identity related crime within the remaining institutions in the private sector, I will examine the feedback provided in the interviews from the fraud professionals who deal with this issue on a day-to-day basis.

5.13. Responses from private sector participants to key research questions

Introduction

In the previous chapter, I examined the identity related crimes specific to finance sector, highlighting the different types of identity crime within this sector, the complex nature of the whole payment infrastructure, approaches employed to prevent this crime (especially the SCP techniques) and finally, some recommendations for taking these prevention techniques and approaches further. Answers to interview questions will enable this research not only to capture more details from the professionals in the finance sector on dealing with this issue but also present a fuller picture of other players' views and approaches in tackling this issue.

This section presents the results from interviews conducted with the private sector participants and includes representatives from the finance sector, retail, telecommunication and other relevant parties. It will focus on the first-hand data collected from participants from the sectors mentioned, capturing their perceptions of identity crime, measurement systems, trends, knowledge of offenders and victims, objectives set, fraud detection methods employed, prevention and mitigation measures used and an examination of the partnership/multi-agency initiatives undertaken and their reported effectiveness. The recommendations of the interviewees will be summarised and finally, the chapter will close by discussing the main points arising from this front-line feedback.

5.13.1. Perception of identity crime

There are various responses to the question on the participants' organisations perception of identity crime. Key perceptions emerging are that identity crime is a threat, tackling it is a high priority, it negatively affects victim organisations' reputations, it is growing, anti-fraud professionals are feeling outpaced by identity criminals, it plays no role in establishing competitive advantage and that in some cases it is regarded as a cost of doing business. Interestingly, the concept in the question had to be explained to one respondent and even then, there was a slight hesitation with the answer - which was that identity crime is considered a threat (R5).

The perception that it is a threat, a major threat or a growing threat is cited by five respondents (R5, R7, R14, R21, R26) with a particular reference that organisations "down-play it and don't talk about it" (R21) and that "if weaknesses exist, public admission promotes awareness of that vulnerability and its subsequent criminal exploitation" (R6).That identity

crime poses a serious risk was cited by four respondents (R11, R12, R19, R21). The corporations' views are varied, for example, a mortgage lender will have a completely different risk perspective than a mail order product provider. It is acknowledged that businesses are different and are impacted in different ways, therefore, different organisations categorise the risk differently (R12).

There is additional recognition that the risks, in the retail sector, are both financial and reputational: it is expensive to prevent identity fraud but these costs, and any subsequent financial losses incurred as a result of a data loss or compromise, play less of a role in influencing businesses to change or implement additional security measures than the reputational damage caused by such compromise (R16). Another respondent states that organisations will essentially deny that identity crime is too much of an issue on the grounds that they are concerned that if they admit to it being an issue, it will attract unwelcome attention from the regulators (R15). From the general public's perception, one respondent offers that they are increasingly understanding how crucial and how frequent the use of their identity has become in acquiring most of the products and services that they wish to obtain in the private sector and public sector and the need to trust organisations who use it (R6). The influence of reputation is further highlighted when one participant states (in relation to ATM fraud) that this is a high priority for them because of the consumer's perception of the risk, further elaborating that even though the risk is low (the number of people who are skimmed is relatively lower than the number of transactions that are taking place) in practice, in any focus group 8 out of 10 people seem to be claiming they have suffered, or they know somebody that has, which is an extraordinarily high number - so the perception of the risk is much higher than fact. Therefore, the perception of customers should be managed so that they know that the ATMs are safe (R11). One participant provides an alternative perception claiming that not only we do not know the full extent of the problem, some businesses are not aware of it, emphasising that if the truth were to be known and the true number of people who have been compromised were discovered, everyone would be shocked (R17).

On the extent to which the identity crime fraternity remain ahead of efforts to contain their activities, three respondents concur (R7, R14, R17). Identity crime is considered to be a growing problem and one that is difficult to tackle as the security systems imbedded in business models, which were adequate to prevent fraud at the time, stop working once the fraudsters, with their agility, find a way round them, making it difficult for businesses to keep up and makes future planning more important (R14). One respondent believes that businesses are very scared because they still do not realise the extent to which fraudsters have the upper hand and that they are still playing catch up (R17). Believing that they do not

fully understand the depth of some of the fraud and they are still learning. They get caught out quite frequently on all sorts of identity related crime, so the fraudsters are two or three steps ahead and when the retailers manage to close one loophole there are still others. Fraudsters just go and change something small and they are back in business (R17).

Other views expressed about the perception of identity crime includes acknowledging that it plays no role in establishing commercial competitive advantage, that each company is at a different stage in tackling the problem, that these factors facilitated collaborative efforts among otherwise-competing companies (R15) and that many organisations simply regard the impacts of identity crime as a cost of doing business (R18) or an opportunity to sell their identity fraud management products and services (R21).

5.13.2. The various organisational levels with responsibility for identity crime.

The issue is discussed and dealt with at various levels within organisations (R14), often depending on the sector, and range from the highest level (R6 & R11) to a more 'operational level'(R11, R15, R18 & R23). Those organisations which manage the issue at the highest level are generally in the retail sector (R6). This sector is sensitive to financial penalties which may be imposed by the ICO if a compromise takes place. They also very sensitive to the negative publicity generated when data compromise happens, especially when it affects the poor and vulnerable placing. Such instances put the business community under pressure to be seen to be responding at the highest organisational level (R11). One participant states that he reports directly to the financial crime director who reports into the executive board who co-ordinates initiatives across the group in the UK (R18). Another respondent states that most of the credit retailers have a large anti-fraud team in their financial services team because they use various technologies and sometimes, they use outside agencies to screen the applications and transactions for suspicious ones. For example, one retailer has 100 full time staff who prevent £16million worth of fraud every year (R19).

Those respondents whose organisations have relegated identity crime to lower, more operational levels include smaller businesses or those which are able to maintain a low public profile (R15). Often, identity crime management is the responsibility of the finance department thus senior management is not particularly aware of or called upon to deal with it. In some smaller front-line retailers, they employ as little as 2 full time staff (R11).

5.13.3. The extent to which participants are impacted by this crime

The emergent themes point to differences in the size and complexity of the organisation in question. Some respondents admit to being impacted by identity crime but are unable to "get a handle on it" (R11), or they prefer to downplay it (R14).

Divergent responses are presented about larger entities with some claims that these have superior identity crime protection systems and more stringent processes (R5 & R6) whilst others highlight the greater complexities of larger, global organisations which produce greater weaknesses and thus more opportunities for fraudsters, particularly in the area of outsourced third party product and service providers (R5 & R23).

Conversely, smaller organisations, having weaker identity crime defences may, on the one hand be more susceptible to successful attack by fraudsters (R6), and on the other, be safer as they have a smaller customer base and know those customers more intimately and are thus not so easily deceived (R23).

5.13.4. Measuring this crime

Three issues are highlighted by participants with regards to measuring this crime. It is believed that this crime is hard to identify because there is a lack of clarity (R14), the police do not record identity related crimes (R23) and finally, the figures that exist in this area do very little to bring some clarity to this issue. One participant states that "I keep away from numbers because people are totally confused" (R21). Measuring this crime is one of the major challenges that exist in dealing with this issue (R23). One participant states that not only do we not know the full extent of the problem, some businesses are not even aware of it (R6). Another participant thinks that no one knows how much identity fraud is committed as much of it is written off as bad debt (R12). In terms of correctly measuring this crime, the banking industry is the market leader. Some industries do not collect and collate information in a similar vein to the financial sector, but they think that this is something that will happen in the future, as these industries continue working collectively on the issue but concerns still exists in 'showing your hand' to others (R14).

There is also the belief that while everyone is so concerned about impersonation, there is a huge amount of identity creation happening, which is much harder to detect. Some fraudsters add themselves to the electoral roll, potentially forging identity documents, making applications for a current account, credit card, loans and maybe running them successfully for quite some time and building up a credit history and eventually turning bad, that may look

like somebody going into debt but in reality it is something more sophisticated, so that has been underestimated (R12).

5.13.5. Trends/methods

The three key trends noted by respondents are that fraudsters are attacking newer, data rich companies with sub-optimum identity data protection routines such as the mobile phone companies (R6 & R14), that corporate identity theft, as a basis for employment scams of immigrant labour (R24) or as a means to seduce smaller companies to trade and pay in advance and then defraud them (R24), are currently dominating the modus operandi of identity fraudsters.

5.13.6. Defining identity crimes

This question produces many responses with the most common themes being that is a complex subject, there is no clear definition of identity crime and that there is a focus on combatting it rather than debating its definition. Comments include: “Some sectors have been trying to get standard definitions around all sorts of fraud types but they believe that identity crimes are the hardest to define (R23)”, “it is a complex issue and one definition can’t fit it all (R16)”, “One of the issues that comes up all the time is whether to call it identity fraud or identity theft or identity crime, and there seems to be different opinions and different forums seem to have different names for it” and “the Home Office considers all types of payment fraud to be identity crime but the banking industry has different definitions for each type of card or payment fraud (R16). As far as one participant is concerned there isn’t an agreed definition (R7). Other contributors offer the following: defining identity crime presents an issue similar to measuring it, it is a very difficult area (R24) and others state that they don’t really define it (R18 & R26). Another interviewee goes even further by saying that they do not have a clue and that returning money stolen from customers is a top priority rather than looking for a definition (R19). Despite the majority of participants having issues in this area, only one claims that they have clear definitions depending on which products or services are defrauded (R2).

5.13.7. Private sector’s knowledge of the victims

Themes emerging from responses include the ubiquity of victims and the increased risk amongst specific demographics, the impact on organisations versus individuals, the lack of consumer awareness of identity crime, the invisibility of victims to some organisations, the banking system taking the brunt of assisting victims hence their strategy to transfer liability to

victims, the fact that organisations are also vulnerable to having their corporate identities stolen and the efforts to create an effective victim support system.

One participant believes that everybody, the general public, small and large companies and the government are all victims of this crime (R15). Three respondents offer that victims are the general public, businesses and individuals who use the services of the banks and other government organisations (R11, R15 & R23). Whilst victims are believed to be variety of people across the social spectrum (R14), one respondent believes that the people who use their credit cards everywhere tend to be victims alongside specific sections of the society such as people who rent and change their address (which makes people quite vulnerable because someone can pick up their mail) (R12). One of the segments of society which is most vulnerable to this crime is the student population which is mainly due to their lifestyle. Their identities are not used straight away by the fraudsters, instead they wait until these students get a job and their credit rating improves to abuse their data (R16).

A leading theme from the research was that the victim organisations and financial institutions suffer financial and reputational loss whereas the individual victim suffers inconvenience and often emotional upheaval (R11 & R19). There are two implications for businesses with identity crime, one is financial loss and the other reputational and the fact that if someone becomes a victim they will not shop there again believing that if the fraudsters hacked there once, they can hack again (R17). Another participant believes his company to be the biggest victim with the consumers only being inconvenienced (R18). The issue of identity crime is not confined to individuals, businesses and organisations are victims as well by having their identity stolen (R15). This point is further elaborated by stating that companies and businesses are victimised in two different ways. In one, their identity is stolen by fraudsters when they pretend to suppliers to be them and in the second one the details of consumers are stolen from a company or business (R24).

Another common theme amongst respondents is the lack of awareness of identity crime. The Home Office, in collaboration with other businesses and organisations, addressed it by establishing the Identity Fraud Consumer Awareness Group (IFCAG) with a number of initiatives, one of which was the development of an identity fraud prevention website to increase awareness about preventing victimisation with tips and advice. It was a practical guideline about what should be done. The website was then expanded into leaflets because not everybody has access to a computer and the internet. These leaflets are now freely available in Citizen Advice Bureaus (CABs), public libraries, police stations and various

government organisations such as the DVLA. They were also made available to all the banks and they were able to label them and incorporate them into statements as well (R16).

Some organisations never get to find out who the victims are. On rare occasions someone might get through to report their victimisation but generally victims are advised to contact their bank or card issuer to deal with the issue (R2). Another participant argues that they don't receive any information about victims as they are a strategic organisation and it is not necessary for them to have such information (R13). Organisations that focus on strategic responses to this issue are less in contact with the victims and instead use the collected data to focus their strategic response on the sectors of society that present the highest risk of victimisation in this area (R16). Some commercial businesses claim that they do not have the set up to assist victims to recover from this type of crime and that their procedures simply extend to co-operating with the agencies charged with solving /fixing the crime (R26).

Banks are getting tougher on what constitutes as negligence (R26) something that will have a very devastating impact on the victims. As some of victims already think that it is worse than being burgled (R19). The banking industry's message to their customers is that providing the customer hasn't been negligent with their PIN number or other personal data the banks will restore the damage. Unfortunately, however, the banks find that some of their customers are reckless with their PIN numbers (R11). The impact on some victims has been so great that there have been cases of suicide amongst them (R24). Another interviewee refers to the challenges of knowing who the real customer is, especially when they call and claim to be the victims of identity crime. The fraudsters know this and are using the technique to defraud the banks (R23).

The retail industry has been working a lot to convince the government that this is not a victimless crime or a crime against an organisation. Some of the government organisations such as NFIB (National Fraud Intelligence Bureau) and Action Fraud believe that the real victims of this crime are the businesses who bear the financial loss and are denying the impact that this victimisation is having on the individuals (R19). Some attempts have been made to help the victims of identity crime. Previously, a victim they had to call each of the 3 credit reference agencies. However, now the credit reference agencies have joined forces so a victim only needs to call one of the agencies, which then contacts all the lenders on their behalf and provides them with a year free of their credit report. As well as general advice (R12) they are given a password and a case worker to help them out (R23 & R24). Although these agencies provide a service for victims of fraud to help them with their victimisation, they get their money back by selling other products to victims (R16).

5.13.8. Private sector's knowledge of the offenders

Participants' responses span the spectrum from being unable to identify fraudsters, to opportunistic individuals to organised crime gangs and finally to nation states. Two participants (R18, R26) state that they do not have a clue who carries out these crimes- one elaborate by stating that they do not have a clue because most of their resources and time are used to help the victims and give their money back (R18). Another respondent states that identity crime involves a lot of opportunistic behaviour, arguing that there are large numbers of people who move into someone else's address, pick up their mail and abuse their data. Most people do not know the culprits, but some victims blame it on ex-spouses, ex-partners or other family members. The rest of this crime is believed to have been committed by organised gangs (R12). This statement is further elaborate by another participant who argues that this crime is perpetrated by small time crooks on an individual basis right the way to organised crime networks who are very specialised in identity related crimes from fake passports to international documentation (R15). The focus on organised crime gangs also focusses on their nationalities. "Apart from muggings which are the last resort of the desperate, the others are organised criminal groups, the information available indicates that they are mostly East European, Romanians are the majority. The funds obtained from identity crimes are used for other criminal activities" (R11). The offenders are either the last resort of the desperate or organised criminal gangs. The data that some businesses have indicates Eastern European gangs being mostly the foot soldiers in ATM fraud and mostly Romanians (R11). Another interviewee makes the distinction between the foot soldiers and the big bosses. The latter tend to be in other countries collecting the proceeds of their crime while the former is in the UK using stolen or fake identities. The foot soldiers come to the UK to commit the crimes and when law enforcement recognises them and just before any action is taken against them, they leave and new faces come to the UK which makes catching them extremely difficult (R17). Some fraudsters behave like businesses, with professionalism, and sit around the table and discuss their MO's and data attacks (R12).

Another response highlights that the organised crime networks committing this crime have links to terrorism or people trafficking (R16) whilst one interviewee cites that cyber-attacks for identity harvesting can be state sponsored, mainly from Russia and China, using organised gangs and individuals (R24).

5.13.9. Objectives employed with regards to identity crime

The objectives for the private sector are divided into two main groups of participants: those representing trade associations and those that belong to private businesses and organisations. This data is, therefore, presented differently as these two groups have different functions and objectives.

Trade associations (R7, R11, R14, R15, R16 & R17)

The seven main objectives of these representatives are: remaining the leading organisation in the UK in tackling, preventing and working with others to prevent identity fraud, reducing the impact of identity crimes and reducing the amount by which identity issues enable wider crime, are two of the objectives generally stated, sharing information and better intelligence sharing across government and with private sector and more effective ways of ensuring that intelligence reaches the front-line practitioners, raising awareness by campaign, educating customers and educating the membership base on data protection and the importance of the effective destruction of identity descriptor information, working collaboratively (the issue is non-competitive, looking to either eliminate it or displace it) and reducing the total number of attacks by encouraging members to work together, minimising fraud losses and disrupting and preventing fraud and finally data mining and matching.

Private sector (R2, R5, R15, R18, R23, R24 & R26)

Objectives vary more widely in this group but can be categorised into four different levels: reducing the value attached to each transaction, staff awareness campaigns, additional checks carried out by staff and effective disciplinary processes. These manifest themselves in the following tactics: raising awareness that anyone can become a victim, teaching them about the signs of victimisation and how people can protect themselves, having identification control, targeted messages, risk assessment at top level, managing the big threat of insiders enabling identity crime, to have an intelligence capability and finally to adhere to the requirements of the Data Protection Act.

5.13.10. How these objectives are set

The methodology driving the setting of objectives varies by type of organisation. Data that is collected from member organisations are used to identify potential identity fraud attacks and to devise strategies/objectives to address them. This is achieved by using two resources: members directly contacting their respective association or the association's data analysis identifying and highlighting the necessary trends (R11).

For one association, the committees are presented with a large amount of management information which enables them to discover and highlight developing trends. Either this data will be used, or the members present at the committee will put forward an issue that they have been experiencing. Further research may be carried out and then the issues are addressed. This whole process involves regular monitoring (R16).

For some organisations the different business areas set their own objectives as part of a business planning process. Once these objectives are set there may be interdepartmental collaboration to achieve them (R15).

For other organisations, each business unit sets its own objectives and then communicates them to the other units. These objectives are also shared with, or worked on collaboratively with, other businesses in the same sector (R23).

For smaller businesses, these objectives are set by their finance departments as they are the ones who see the data and can highlight fraudulent transactions. The objectives are set on an annual basis and the costs of handling this and the financial losses caused by fraudulent activities are built into the pricing structure (R18).

Within the finance sector, the Association is believed to be a very useful resource to help individual businesses set their objectives. The businesses use all their resources to tackle fraud issues but co-ordination is necessary with other business units. For example, one participant refers to a calendar where different business units' activities are demonstrated inside the organisation as a whole. Fraud campaigns cannot be organised at the same time as marketing campaigns for new products (R23).

5.13.11. Who sets the objectives

Broadly, the objectives of the trade associations are set by the members, however, those of larger companies, such as retailers are set by senior management.

The objectives of the organisations that are member-driven are set entirely by their members but because the size of each member of such organisations and their objectives may vary from each other, the membership organisation sets the objectives according to what they think the members want and gets the members to approve them (R11).

With other associations members who set their own objectives, they have various committees with a chair and a deputy chair. They use management information enabling them to compare members' fraud levels to each other and to set benchmarks (R16).

Within some businesses, a risk assessment is created at the top level of management which is overseen by the PLC and an Audit Committee, so a member of the PLC board, non-executive director, would generally chair that particular group, with the CEO and the Chairman also present at this board. The board oversees the good practice around not just identity crimes, but everything else in the company, and then under this board there is a corporate governance group, a working group and an IT security group and an intelligence capability sitting under this. The board sets the overall objectives and the groups sitting underneath that board carry out the work (R24).

5.13.12. Detection methods employed by the private sector

The private sector employs fourteen key methods to tackle identity related crimes. These methods include data-sharing, internal and external customer data monitoring, information technology systems, whistleblowing campaigns, engagement with law enforcement agencies, using a holistic approach.

Holistic approach: detection of fraud, for some, is using lots of different methods such as whistle blowing alongside technology such as data mining, where irregular patterns are discovered. Data mining also helps businesses to build a case with enough evidence for potential investigations (R17, R18, R19 & R23).

Good relationships with other stakeholders: this method is believed to be effective in order to identify problems in a timely manner (R2). It also helps some organisations to detect identity crimes.

Liaison with other organisations: has been an effective and helpful way for some in their detection efforts (R5).

CIFAS database: the other data source that is believed to have helped in the detection of fraud is the use of CIFAS database (R19).

Customers: in some cases, the organisations interviewed found out about the crimes through their customers phoning in and complaining (R24).

Monitoring customer chargebacks (passive detection): this is a method that is prevalent mainly in the retail environment. This should be treated as an outcome of a compromise rather than a detection method (R2).

Customer Blacklists: some believe it to be almost impossible to detect this crime with the first contact with the customer but using a blacklist of suspicious cards provided by the credit

companies or other retailers operating in the same space increases the chances of successfully preventing the fraud. However, if the fraudsters are not caught at the first attempt, which mainly they are not, then there is no way to detect the crime (R18).

Manual and software detection systems: manual systems are used to detect identity crimes as well as software systems such as neural networks for unusual patterns (R19, R23 & R24). Some participants closely follow the new developments in fraud detection software so that they can utilise the latest technologies in this area (R23). In some organisations, regular monthly meetings are held to monitor identity crime and trends in order to put necessary measures in place to prevent it. Once an issue is identified then necessary investigative techniques need to be developed to deal with it (R23).

Detect: is used by some participants which is a software that examines application data and points out if there are any discrepancies. It also checks to see if there are any matches against other applications. For example, if a mobile number has been used by two different applicants it would be highlighted (R12).

Dashboard approach: In some large organisations, dashboard approach is used to detect this crime (R14).

Common Point of Purchase (CPP): with card fraud CPP would be a way to detect where card data has been compromised (R11 & R24).

Device recognition: a technology which is mainly used by retailers to detect identity crimes (R19).

Hunter: this system basically records where fraud has occurred and whether an application has been declined (R12). Although a range of technology-based systems are used to detect identity related crime, they are not free of problems. They cause something called ‘false positives’ where a genuine transaction is highlighted as being fraudulent. Additionally, some fraud prevention techniques, such as Verified by Visa and Secure by Mastercard, are believed to be not as effective as they sound (R19).

Whistle blowing: some businesses are using this technique both internally and outside the business to get information on fraudsters and those within their organisations who might be collaborating with fraudsters or who may have been put in their job by the criminals (R17).

Law Enforcement

There is a big difference between various organisations when it comes to investigating identity crime. This depends on the nature of the organisation and their role/business. In some organisations, serious investigations are not carried out at all. In most cases, it is believed that the card issuer will just pay the victim and will not discover the point of compromise and, in instances that the point of compromise is identified, the only action taken is to stop or block the cards that have been used. Additionally, the police do not get involved for standard skimming incidents (R11).

Other organisations go further than just reporting it. They involve law enforcement once a fraud is detected in order to capture the offenders by using a method called 'control delivery' whereby, if someone is suspected of not being the person they purport to be, the parcel delivery will be run and a police officer will be close by to arrest the suspect. This strategy is very successful to the point that it has enabled the police to access some of the organised crime groups. Many police forces are happy to cooperate with businesses using this method but other police forces are not very helpful or keen to participate with such techniques (R19).

Most participants were not aware of the percentage of cases reported to the police that were investigated and, once again, most participants were not aware of the percentage of investigated crimes that resulted in prosecution. There is only one interviewee who is aware that only 3% of cases passed to the police were investigated (R24). There are some efforts to have the numbers of cases that go to the forces outside of the MET published because it is felt that ,once the Commissioner knows how "awful the performance is", he will have to find the resources to deal with it. Despite the low investigation rate, one participant believes that the prosecution rate has increased significantly (R24).

Some organisations experience identity crimes only in relation to people seeking employment with them. In these cases, the HR team and usually a liaison person working with the Border Agency, deals with the issue and due to "stringent processes and an excellent fraud department" the respondent claimed to have no issues in this area (R5).

5.13.13. Prevention methods employed by the private sector

One interviewee states that the mechanisms to address identity theft are not simple or straightforward. It needs to be embedded as part of business process (R15). As the nature of business is different for various organisations, there may be slight differences in the type of prevention methods that they employ. To highlight these differences better, the prevention

techniques employed by different sectors, finance, retailers and telecommunications, are presented individually.

Financial industry

The financial industry uses a number of methods to prevent and mitigate identity theft crimes. Protecting consumer data is one of them which plays a major role in their strategy, making sure that consumer data held by all organisations involved in the Payment process is secure (R15) and making sure that the people who have access to consumer data can only access part of this information and not all of it which is called the 'segregation' technique. Therefore, the employees with higher positions (such as team leaders) have more access to data than the ordinary front-line employees (R15). Sharing information and intelligence is another tool used which is an important and growing focus for the banks (R23). Strategies are also employed to limit both internal and external attempts to steal data (R15) in addition to education and raising awareness (R23).

Developing an understanding of what criminals are doing and their methods (R23) is another method used along with employing ex-police officers. One of the organisations interviewed employed ex-police officers to identify current and potential insider criminals. Another technique employed is that, when an offender is detected, the organisation ensures that enough evidence is assembled before the police are contacted and are asked to come and arrest the individual. The police are happy with this approach, as effectively, all the ground work has been done and all the police have to do is to turn up and make an arrest with all the supported evidence so they can prosecute and score points for a successful arrest (R15). This approach is also effective in deterring others from internal wrongdoing as the arrested and handcuffed individual is walked through the office so all the other employees can witness his/her arrest. It is an effective 'naming and shaming' technique. However, this practice is not common across the banking sector and some banks even "frown upon it". Most would just go as far as suspending the individual, but this would make collecting the evidence difficult if the suspect gets rid of it therefore making it a disciplinary matter (R15).

Disrupting the criminals' activities is another technique used. It is argued that catching the criminals is not always easy, but if their activities are interrupted and disrupted, they may give up their efforts (R23). Attempts are also made to recover some of the money from the criminals who have been arrested and prosecuted (R23).

Developing and providing a platform for all the banks to report their cases so that a collective case can be presented for possible investigation (R16) and encrypting the PIN number

instantly when it is entered on the ATM machines (R11) are two other techniques employed by this sector.

The financial institutions also focus on using specific software on the ATM machines which makes it difficult to break into them. Although this software is effective, circumventing it is not impossible. In addition, the use of a Card Protection Kit is effective in making it difficult for the fraudsters to skim the cards. However, anti-skimming devices are not fitted to all machines because it is believed that not all the machines are vulnerable and the vulnerability varies (machines inside the banks or shops or the ones which are less busy are less vulnerable) (R11). Other techniques are also used to protect the ATM machines, such as physical barriers, but in some cases these methods have been counterproductive since some criminals have removed them and replaced them with skimming devices (R11).

Retailers

Retailers similar to the financial sector employ a number of techniques to prevent and mitigate this crime. Education is a major technique which is believed to require government assistance as it is a very big task (R24) along with staff awareness. Some retailers take the approach of telling their staff about identity crime scams on their employment induction day, sending them the message that “don’t even try to commit insider identity crime because we will know what you are up to and if we catch you, you end up with a criminal record” (R17). Other retailers take the approach of not saying anything and just building the evidence and the case in the background in case of a suspected insider identity fraud. But making sure that they tell everyone else that they have caught someone thereby sending a prevention message to their employees (R17). It is believed that between 10 to 14% of retail identity theft is due to insiders (R17).

For one participant, whistle blowing seems to be not so effective because their employees tend to work in small teams and if the offender is aggressive it will make it difficult for the whistle blower. If the offender finds out or suspects the whistle blower, they can make it very difficult and dangerous for them (R17). Nevertheless, it is a technique which is employed by some retailers to tackle the issue.

One respondent believes that, with respect to sensitive data, it is easier to protect something when it is not there than to protect it when it is present therefore adhering to PCI DSS is a major technique employed by this sector. Data protection needs to be embedded as part of the day-to-day business processes, something that small to medium sized businesses are not doing at the moment (R6). In the UK, all large retailers are at some stage on their

journey towards compliance with Data Protection Act, and even if they are not fully compliant, they are able to evidence their status in their journey. Medium sized retailers, however, are being fined regularly for not complying and are, to some extent, working on their compliance. The small sized companies are where the most risk is (R6).

Other techniques employed include: intelligence collection, trying to collect as much information as they can about those who commit this crime (R24), employing technology to combat identity crime (R24) and finally, lobbying. Industry representatives lobby for appropriate use and proper response by law enforcement agencies (R24).

Telecoms industry

The telecom industry members are believed to have a dashboard approach to tackling this fraud (R14). They have an acceptable amount of losses and while the losses are at this level, it stays below the radar, but as soon as it exceeds this the alarm goes off (R14).

5.13.14. The organisations that the private sector works with in partnership

All the private sector respondents interviewed work with other organisations to combat this issue. Banking and financial sectors work with the following organisations: other banks or financial institutions, Dedicated Cheque and Plastic Crime Unit (DCPCU), Crimestoppers, Leasing reference system (document checker), IFCAG**,** Citizen Advice Bureaux (CABs),Public libraries**,** DVLA, Scottish Business Crime Centre**,** National Consumer Council, Credit reference agencies**,** UK Payments, BBA, SOCA, Police, and IPS.

Retailers' efforts are divided into strategic or operational collaborations. Respondents report that, until recently, the retail industry has not been good at working collaboratively, but this is now changing. They work with following organisations: British Transport Police, banks, Visa and Mastercard, IFCAG, Information commissioner, Scottish Business Crime Centre, FFA, FFB, NFIB, Metropolitan Police, NCA, Insolvency Service, National Trading Standards, Crimestoppers, Vendors, professional ethical hackers, professional psychologists, Law enforcement, prosecution authorities, British Retail Consortium (BRC), Police commissioner, Mayor's office and CIFAS.

5.13.15. The context within which these organisations work together

Private companies and organisations

The context within which the private companies and organisations work can be categorised to six main activities. The first one is focused on influencing government, Chief of Police and

the Mayor's Office at a strategic level by telling them what they can do to help (R19) along with law enforcement engagement which is at an operational level and is focused on trying to persuade them to accept, and act upon, fraud reports from retailers (R19). Efforts are directed at better fraud screening to improve fraud screening which happens on a one-to-one basis between retailers and the vendors (R19). Information sharing is next trying to start up an information sharing database (R19) and to maintain the various data sharing initiatives already in place (R21 & R26). The last two activities that these partnerships focus on are raising awareness and product development (R21).

Associations

There are four main activities that the associations focus on which are liaising over the Data Protection Act (GDPR) (R7), encouraging law enforcement to take more interest in this crime (R11), sharing problems (R14) and finally raising awareness about identity crime by developing a website/ leaflets and running campaigns (R16).

5.13.16. Effectiveness of these collaborations

Banks and financial companies and organisations

Five respondents contributed answers to the effectiveness of collaborative initiatives. One respondent stated that it has been effective but has not achieved as much as it might have done yet, however, it has been effective in demonstrating that something is being done to address the issue (R11). Another participant called these efforts pathetic at best, arguing that some organisations use it to promote their services (R15) and another stated that it depends on "who you believe" (R16).

The partnership work is believed, however, to have been effective at raising the profile of identity crime, regardless of whether people are acting on the advice provided in these forums (R16). Another interviewee (R23) states that there are struggles to set up the mechanisms to get the information quickly to those participating in these partnerships. The fraudsters can change tack, can alter what they do so quickly, that by the time the industry gets itself geared up for it, they've moved on to something else. The partnership efforts would be effective if the responses to new threats were quicker (R23).

Retail

One participant believes that these collaborations work very well elaborating that It allows all sides to learn from each other (R6). Another argues that they have been effective but in

different ways such as having a wider audience to communicate messages to (R7). Another interviewee believes that the police to be effective in partnerships (R5).

5.13.17. What else needs to be done to tackle the issue

Several themes emerge from respondents in response to this question. Introducing biometric identification, improved government commitment and performance, better data on identity crime and its victims, preventing the shift of responsibility to consumers, better management by the credit industry, recognising that crime displacement is not a remedy and addressing poor commercial practices or adopting mitigation instead of defence are key topics.

One of the participants believes that the real solution will be some sort of biometric system of identification, one that does not rely on using static data but instead relies on live real time mechanisms to confirm the biometric data. This is, however, not completely free of vulnerability either (R15). On identity cards, opinions are divided on the value and expediency that a single identity card would offer in tackling this crime. There are those who believe that this will be an effective method in reducing and removing some of the existing vulnerabilities in this area, such as making it more difficult for people to change their names regularly with a national registration system in place (R7). On the other hand, there are those who argue that the use of a single document/method or device for identifying people would increase the value of that document to criminals and, therefore, increase the efforts to steal such a document or device to commit crime (R7). This group supports the idea of a multi-authorisation method as presenting a more secure technique to verify identities.

The role of the government is scrutinised as participants confirm the belief that the government needs to play its part in tackling this issue (R23), a statement that has been made by several interviewees. Addressing this issue is politically motivated by the government, an attitude that was evident with the establishment of the National Fraud Authority, which was purely to show that something was being done (R15). The government's strategy for dealing with fraud is not directed at the right aspect and is more focussed on what people think of fraud rather than tackling the issue itself. Complex identity fraud requires a very specialised approach to tackle it effectively and properly (R11). One participant stressed that data problems arise when governments (both past and present) divert parts of the public sector to the private in order to reduce public sector debt. An example is the utility organisations which used to be run by the public sector but are now run by private companies. An important issue within these organisations is the lack of protection of personal data (R14). Another emergent theme was to persuade the government that this is not a victimless crime. And although currently there is a lot happening, there is still a belief

that the government needs to be doing its part and needs to take this seriously (R19). Businesses criticise the government for not realising how much the business community are actually doing to address this issue (R17). The biggest element of this crime is the cyber side which the government is focusing on and this focus needs to be continued (R19). The same participant continues that the first thing should be the injection of some money by government into this area (R19).

Better information is a central theme for better identity crime prevention strategies. One of the major issues in this area is that the official statistics are unreliable, few offences are detected, reported and prosecuted (R14). The same issues exist with relation to information on victims. In some cases, the liability is not very clear and the collateral damage on victims is poorly understood (R14). To add to the problem, victims feel reluctant to admit it due to fear of their credibility being impacted in their community. And those victims who suffer from disability are impacted the worst by this fraud (R14).

Other contributing factors to improving efforts to tackle identity crime are recognised as reducing the carelessness of individuals which is compounded by complex contracts (consumers have to sign with private companies to access their services and products) which stop companies from being liable, as the consumers are not given enough time to read and understand the terms and conditions (R14). Others demand a holistic approach with one participant stating that this is an issue for the whole nation and argues that everyone needs to work on this collectively across all domains and it needs to be recognised that there is a big issue here that needs attention and work. A range of solutions are required in all different facets (R15). One participant takes that point further by arguing that this is everyone's responsibility not just the corporation's (R6). Everyone (the government, companies, individuals) needs to get out of the ostrich mentality and accept that this is an issue, and to get it into the public domain and start a debate around it. What needs to be done is a proper and structured approach to identify, sensible, pragmatic solutions and appropriate penalties in law and appropriate powers for the police (R15). Another respondent believes that we are on the right path but the first stage on this path is to recognise that this is a problem, the second stage is to have a 'descent' plan to tackle it, and the third is to have the intelligence to know what methodologies the criminals are adopting (R24). This issue needs a multifaceted approach, there needs to be an understanding of where work needs to be started and where it needs to be finished (R14).

The focus also fell on improvements required by the credit industry. The credit industry has been blamed for the problem, but they have actually been very proactive in terms of

recognising the growing organised crime element and putting in place measures to combat it. If it was not for these efforts, the problem would have been far worse (R6). There is a belief that ATM operators and card issuers are not doing as much as they ought to and are not identifying the point of compromise as quickly or as accurately as they should, because it is too complicated or too difficult, so they cannot be bothered with it. This is due to either lack of technological abilities or lack of human resources (R11).

The displacement of identity criminals was another area generating discussion. One of the respondents referred to a period of time, that due to employing a successful fraud prevention strategy within their respective organisation, the fraud figures decreased. However, they saw from industry data that the same amount of fraud had increased in the other organisations in the same sector. Although this issue is believed not to be one which produces a competitive advantage among companies, those that manage to do well in reducing their fraud figures don't feel compelled to share the techniques they used to achieve it with the others, so preferring to keep the upper hand (R15).

Many businesses do not take their data protection responsibility seriously and unless they are caught by the Information Commissioner's Office, they don't take it seriously (R7). It is believed that the industry cannot do much in this area and that they simply rely on the Information Commissioners Office to move this up their agenda. A lot of the businesses are aware of their responsibilities, but unless there is a force of law, they will not meet their responsibilities (R7). Some businesses are less prepared when it comes to strategic planning for things of this nature, taking the view that for the things that they don't understand or they can't deal with themselves, they will just take a position and mitigate against it financially (R26).

Enforcement

Feedback concerning law enforcement's approach to identity crime offered by respondents focussed on the fact that it is assigned a low priority, is critically underfunded, is approached at a local, regional level when the criminals are often national or international and that the void left by law enforcement is having to be filled by the private sector who feel overwhelmed at the task.

There were a number of issues that were identified with the policing of this crime. The first and principal weaknesses is that fraud is not one of the priorities for law enforcement. The policies are supposed to be set, increasingly, at a local level so the police seek local community feedback on what they think is the issue and pursue that and identity fraud will

certainly not be on that list (R11). So, all the while the forces of law enforcement are focused on local issues, the organised criminal groups committing identity related crimes are operating at national and international levels. The issue is far worse at provincial level since they simply do not take notice of this issue. This is something that the retail representatives are currently lobbying to rectify so that transparency is provided in terms of what the regional police forces do with the crime sent to them by the National Fraud Intelligence Bureau (R19). One of the respondents is currently lobbying for 43 police forces to show what they do with intelligence they receive for fraud (R19). One of the biggest issues is that the regional police forces do not have fraud as their priority (R19) as their priority is more set at local level (R11). The Metropolitan police is forming an anti-fraud team; with these activities there is a hope that the provincial forces would take notice of this crime (R19). The police also do not have set guidelines and a clear priority structure to pick cases and they seem to just pick the ones that look interesting to them to investigate (R11). Additionally, this fraud is being carried out by international crime groups, they are based in one area and commit their crimes in the other which makes it harder for the enforcement purposes and makes it difficult to nail down at a local level (R11). Respondents also acknowledged that with the police budget being cut, they will be doing less and less investigations and, therefore, there will be more civil prosecution, obtaining the proceeds of crime which will then fund more and more operations and investment in solutions (R17).

As a result, the retailers find increasingly that they need to deal with the issue themselves and they state that law enforcement agencies need to realise that retailers are doing more and more in tackling this issue (R19) a task which is hampered as liaison with the police and within the police is difficult. There is no involvement, and information sharing with businesses from the police is limited (R11). In addition, the police do not have the necessary resources to provide businesses with training on identifying forged or counterfeited documents. They are more focused on raising awareness as and when scams are in progress, but it takes time to gather enough evidence to form and devise awareness raising messages (R21). However, this could be short-sighted as the gap between the fraudsters and their latest MOs and the industry catching up with these needs to be shortened as they always seem to be ahead and by the time we catch up with them they have moved on to something else (R14).

Awareness raising and education on prevention

There is general agreement among interviewees that awareness-raising and identity crime prevention messages need to be increased, be more relevant and engaging and that the government must increase its work in this arena. The challenges remain the restrictions of

the lack of accurate and timely data, people's behavioural patterns and the speed of change of identity criminals' methods and targets.

One participant believes that this crime will grow and impact consumers even more, therefore, prevention messages need to be increased, accepting meanwhile that this could be quite challenging because as soon as an area is focused on, the fraudsters move to something else (R6). There is a more negative feedback from another respondent who argues that the difficulty is that you can educate people, but you cannot stop them from sharing their personal information freely (R16). However, on a more positive note another respondent believed that in 5 to 10 year's time there will be a more equal playing field because of more intelligence leading to loss prevention and businesses taking it more seriously (R19).

With respect to the available data, the different statistics that exist in this area are confusing consumers - but simple messages, highlighting to certain populations who are more at risk, would be useful, stating that because of their age range, their profile or the area they live in, they are more at risk of becoming a victim - but unfortunately, the co-operation of data enabling agencies to do that is not there and is not available (R12). Everyone needs to be made aware of the risks to their identities and to their data in general. It is argued that even those who work in this area and more aware of the risks get caught out (R6). A need for awareness exists about the data people can potentially share with fraudsters as they are living busy lives and ignoring things and saying that they will come back to it (R14).

The government departments involved in data and identity are perceived as not doing enough to lead, or even contribute to the efforts to prevent identity crime. There is a need for the Information Security Commission's office to start making people more aware of the risks involved in having personal data and to be more vocal about what they would do if people don't protect the data (R6).

And finally, the speed of change means there is a need to develop the ability to identify very quickly where new identity fraud techniques are breaking out so that messages can be formed and communicated to stop people falling victim to the new threats (R21). Prevention messages need to be stepped up which is challenging as every time you focus on one area something else comes up - an example is the social media sites, because a few years ago nobody could foresee how they could be utilised for fraudulent purposes (R21 & R23).

Data sharing and collaboration

Key themes from this question include the need for even more data sharing and collaboration, the fact that many identity criminals operate across industry sectors and that the public sector is not as effective as the private sector in sharing critical data (possibly hampered by privacy issues). There is an emphasis on more collaboration (R11& R17) and more professionalism (R17) by the participants. Every company should make efforts to engage in collaborative projects with other partners. The more data you have the more ability you have to bring different data sources together and the more you have a chance to catch a identity fraudsters (R21). Another interviewee stated that a proactive company would work on their own 50% and with others 50% (R24).

Furthermore, it is stated that quite often the same people who are involved in retail fraud are also involved in charity fraud and gaming fraud because they use the same credentials to commit different sorts of fraud (R19). It may not be exactly the same people but there will be links, because there will be a team of people who are using the same credentials to commit the fraud against different industries (R19).

It is crucial to acquire a better understanding of when data should be shared, by whom and why. There is division at the moment between the public and private sectors and while the private sector has been sharing data effectively for a long time, the public sector hasn't and there is not really a cross over. However, the same people who commit fraud against the private sector commit it against the public sector too, so sharing data would be very beneficial (R12). The public sector, however, may have issues and whilst agreeing that maximizing data sharing is vital, it may have conflicts with privacy and people's rights - but the more different and wider sources of data available the more effective it would be (R21).

Business community efforts

Major topics emerging from interviews include the need for greater professionalism and structure from private sector organisations, the internal struggle between commercial necessity and data security, the dilemmas of SMEs (small to medium sized enterprises) faced with identity crime, the vital role played by IT systems, the danger of publicly available personal data and the discrepancy between efforts applied to tackle identity crime and the actual results achieved.

One respondent (R17) calls for more professionalism and more professional and academically accredited staff in the identity crime arena. He observes that the cases that look the most interesting are picked off the shelf to be investigated instead of a structured

and evaluative method to determine which case to investigate or investigate first (R17). This extends to product and systems development teams as employees need to be aware when they are introducing new systems or new products or creating new databases that they will get attacked and targeted by fraudsters. More thought needs to be given to these, an example was the planning application database which went on-line and everyone could access it with all the data and signatures on it (R21). Another contribution outlines that the carelessness of the individuals within companies needs to be managed as their careless acts of poor vigilance or doing their job efficiently in protecting data, causes the individuals to fall victim to this crime and bear the liability for it (R14). In contrast, there is grudging respect from one respondent for the professionalism of identity criminals when he states that one of the major issues is that the fake documents produced by the organised gangs are so professionally done that distinguishing them is very difficult. Therefore, the challenge is identifying these fake documents and knowing what to look for. Advice and training need to be provided in this area (R14).

The conflict between commerciality and security is highlighted by the following contributions. Security campaigns needs to be given priority over others. At the moment, if there is a new campaign for a new mortgage or a new offer, the security leaflets are pushed out the way to make room for that (R23). Television “soaps” need to be utilised to send messages to the public even if it is just one line (R23). There is no harmony between the two parts of the business as the fraud team would push for more restrictions and the customer service team would push back, as this would impact customers. This needs to be balanced (R2).

Comments also focussed on the size of the enterprises and the varying issues they face. It is believed that most SMEs have not even given this area a thought which makes them more vulnerable. This is surprising as they actually have more risk of going completely bankrupt if a compromise happens to them (R24). One participant argues that, in their industry, the companies are not big enough to take action on their own and, therefore, shift the responsibility to the financial institutions and law enforcement agencies of providing the SMEs with advice on how best to deal with this issue, which is becoming more real and worse every day (R18). Equally, the fact that financial institutions are trying to cover up how serious identity crime is, is not helping other businesses, and it is not helping to deal effectively with this problem. (R18). Smaller retailers are also slow to adopt IT systems and processes which will offer some protection against becoming victims. One respondent points out that vulnerabilities still exist with the smaller size retailers. The card schemes prefer to work on a collaborative basis. So, if the retailer is applying some effort to protect its environment, then the schemes realise that they are on a journey towards compliance-

however, the smaller retailers are receiving penalties on a monthly basis from the acquirers in an effort to push them into starting their journey towards complying with Data Protection requirements or at least evidencing that they have started their journey (R6).

The value of robust IT systems and manual processes is also referenced, particularly in times change. Most retailers have anti-fraud teams within their financial services departments using various technologies and sometimes using outside agencies to screen the applications and transactions for suspicious ones, but still, in order to be certain they need to contact the customer and talk to them directly (R19). The payment systems infrastructure is huge and therefore, applying security measures is expensive and takes time. There is a hope that practitioners in the future try and be proactive and anticipate future threats rather than wait and react (R11). The other thing that hinders identity crime efforts is the change that a lot of businesses go through during mergers, acquisitions and alliances and that keeps their eye off the ball (R11).

Better management and control of publicly available personal data is another area highlighted for improvement. Awareness needs to be raised about what information is published on the public space because the fraudsters are very good at doing their research into the latest developments to stay ahead of the game. Therefore, publishing key personal data needs to be minimised and limited (R14). Even the Electoral Roll is cited. There are two parts to the Electoral Roll: the full Electoral Roll and the edited version. The edited version is used by the credit reference agencies for marketing and authentication. It was recommended that the edited version of the Electoral Roll be scrapped (R12). In addition, criminals overproduce false personal data. One participant argues that people manipulate their credit history and there are those who register 10 identities and build credit histories in order to abuse them later. There needs to be a balance between protecting people's privacy and more transparency needed for better protecting data as the Data Protection Act doesn't cover everything (R12).

Another minor theme which surface was corporate identity crime which one participant regards as underreported and less understood. There have been some attempts to educate small business owners on the severe impacts such victimisation can have on them, it can wipe out somebody's business (R21).

Finally, improvement is needed in implementing, at operational levels, the strategies agreed at senior management and trade association levels. Although a lot of activity is happening to tackle identity crime issues it seems that not much is being achieved. There are endless

conferences on these subjects, people have their meetings and have their forums and papers are being produced but nothing actually seems to be changing (R7).

5.13.18. Discussion

Several themes have emerged from the research amongst the private sector respondents. Most participants in the private sector perceived identity crime to present a significant threat. Despite this, there was a strong reluctance from some respondents to answer the questions. This reluctance was supported by the number of rejections received by the researcher for interview requests at the commencement of the study from the private sector. It was also evident from the responses that many businesses are still trying to brush this issue under the carpet using the excuse that if they talk about it their vulnerability will be exploited. This belief was also captured by Cashell et al, (2004: 13 cited in Wall, 2007:20) stating that "Corporate victims are particularly fearful that publicising corporate vulnerabilities might encourage attackers, damage the business and compound workforce concerns about their job security".

Much concern is directed towards consumers' perception of the risk. This has heavier weight than the financial loss experienced by businesses which is deemed relatively low compared to the organisation's total turnover and can, therefore, be tolerated. When people fall victim to this crime their perception of the risk increases and as more people become victims, and share their experiences by word of mouth and social media, the fear of identity crime increases disproportionally to the actual risk of becoming a victim.

In line with the private sector's perception of identity crime, respondents indicate that the priority given to this issue differs in various organisations, however, when a company suffers a data compromise, the issue is swiftly escalated to the highest executive level so that re-assurances can be given to customers and the media that defences have now been established to prevent recurrence and that any losses will be borne by the company. This reaction is evidence that the company fears the impact of the reputational damage leading to a loss of customers' confidence and their business more than the impact of the fraud itself and the impact on the clients who have been victimised. Some of the participants believe that identity crimes are a natural part of their business and cannot be fully eliminated. This view is supported by Durkheim who believes that:

> "To classify crime among the phenomena of normal sociology is not to say merely that it is an inevitable, although regrettable, phenomenon, due to the incorrigible wickedness of men; it is to affirm that it is a factor in public health, an integral part of

> all societies…crime would not thereby disappear; it would only change its form, for the very cause which would thus dry up the sources of criminality would immediately open up new ones." (Durkheim, 1938: 67)

Identity crime has different impacts on different types and sizes of private sector companies. There are differences of opinion amongst the participants in the private sector on which businesses are being impacted most. Some believe that the larger businesses are impacted more than the smaller ones. This could be due to the fact that the larger businesses are targeted more often, however, the impact is heavier and harder on smaller businesses (especially with data compromise) which frequently results in business closure or bankruptcy. It is, therefore, interesting to note from the practitioners questioned, that smaller retailers, who are more vulnerable to compromises, take data protection less seriously than their much larger counterparts.The larger businesses have the means to acquire security measures ahead of the smaller ones which often results in the crime being displaced to the latter thereby securing an advantage for the former for a period before the criminal fraternity retaliates with a new and improved MO. One common theme from participants is the major challenge that all organisations face in keeping up with the fraudsters; they seem to be always a step ahead of the fraud fighting community.

With respect to the treatment of identity crime in the private sector it is apparent from the feedback that there is still a broad lack of understanding and the issues inherent in defining and measuring it go hand in hand. This issue with definition was captured by White and Fisher (2008) in the literature review and it is clear that it has not been resolved. With the exception of the finance sector, the trade associations of other sectors which are heavily impacted by this crime (such as the telecoms and train operating companies) still have not developed rigorous methods to measure the amount of losses nor the systematic collaborative approach that the finance sector has to fighting identity related crimes. Interestingly, the data quoted by a couple of participants to indicate the amount of losses attributable to identity crime are many times higher than the ones that have been published. Is it that they have a better understanding of the true losses, ones that have not been reflected in the studies? For the non-finance sector, defining identity crime is not as pressing a priority as the day to day operational challenges of victim support (in terms of returning stolen funds and rectifying account take over) take precedence over academic and operational definitions and effective measurement. The majority of participants acknowledge that there is a core weakness here but often do not operate at the strategic levels within their organisations which have the power to resolve it. In addition, commercial necessity often

prevails over security measures with marketing campaigns taking precedence over security updates and messages.

As much as little effort has been applied to the definition and measurement of identity crime itself, equally little emphasis has been given to victims and offenders. Generally, there is a lack of knowledge about the victims of this crime, a theme that emerged from the literature review and the feedback from the public sector respondents. The organisations, operating in a strategic capacity, use data produced by the research companies that highlight the riskiest segments of society at which they direct their anti-fraud awareness campaigns, but the businesses do not make any efforts to develop a better understanding of their victims, the victims' behavior and the driving force behind the decisions they make that ultimately result in their victimisation. Even though some private entities are concerned with the plight of victims the general attitude is that the real victims are the businesses who suffer financial loss whist the victims are merely inconvenienced. This is not surprising considering the prevailing low morals in the financial world where the operators do not feel the pain of these consumers as they are too far removed from the effects of their actions (Ruggiero, 2017:2).

The lack of knowledge about victims of this crime is also reflected in the lack of knowledge of the offenders. No in-depth analysis of offenders has been commissioned by the private sector. There is a general feeling that the identification, correction and, if necessary, prosecution of offenders is the role of the state and the public sector and that it is the responsibility of the private sector to use all available practical techniques to protect their identity assets. What does concern the private sector, and which results in a feeling of powerlessness, is the involvement of some nation states in the cyber-attacks which disrupt the general business environment or their particular area of trade. Organised crime gangs operating nationally or internationally are also feared and begrudgingly respected as their strategies, professionalism, flexibility and speed of action compare extremely favorably to those of the anti-fraud practitioners in the private sector.

About identity crime detection, respondents offered a long list of techniques employed within private sector organisations (both human and technology systems-driven) to enhance crime detection rates. There are differences between businesses, some merely reporting it whilst others work to assist and persuade law enforcement to apprehend and arrest the culprits by contributing data, evidence and devising collaborative strategies to improve the success rate and achieve the objective. From my personal experience inside the industry, such activities were the result of the proactivity of the professional in charge of identity crimes in the

particular organisation and success is heavily influenced by that professional's approach, tenacity and attitude.

With regards to the identity theft protection strategies actually employed by the private sector, these can be broadly classed as based on practical situational crime prevention techniques (mainly those focused on increasing the efforts and increasing the risk). However, there is an acceptance among respondents that today, situational crime prevention techniques alone are insufficient to tackle identity crime. These have, therefore, been extensively expanded to include intelligence and data-sharing within their closed industry frameworks.

On the subject of what objectives are pursued by the respondents, and how these objectives are set and by whom, the answers vary. Within certain private sector organisations, their respective trade association plays a crucial role in managing and setting the objectives to tackle this issue collectively and individually. For these associations, it is mainly the data collected from members which drives the risk assessment processes and thereafter, the setting and prioritising of objectives. For those companies which do not rely solely on guidance from their trade association, there are clear differences between large businesses and small business in setting their objectives. Larger businesses, often with their own internal fraud teams, have statistically significant company specific data which they overlay on data provided from their trade association. Objectives are set at board level and strategies devised to meet them. Within smaller businesses the finance department is often responsible for making decisions on identity crime objectives and in some even smaller businesses, no objectives are set at all. With such diverse approaches to data collection, risk assessment and objective setting by companies in this sector, it begs the question of how effectively they can collaborate.

Throughout the responses collected, a central theme, not strictly associated with situational crime prevention but rather addressing the wider community of victims and potential victims, was the recognition of the need for better education and awareness-raising by both the public and private sector. A sentiment echoed by Ponter et al. (2008) and Cassim (2015). These issues have not yet been resolved and are ongoing, even though organisations of some respondents felt that this was not a priority or rather it was somebody else's responsibility. The most cited agency for developing and managing these initiatives was the relevant trade association and thereafter, the commercial collaborations established over time. All the private sector representatives work with substantial number of organisations in their partnership/ collaborative efforts. In terms of the context within which this collaborative

work takes place it is once again centred on raising awareness which is clearly at the top of both associations and the private organisations agendas. However, there are disagreements on the effectiveness of these collaborations with most respondents believing that they have not achieved as much as they should. It is mostly the retail industry that has found these collaborations to be effective. Is this perhaps because they have for some time been used to working in such partnerships as the Business Crime Reduction Partnerships which have, for a long time, been assisting in the implementation of effective counter measures for retailers to tackle shoplifting? As a result, retailers already have the mechanism and understanding of how an effective partnership ought to be run and the measures they can take to maximise its benefits. Despite the successes achieved in this sector, it was evident from my work experience within the finance sector that, despite the campaigns to educate and raise awareness about protecting consumer data (and any products which contain consumer data), businesses are still not doing enough to protect it. In some places, the messages that are shared among strategists and professionals at senior management levels (who are present at the meetings at which these issues are discussed) do not filter down completely or effectively to the front line identity fraud prevention teams, until, of course, a serious data compromise occurs.

In summary, from the perspective of private sector professionals, identity related crimes present significant threat and consumer's perception of this risk is an important factor for the operators in this sector. Issues with definition and measurement exists and little emphasis has been directed towards understanding the victims and offenders of identity crimes. As different organisations are impacted differently by this crime, they priortise it differently and therefore various amount of resources are employed to address it. Situational crime prevention techniques along with intelligence and data-sharing are utilised to tackle this issue. Partnerships are considered to be effective by only some of the participants, but better education and awareness-raising is a theme that most professionals agree upon.

6. Responding to the research aims and answering the research questions

This chapter brings together the findings of the last two chapters which examined identity related crimes from the perspectives of public and private organisations' personnel. Some of the major themes that arose, were the impact of this crime on all members of the society from individuals to large organisations and government and particularly the government's lack of commitment and ownership of this crime. Issues still remain with defining and measuring this crime and, with the exception of the finance sector, no other sector is effectively collecting and analysing data on this issue and a lack of knowledge about victims and offenders of this crime still prevails. Common prevention themes will be highlighted and the mixed response to partnerships' effectiveness will be examined. Finally, the chapter will catalogue participants' recommendations followed by a short proposal on future research.

As Garland (1990:30) states, criminal acts have major consequences in society. They violate "sentiments and emotions which are deeply ingrained in most members of society", shocking their healthy consciences causing psychological reactions, even among those members of society not directly involved. Identity related crimes are similar to other types of crime in that they also impact society. Identity crime offenders do not discriminate, they victimise people, old, young and even dead and then move on to governments and private companies, small and large. On individuals, the financial impact of this crime ranges from a few hundred pounds to thousands of pounds and often a person's entire life savings, and the emotional impact ranges from inconvenience to emotional trauma to the point that the victim commits suicide. One respondent believed that identity crime is more intrusive than burglary and is more personal. For organisations, however, reports indicate some are impacted severely, some experience reputational damage and some completely deny any impact at all. One of the participants articulated this point very well by stating that at one extreme this is not a problem and at the other extreme it is a massive problem and the truth is somewhere in the middle (R25). At the moment, the other crime type which is moving as fast, or even faster, than identity crime is cyber-crime, which is itself an enabler of identity crime.

The literature review highlighted the current understanding of this crime or the lack of it. It captured the challenges with defining this crime and the ways it can be committed. Criminological theories that can offer help in understanding offenders' motives were highlighted, victim's struggles were identified and finally, recommendations from the academic perspective were summarised. The literature review highlighted that most

rhetorical knowledge about this crime is generated by academia and that there are gaps in our understanding of this crime from the perspectives of the public and private frontline professional tackling this crime. The methodology chapter highlighted the research approach in collecting the necessary data to fill the gaps about this crime which is by way of face-to-face interviews generating qualitative data.

In the last two chapters primary (data from interviews) and secondary data (document analysis) enabled me to discuss identity crime from the perspective of the professionals from both public and private sectors. It was evident that identity crimes are proving challenging to both these sectors as well as the general public. Amongst the challenges is that the academic community is finding hard to explain it, law enforcement, government and the private sector are finding it hard to tackle it and the general public are struggling to keep their identifying information safe to prevent becoming victims to it. Additionally, several respondents pointed out the role of identity crime as an enabler of other, arguably more serious, crimes such as terrorism and human trafficking. Reference was made to the fact that most identity related crimes may each be minor in nature, but the large number of instances means structuring victim profiles and developing prevention strategies is complicated, and the overall effect on society is significant.

The government and commercial organisations are doing little to educate people about this crime and teaching how to reduce the chances of falling victim to it so that people's understanding increases, confidence grows and perceptions align more closely with actual data. The other issue is that at the moment there are different sources of data and information. The participants believe that it is very difficult to engage people's attention so that they listen to identity crime prevention messages when there are so many of them in the public domain. This also creates trust issues as people do not know which source to believe. A survey commissioned by Equifax on the UK perception of identity fraud in 2017 revealed that there is a lot more that can be done in terms of helping consumers protect their personal information online, 40% of people don't have antivirus programs on their computers, tablets or smart-phones and more fundamentally, there is a basic lack of understanding about the scope of identity fraud. It is, therefore, the responsibility of all those involved to protect themselves from becoming victims. Awareness is slowly growing, according to Equifax research. In a similar study conducted in Canada, 29% of consumers agreed with the statement "I hear a lot about identity theft, but I am not sure what it means" (cited in Archer et al. 2012:17).

It is evident from the statements made by the professionals in this area that no one body or organisation has an overall measure of the amount of identity crime being committed. Even current data is deemed to be insufficient and inaccurate due to the level of identity crime being conducted on the Dark Web. Throughout the responses to the questions, fraud practitioners constantly refer to the problems of defining and measuring this crime, the latter being dependent on the former. In the previous chapters, the particular argument between the government and the banking industry on whether to include card fraud as identity crime was examined. However, this is only a small part of a much wider issue centred on defining this crime. The definition that the Home Office (2008) provided was considered to be too broad. Their attempt to create a single definition has not worked because some of the fraud practitioners interviewed are still not aware of these definitions, some even have given up on working on a definition. Despite this response, the Home Office's broad definition for identity theft/fraud is accurate, but what the industry is finding difficult is defining 'identity'. Every organisation provides different products and services therefore, a single definition of an identity may not fit them all. The same business/government sectors may adhere to one definition, but this may not be accurate or appropriate across a number of different sectors. It is this failure to devise a commonly accepted definition which makes the standardisation and collective reporting of this crime impossible.

As stated in the previous chapters, Action Fraud has no identity crime category, therefore, no data can be collected for it and it has no visibility. The only sector that collects accurate information and publishes it on a regular basis is the finance sector. The model that is used there, could be copied by other sectors which could benefit from the experience and templates already developed. However, the feeling among participants was that achieving full compliance in their sector would currently be impossible as too many companies do not record, or do not share the data that they do record and even industry bodies seem unable to enforce this.

Respondents' feedback on victims indicated that identity crime produces more than one victim per crime event. Identity crime creates multiple victims with very diverse types of victimisation and different impacts on its victims. Organisations suffer financial and reputational damage and the individuals who are inconvenienced also often suffer emotional damage. In most instances, organisations, which in some cases through their negligence are facilitators of this crime, make little or no efforts to develop a better understanding of the victim's ordeal. Study data indicates that participants that have a more strategic role are more removed from the victim and, in fact, are happy to be so. It is not surprising then that once someone becomes a victim, the lack of support contributes to the fear of victimisation

becoming so much more than the real threat. This dilemma has been made worse by the lack of concrete information available about victims.

Study data also indicated that the fate of victims will likely continue to worsen as the banks have decided to become tougher on negligent consumers. It is true that some consumers are careless when using their identifying information and with the belief that the banks will reimburse them should they fall victim to this crime, they are not as vigilant as they should be. As fraudsters are becoming highly sophisticated, aided by the latest technology, and with the internet offering wide access to mass audiences who are less sophisticated, it is very hard to draw the line between someone who has been negligent and a real victim of crime. Therefore, although organisations are also victims as reputational damage causes loss of confidence which in turn results in financial loss, consumers seem to be the bigger losers with initial financial loss, credit score damage, emotional problems and the inconvenience of sorting out the problem.

Before victims can be effectively helped, they need to be acknowledged as victims. According to the United Nations Declaration of Basic principles of Justice for Victims of Crime and Abuse of Powers, victims are defined as:

'Victims' means persons who, individually or collectively, have suffered harm, including physical or mental injury, emotional suffering, economic loss or substantial impairment of their fundamental rights, through acts or omissions that are in violation of criminal laws operative within Member States, including those laws proscribing criminal abuse of power.

Despite this, several participants remain of the view that, as victims are generally reimbursed, thereby suffering no lasting financial loss, they are not, in fact, victims. Nineteen percent of participants believed that there is plenty of support for victims of identity crime. At the moment the credit reference agencies provide help to victims by contacting all the banks and lenders on the victim's behalf, Action Fraud would provide some counselling for those who are suffering from emotional problems and CIFAS provides protective registration. A distraught victim needs to contact all these agencies to start to deal with the issue. In addition, victims need help from commercial organisations (such as internet providers/satellite TV companies etc) whose services are acquired illegally by identity criminals. A single commercial body holding responsibility for facilitating this and providing a one-stop shop for victims would be ideal.

Feedback on identity crime detection reveals that seventy-eight percent of respondents take a proactive rather than reactive approach to detecting identity crime. Some of the

participants from the private sector did not answer the questions related to detection methods employed by their organisations, fearing the loss of competitive edge and the fact that disclosure may alert fraudsters to their current methods. In terms of proactive tactics, respondents agree that a single mechanism is not sufficient. A holistic approach encompassing technology and intelligence sharing is employed for effective detection. It is equally important to maintain the most up-to-date IT systems and that communications with partners remain constantly open to promote the sharing information for better detection.

The picture for investigating and prosecuting identity crimes is very revealing. Only 3% of detected crimes passed to the police are investigated. There was a significant lack of interest by most participants in knowing what happened to the detected crimes once reported to law enforcement agencies. This results in a wide range of approaches across organisations to reporting identity crime. At the moment, the main focus of organisations is to prevent identity crime and focus on repayment strategies to victims. This is not surprising considering the low investigation rate. Low investigation and even lower prosecution rates remove incentives for fraud practitioners to focus on reporting identity crime, preferring instead to concentrate on preventing it.

The UK's National Cyber Security Strategy's (2016- 2021) overall objectives are divided into three main areas: to defend data and systems and make them resilient to attacks, to deter, understand, investigate and disrupt hostile attacks against the UK and finally to develop an innovative growing cyber security industry which is underpinned by scientific research and development. The public sector respondents highlighted identifying fraud, prosecuting it, stopping it and learning from it as their major objectives which mostly run parallel to the UK Cyber Security strategy. Additionally, respondents' answers strongly indicated that identity crime is an enabler of other, more serious, crime types including terrorism. The 2018 CONTEST Strategy which shapes counter-terrorism policing strategy and tactics under the four 'Ps' work streams addresses this in its 'prevent' section on stopping people engaging in activities which could support terrorism.

This study has highlighted three strong common identity crime prevention themes amongst respondents' answers. The central strategy is education, awareness-raising campaigns and dealing with them. For both banking and retail sectors, 'insiders' (staff involved in committing identity crime) are a big issue, therefore, they both have strategies to deal with "insiders". Although other sector participants (such as insurance providers, hospitality and travel agencies) were not present in this study (due to a lack of willingness to take part) it would be unlikely that they would not suffer from the same issue. One positive development here is

that the banking and retail sectors, having identified and accepted the participation of individuals inside their organisations in identity crime related thefts, have common grounds and purpose in working together to eliminate it. A point of common agreement amongst respondents was that teams set up to tackle identity crime need to be multi-functional and consist of members drawn from various sectors (as each sector may be affected differently), so that all parties can be involved in the decision-making and developing solutions.

Directing prevention methods towards identity crime will be shaped by the risk perception of the organisations being impacted by it. Risk perception and judgment is a complex phenomenon and differs from one person to the other as Otway and Pahner (1980) analyse: "the perception of risks is a crucial factor in forming attitudes; obviously people respond to a threatening situation based upon what they perceive it to be." This perception differs from one society to the other and one person to the other. This assertion is supported by Douglas and Wildavsky (1982) who state that each individual or society creates their sets of criteria against which the risks will be interpreted and measured. These varied perceptions, which were also covered at the beginning of this study, may have a negative impact on the collaborative activities in this area.

Participants also highlight that identity crimes, at least on the current scale, are a relatively new crime type and it takes time for organisations to develop their safety cultures and for them to develop a system of commonly shared values (Toft and Reynolds,1994:26). It is also important for organisations to learn from the data compromises that they have suffered and share those learnings with the others. There seems to be uncertainty among respondents regarding which activities require focus to tackle the issue. "Should the focus of the activity be on enforcement type activity by the police, should it be about disrupting identity factories, prosecuting people, or actually should the focus be on stopping people using those documents, so verification services and how we deal with it... we don't know because we haven't got the complete picture yet" (R7). However, the identity fraud threat assessment currently being produced is designed to provide the focus for the industry to go forward, ensuring that the most significant concerns are prioritised, addressed and resourced. One respondent commented that since the terrorist attacks of 9/11 and 7/7, identity fraud in his organisation had developed a much higher profile and as a result, even though a large amount of work was being undertaken, some of it was not being communicated downwards due to the sensitivity of the information.

Partnerships were another theme emerging clearly from the respondents' answers. There are currently two partnership groups working specifically on identity related crimes: The

ACPO (Association of Chief Police Officers) Working Group on Identity Crime and the Identity Fraud Consumer Awareness Group (IFCAG).

In addition to the above partnerships, there are other sector-specific forums that are run by organisations in the areas of finance, retail, insurance and telecoms. These smaller forums have different scopes and remits and are focused on sector-specific aspects of identity crimes. However, most partnerships include law enforcement, public and private companies and different trade associations.

The basis of the current partnerships is information sharing about current threats, the methods used by public and private sectors to tackle the issue and also awareness-raising amongst consumers and small businesses. IFCAG, in addition to having a website to help raise awareness amongst the public and the small business community, developed leaflets and posters which were used in various places and by various organisations such as universities and Citizen Advice Bureaux in order to raise awareness and advise customers on ways that they can protect themselves. But even amongst fraud prevention practitioners, it is difficult to ascertain how effective this awareness-raising exercise has been. Monahan (2009), in his examination of the neoliberal governance and identity theft vulnerabilities, heavily criticises the law enforcement's response to this issue by "pushing the responsibility onto individuals". He states that although self-protection is very important "this approach neglects the political and economic forces and systemic vulnerabilities that may be contributing to identity theft in the first place." Negligence anywhere in the loop will cause compromise and, therefore, this must be a common, shared responsibility.

All organisations interviewed work in partnership with at least one other organisation. The one organisation that everyone works with is the police. Government organisations worked with the most other organisations (41), retailers were the next most co-operative (24) then banks and financial institutions (17) followed by law enforcement (8).

There were mainly two foci for the partnerships: strategic and operational. The common activities were data-sharing on intelligence and reports. The other areas in which collaborative work took place were raising awareness, prevention such as fraud screening and product development, discussing common problems and finally encouraging law enforcement to do more.

There are no data or statistics to evaluate the general effectiveness of these partnerships but there were three specific areas where changes that they championed proved effective. One was making deceased persons' data available to various organisations by the General

Register Office which was enabled through the changes made to the Serious Crime Act. The second was the lobbying which resulted in the temporary inclusion of identity fraud on the National Crime Survey. The third successful outcome of these partnerships was the provision and sharing of the top fifteen addresses used for identity fraud within each individual police force area.

Despite the above there was some scepticism highlighted by the mixed responses from all participants in terms of the effectiveness of these collaborations. The response from the banking sector ranged from “pathetic at best” through to “depends who you believe” to “they work very well.” These varied responses could be due to the different expectations that partners have from these collaborations.

Another theme emerging from the data was that “being seen to be doing something about it” seemed to be more important than “actually doing something about it” with the result that many of these partnerships ended up being regarded as no more than ‘talking shops’. One particular comment that resonated with disappointment and frustration was that the partnership approach resulted in a trade-off between knowledge acquisition and the speed of application of the knowledge to combat the crime, particularly as identity fraudsters were developing MO’s at a an accelerated rate. Equally, although respondents recognised that much had been achieved, it was still accepted that much was still left to be achieved. Retailers in the study believed that the two most effective activities have been data-sharing and education/raising awareness even though much of the public sector does not share data and some private sector participants also decline due to competitive issues. Additionally, the members of the partnerships have varying degrees of involvement, some relying on and using the data extensively in their identity crime prevention strategies and some broadly ignoring it. The extent of participant engagement and pro-activity within the forums was believed to depend on the nature of the business and potential risks. There is no effective mechanism to monitor/measure the degree of member’s participation, nor the value of the strategies implemented as a result of the partnership. Crawford (1997:236) supports this observation with reference to partnerships in general stating “Joint and negotiated decisions tie the parties into corporate policy and outcomes but fail to identify lines of responsibility. Institutional complexity further obscures who is accountable to whom and for what.”

This does not necessarily mean that partnerships are not working but instead it calls for robust measurement of the impact these collaborations are having which can sometimes be hindered by incompatible systems and definitions and conflicting objectives.

The journey from theory to practical implementation was considered by the participants of the study. It was generally felt that policy and strategy collaboration was easy. However, at the tactical and operational level it was difficult to implement strategies. Collaboration between government and the private sector on tackling identity crime is strained as the latter regards the former's initiatives as expensive and thus rejects them as commercially unworkable. On the other hand, businesses could do more to improve identity crime prevention strategies and defences but do not, preferring instead to accept identity crime as, currently, a small cost of doing business. Respondents also remarked that, at the international level, collaboration between governments and national law enforcement agencies is hindered by problems with definition, slow bureaucracy and the varied rank of delegates attending international committees. International forums need delegates with executive, decision-making powers but are often composed of individuals of lower, administrative rank which hinders progress.

Data sharing is the most common and enduring task on which partnerships focus but some collaborations are also temporary/event driven or driven by specific MO's. The private sector, particularly smaller organisations, approaches data-sharing on a cost-benefit basis. If no benefit is expected, then no resources will be spent on it. However, study data indicated the dangers of excluding them from industry collaborations as, currently, they are introspective and insular and as such are at risk, and the impact of victimisation can be quite severe on them. Larger private sector companies take a more open view and share data, and advertise that they do, as responsible companies. It is good for their reputation and in proving they are proactive in the fight against identity crime and, more cynically, as a defence against possible negligence claims in the event of a breach.

There seems to be two types of partnerships 1) those who need to communicate to solve a specific problem 2) passive data-sharing. The first one mimics how organised gangs work but the second one, data-sharing, is ongoing and constant. This enables the channels of communication to remain open making it easier to work on other issues together as the partnership members do not have to create things from scratch.

Respondents commented on the structure of partnerships, in particular, the questions of responsibility and accountability. The process of decision-making needs to be clear along with the process of financial management, acknowledging that partnerships are complex entities and therefore not free of challenges in these areas. In partnerships, conflict is a very natural ingredient but what defines a successful partnership is the management of that

conflict through re-negotiation, compromise for the collective good, understanding and communication.

6.1. Participants' recommendations

Many recommendations were made by participants in tackling the problem of identity crime. These could provide the basis of an agenda that could be used on a national level in an effort to improve the response to this ever-growing concern/issue. The most important point arising from this research was the need for one national body to champion the fight against identity crime. All respondents have an interest in identity crime but it's nobody's number one priority. The government needs to show commitment to a long-term strategy and resources and create a central department to own and champion the fight against identity crime. The NFA was established to provide leadership and direction in tackling all facets of identity crime but it was dissolved. There is a need for a government body to fill this void but one with regulatory powers so that organisations will be held accountable if they do not participate or do not deliver. The government needs to understand identity crime is not victimless. Fraud, and identity crime in particular, need to be higher up the priority list of law enforcement at national and local level. Identity crime must feature in the high-level national strategic plan in order to receive attention and support at local level. A further recommendation focussed on the need to look outside national borders as identity crime, enabled by cyber-crime, is transnational, the response is national and law enforcement is helpless until there is a global organisation charged with prevention which enables country law enforcement agencies to act across borders (which even Interpol is unable to achieve without close co-operation between national police forces). At all levels, identity crime needs to be recognised, a plan developed to address it, intelligence established to keep up with criminal MO's and adequate resources allocated to prevent it.

The private sector also needs to do more to lobby government and law enforcement to allocate resources to fight identity crime because it is an enabler of other serious crimes like drugs, terrorism, people trafficking etc. A more professional approach from non-governmental organisations is also needed in fighting identity crime, including the creation of a professional body (like the Institute of Directors), more criminology graduates, more structured approaches to strategic and operational crime prevention/ mitigation plans, better training of frontline staff to recognise identity crime and better co-operation between industry and local police forces.

There needs to be an approach of collective responsibility across government, business and individuals to publicise the issue of identity crime, stimulate debate, and develop a structured approach with pragmatic solutions, timelines and funds as well as better empowerment of law enforcement and courts. In the same way that recommendations call for a single organisation taking the responsibility in this area there is a recommendation for the creation of one document to verify identity which is purpose built for the job, not a mixture of passport, utility bill and driving license.

Cyber-crime is becoming increasingly a platform that is enabling identity related crimes. In fact, Goodman (2015:105) has gone so far as to say that it 'revolutionises' this crime. Identity crime is not something new, it has always existed, but the internet has just taken it to a completely new level. This is not surprising as surveillance, collecting and selling data from users' browsing and transaction habits is the business model of most of the large companies which dominate the internet (Google, Facebook, Twitter, Yahoo etc). In 2012, the Wall Street Journal published an article stating that one of the fastest-growing businesses today is spying on Internet users. In the report, fifty of the most popular web sites were highlighted and it was discovered that on average each left more than 64 cookie tracking files for their advertisers to trace people's online activities (Laney 2012). Therefore, more research is needed into cyber-crime, how fraudsters use it and how to better protect identities. Forcing these companies and social media platforms to be responsible with client data and to assist with educating their users on the dangers of it is another step that needs to be taken. However, even these major companies are vulnerable to data compromise, for example, Facebook's security department admitted that over 600,000 accounts are compromised every day (Goodman, 2015:132). And even more worryingly, in 2013, the data broker Experian mistakenly sold the personal data of nearly two-thirds of all Americans to an organised crime group in Vietnam (ibid:135) and they only found out about the compromise when the US Secret Service discovered the information for sale on the hacker websites and contacted Experian. To make matters worse the companies that make anti-virus program have been targeted by hacks and successfully infiltrated. Symantec, the maker of the Norton anti-virus suite of programmes, had 1.27 gigabytes of its security software source code stolen and cash demands were made in exchange for it not being posted on the well-known hacker website PrivateBay (Goodman, 2015). In September 2018 British Airways admitted to suffering a data breach which involved the theft of over 400,000 customer names, addresses and complete transaction history of the data subjects over a two-week period. Most recently, in March 2020, Virgin Media suffered a breach losing 900,000 complete customer records. Not having a social media profile is not a safety option either as it was proven in the case of

Ron Noble. He did not have any social media accounts, yet an organised gang created a Facebook page in his name stealing data from an Interpol website (ibid).

So far, the identity criminals are only stealing and using attributed personal information, they have not yet moved on to targeting biological data - but this is only a matter of time. As soon as companies and institutions begin to insist their customers use biometrics to access goods and services, the identity criminals will begin to steal biometric data by system infiltration. One of the recommendations that has been made was the wider use of biometrics, but this generates concerns about the personal and physical safety of the victim (such as having a finger chopped off to access fingerprint-protected data).

Respondents highlighted a number of issues with regards to law enforcement and its involvement with this crime. There is no specific offence of identity crime. There is disagreement among respondents as to the effectiveness of the Fraud Act of 2006 in identifying and prosecuting identity crime. There is a general agreement that current laws are not enforced properly or fully, and the current legislation has gaps, but there is no government desire or urgency to plug these. Primarily, law enforcement agencies need to be made to disclose their efforts, or lack thereof, in tackling this crime. They also need more government resources/funds to tackle this as most police forces have insufficient computer resources for their identity crime forensics teams. Law enforcement agencies are conflicted between the duty to reduce crime and the duty to reduce crime figures, which are entirely not the same objective, and identity crime needs to be recorded as such, not classified elsewhere. Because of this lack of action and interest from law enforcement, retailers routinely refuse to report identity crime which is unhelpful in gaining a true picture of the size and nature of the crime. Enforcement of existing laws (by the ICO) is needed to shock companies into taking data protection and identity crime seriously. Penalties should be introduced for those organisations which do not comply with the law and better support is required in this area for SME's who, alone, often lack the resources to combat identity crime.

Another core recommendation concerns the education of the general public, especially vulnerable groups (students, pensioners, mental health patients) on how to avoid scams, phishing etc. which should be sponsored by the ICO. Education is needed on the scale and cross-demographic nature of identity crime so individuals, businesses, organisations and associations can be made aware of its dangers and be able to discuss it without fear of losing reputation/credibility. One very interesting recommendation was made by a respondent who suggested incorporating identity crime into storylines of TV soaps and dramas to really boost awareness (R23).

Fraudsters constantly develop new and creative methods to defraud consumers. Respondents agree that identity crime prevention professionals, faced with crimes that have been committed as a result of employing new technologies, suffer badly from a lack of accurate data and statistics. This is a problem common to both identity crime and cyber-crime. This is supported by Wall (2011:20) arguing that low levels of reporting, leading to low levels of police action and fewer prosecutions and fewer statistics, reducing the amount of available knowledge about offenders which then ultimately hampers the development of criminology of this type offenders.

When a new trend is spotted it takes a while for it to be communicated to the wider public so that they can be aware of it and therefore not to fall victim to it. A recommendation was supported for the development of specific communication routes within government and industry so that these trends can be communicated to the public faster and more effectively. To aid prevention, the various criminal groups, working together to commit each stage of the crime, need to be identified. Whether the group is designing it, making it, selling it, using it, selling data proceeds or committing fraud using fake identities, each stage needs investigation. This is made more difficult because identity criminals rarely meet physically, preferring instead to communicate using the black web. More effort is required by identity crime prevention professionals to penetrate the black web to trap fraudsters in their own environment. IT systems designers and companies developing and running computerised systems carrying identity evidence need to consider safeguards at the time of development of the system rather than later as an afterthought. Rigorous and regular testing needs to be carried out to prevent illegal access. A further recommendation concerned the regulation, by law, of the sale of certain ‘professional/forensic’ printers which can produce fake documents which are impossible to spot with the naked eye.

One of the major vulnerabilities highlighted by one of the participants is changing names. People in the UK can very easily change their name and they can do it as often as they wish. “We know of people in the UK who change their names 12 times in a year. If you are changing your name 12 times in a year it is very difficult to think of a reason why you would do that unless you are doing it for criminal purposes, but that person is quite within their rights to change their name however often they want” (R9). Although this has been highlighted as a vulnerability, there are no plans at the moment in the UK to change this right, despite the fact that the name change confuses the system and puts willing fraudsters always a step ahead of the law enforcement agencies.

The World Economic Forum dubbed da ta “the new oil” but where oil is protected by fences, cameras, guns etc millions of data such as identity related information are stored by large companies unprotected (Goodman, 2015:78). A study conducted by the Ponemon Institute (2009) revealed that some marketing managers are prepared to give out key private customer data such as sexual orientation (7%), political affiliation (14%) and credit card details (19%) to third parties in an attempt to increase sales. The study also found that almost two-thirds of the marketing professionals it surveyed admitted consumer information had been lost or stolen over the past two years. This situation needs addressing by law enforcement. The availability of personal data on the Electoral Roll needs reviewing to reduce use by criminals.

Identity crimes agenda

The above data can be used to formulate an agenda for the future. Reducing, mitigating and preventing identity crime requires a multi-layered, multi-dimensional approach which can be summarised into ten distinct areas. However, each area has points of interdependency and overlap with others. In addition, whilst identity crimes may be global, national or local, identity crime education and prevention are local.

Better intelligence sharing: Intelligence and data-sharing already plays a very important role in tackling identity related crime. Identifying data sources and stakeholders who hold the data is the first step. It is imperative to improve intelligence capability as well as the capability to analyse data. These data play an important role in assisting the decision makers to make informed and fully supported decisions. Establishing an intelligence sharing model/protocol is a current and basic need. The model should clearly define the data-sharing responsibilities of each stakeholder, what specific data they will be sharing, in what time frame the data will be shared, facilitating the flow of information and establishing an effective exchange mechanism. These are all critical to identifying opportunities to enhance and expand data-sharing and revise policy and processes to ensure timely reporting and sharing.

Better measurement: After the NFA’s closure, no report was produced on identity crime as a whole. Action Fraud records crime but since they do not have an identity crime category and since identity crime has many facets it is easily reported under other, existing categories. As a result, it is impossible to arrive at a total for the instances of and losses related to this crime type. Additionally, company related identity crime is considered to be a major gap as there is a lack of understanding about the extent of this problem and it’s associated losses. Respondents believe that many companies, by chance or design, fail to report it. Therefore, efforts need to be made to change this attitude and practice.

Enforcement: It is evident from the above that enforcing this crime is a major issue. The police response, or more appropriately, lack of response mirrors that of the government, but this needs to change. If there are to be successes in dealing with identity crime, law enforcement needs to play a bigger part. If funding is the central problem, perhaps some compromise can be made similar to the financial sector financially supporting the Dedicated Card and Payment Crime Unit whereby all the organisations impacted by this crime make a contribution to the cost of enforcing the law.

Consumers' involvement with regulatory issues related to identity: identity crime has a major impact on its consumer victims, yet victims are rarely consulted when decisions are made about this problem. This needs to be changed and consumers should be included on various working groups that deal with this problem. Using the previous analogy, if not consumers themselves, then a body or institution representing consumers (such as the Citizens Advice Bureaux) should be formed and consulted.

Data protection: Data protection needs to play a more prominent role in every industry. This will be achieved by identifying and developing means to protect data, lobbying for organisations to establish a data loss policy which includes swift reporting of such data breaches and considering the issue of compensation to consumers when data is compromised and ways that those affected can be protected adequately. Robust fines for delinquent companies should be introduced and enforced.

Actions on internal fraud: Simply providing training is not enough. Refresher courses should be carried out throughout the course of the employment of the staff to remind them of the importance of this area and the penalties for assisting in the commission of this crime. Examination of the most common instances of staff wrong-doing is required in order to direct and focus strategic response and prevention. In terms of industry best practices, if one company employs an effective crime prevention method it should champion the method or the idea to help others to adopt it. This will reduce the ability of fraudsters to simply shift their focus from one company in the sector to another company which is missing the latest protection methodology.

Cyber-strategy: As discussed earlier, cyber-space has become a place where identity theft and fraud can be easily perpetrated. Therefore, a powerful and effective strategy is needed in dealing with identity crime issues. Such a strategy should develop and execute customer education programmes based on targeting those being targeted by the criminals. It should include data on the implementation of improved controls on passwords and password resets,

increased usage of one-time passwords, aggressive law enforcement and the long term funding of an e-crime capability.

Mobile services: There needs to be customer awareness and education on mobile vulnerabilities and ways that consumers can protect themselves. Additionally, there are no clear lines of responsibility and liability in the mobile networks. Engagement with the industry is needed to define roles and responsibilities. The best way to approach such a strategy is by engaging with the respective mobile network providers.

Crime prevention and aftercare: respondents agree that no matter how diligently businesses and government attempt to protect data in their care, identity fraudsters have unlimited time and sufficient technical resources to exploit loopholes in established systems. Therefore, a focus on aftercare for victims is a necessary component in any sophisticated identity crime prevention policy. In the majority of cases, gross customer negligence being an exception, customers of banks and commercial organisations are generally refunded for losses related to identity crime. However, there still remains a percentage which are not protected or reimbursed. In either case, the inconvenience caused by this fraud to the victim and the emotional turmoil experienced through the intricate processes required to clear their names and restore their credit rating far exceeds the initial financial loss. Therefore, an effective victim support system should go far beyond just reimbursement, it must include immediate reimbursement of the money from a fund already set-up to accomplish this. In some cases of identity related crime, victims are left with no access to money to pay for their most basic needs. Currently, it takes at least 7 days for the banks to complete the correct procedures to confirm that a crime has been committed and to recompense the victim.

Suffering identity crime can, in some cases, be a very daunting experience. Sometimes the victims do not know how and by whom their data has been stolen. This feeling of violation, vulnerability and uncertainty is very unsettling and should be treated with care by the victim support teams. If the fraud team has any information on how the fraud has happened, it should be shared with the victim. If not, the victim needs to be reassured that the necessary steps will be taken by the respective organisation to minimise the impact on them. The next step should be to explain clearly what the processes and procedures are that the victim needs to carry out in order to clear their name.

Aftercare: the bank/organisation needs to ensure that a specific department is set up to look after the victim and, if possible, to allocate a single point of contact for each victim. The worst thing that can happen is to ping-pong the victim between various organisations.

Futurology (Horizon scanning)/fraud forecasting: There have been a number of attempts by the banking industry to address the upcoming or anticipated events that may have a major impact on the threats and the level of fraud in the UK. They have attempted to utilise 3 levels of forecasting in their scanning for future threats: short term (up to 18 months), medium term (1.5 to 3 years) and finally, long term (up to 5 years). The ambition behind such efforts is to be aware of forthcoming changes/events and to predict what impact they may have on threats and fraud. Additionally, the objective is to establish early signs and indicators of emerging MO's or frauds and to have proper prevention methods in place so that, with the slightest indication of fraud taking place, prevention routines can be set in motion. It is extremely difficult to foresee what criminals will do or focus on but by building scenarios based on a correlation between previous or current criminal activities and the existing vulnerabilities and a correlation between vulnerabilities and threats, a better understanding of future issues may be developed. This is a very proactive approach in dealing with identity fraud problems and issues. Any such activities need to be intelligence based and analytical with impact assessments, adequate resources and a time scale. The expertise exists, especially with the Horizon Scanning Centre, which also provides training for organisations who intend to put such measures in place. Some of the key themes that can be explored in this area are technical, regulatory, economic, political, social, environmental, demographic, intelligence and industry/academia collaboration.

Technical addresses such areas as mobile technology, contactless or any other card and ATM related changes or developments; regulatory focusses on the introduction of new rules by the government or the EU such as the Single European Payment Area (SEPA) which may have an impact on identity crime as it will make Euro payments faster between European banks. Since the UK is not part of the Euro it could make the UK less desirable to fraudsters wishing to cash out or launder money. Economic should address recession and the phases of emerging from recession, businesses under pressure to expand and therefore, there may be less robust risk management processes adopted by firms. Global trade is shifting to China which provides potential for fraudsters targeting the West from there. The political aspects centre on the breaking apart of 'super banks', terrorism and cross-border strategies. Social (events) including international sports and major public holidays and the attendant opportunities for identity criminals. Similarly, environmental events such as natural disasters where fraudsters set up fake charities in order to steal people's card and identity data and demographics which are concerned with changes in society and changes in business practices such as cloud computing. To support the use of such techniques South (1998a) argues that criminologists should engage in 'futurology' by exploring the potential

damage of crimes and injuries generated by the manipulation of environmental resources and human and animal populations by corporate interests and governments in pursuit of 'expedient solutions', greed and profits (South,1998a:226). Intelligence should focus on monitoring online criminal activity and chat rooms and monitoring known criminals to develop insights into the thinking of other criminals and gangs. And finally, collaboration between industry and academia needs to be nurtured. At the moment there is a gap between the two with academia criticising the private sector and the private sector not trusting academia. If a bridge can be built between the two, both would benefit as academia would have all the data that businesses hold in relation to this crime, and businesses will benefit from the theoretical knowledge and 'futurology' discoveries that the academics will create.

6.2. Further research agenda

One key purpose for me to undertake this research project was to employ my unique position (as a former finance sector professional and current academic) to explore a topic, that is at a comparatively young stage of its evolution, is growing as a result of increased technological development and significant social and behavioural changes which has had little academic attention, in order to uncover knowledge gaps and to highlight where carefully considered further research could be applied, in such a way that it is able to make a significant contribution to key areas which promote a better understanding of identity crime.

Whilst it is true that the application of rigorous academic analysis and evaluation may not be possible for those following in the footsteps of this study in many areas in this study, there still exist several broad, and yet central topics, which would benefit from academic input. As stated earlier most of the focus of front-line practitioners is on the situational responses to this crime (and even then, not the full range of situational crime prevention techniques) but the root cause analysis of offenders is passing largely unnoticed. Larger scale examination of offender behaviour and disposition has the potential to inform widespread decision-making processes in better devising a more comprehensive set of situational crime prevention techniques. A key observation and common lament from respondents is that the identity crime fighting community is still a reactive community, wherein there exists a time lag in responding to areas that criminals identify as weaknesses and thus target. Developing a better understanding of the fraudsters' patterns may perhaps enable the identity crime fighters to move towards a proactive rather than totally re-active position.

Another theme that is accessible to academia, and that would reward investigation, is the plight of the victims of this crime. This study confirms that there is very little data available on who the victims are, their demographic profiles, their decision-making processes, the degree

to which their actions are the cause of their victimisation and the financial, emotional and behavioural impact that their victimisation exerts on them. A broader and deeper understanding of these victims would enable researchers and identity crime prevention professionals to better assist victims with their ordeal and to better inform and direct the necessary educational and awareness raising strategies and campaigns so that they may be built upon platforms that are shaped from real experience and knowledge.

Data-sharing has emerged as a major contributor to effective identity crime prevention in the 21st century. It is regarded by practitioners as an extension of situational crime prevention strategies and yet very little in-depth study has been undertaken on this prominent crime prevention strategy/technique. Using academic research to develop a better understanding of this phenomenon, culturally, practically, commercially, politically and academically will help to improve it and make it more effective. Study agendas should focus on examining the channels currently used to collect and distribute data, the kind of data shared, its homogeneity or lack thereof and the speed (and roadblocks) in its dissemination.

Transnational identity crime is an area severely lacking in good quality, reliable data and understanding. It may be that, because of the inherent challenges regarding access to reliable information, it is almost impossible to conduct research on this topic but nevertheless some efforts could be made to gauge the possibility of undertaking research on these cross-border criminal entities.

Finally, one respondent stated that some parts of partnerships work better than others. Studies can be undertaken to examine the methodologies used within and between partnerships and multi-agency collaborations to establish best and poor practises so that this can be used to accelerate the effective fight against the growing identity crime fraternity.

7. Conclusion

The aim of this research was to provide both academia and the professional community involved in tackling this issue, with a better understanding of identity crime in the UK from the perspective of the public and private sector. Although this is a crime type that is heavily impacted by international influences, and combating it effectively requires a certain degree of international co-operation, it is evident that the first step in the journey to tackle identity crimes is to develop a better understanding of it. It is not a linear, a straight forward nor even a continuously progressive one but rather it is a crime that is becoming a global problem (Smith, 2010), one that is influenced by a variety of factors such as the speed of development of new technology, rapidly changing consumer behaviour and national and international political agendas.

From an academic point of view, it was encouraging to see evidence of the extensive use of criminological theories (situational crime prevention) by the fraud practitioners in the study. This highlights the valuable contribution that academia and theory can make in fighting identity crime on the front-line. Academia's role in this endeavour is crucial as the theoretical knowledge and research expertise resident here can assist in developing understanding of areas where rigour, informed knowledge and a solid theoretical framework is absent. Explaining identity crime by using criminological theories alone is just as complex as the practicalities of preventing and combatting it. Both approaches require the development and application of a range of theories/methods to understand and tackle this problem and future research should focus on studying such integrated approaches. As the research revealed, co-operation and partnership can be effective to some degree and therefore, co-operation between academia and the non-academic world should be encouraged to continue to develop defences against identity crime. However, despite the prevalence of this crime, and the gaps in understanding of several of its facets, there seems to be a lack of interest on the part of academia to examine it. This could be due to the fact that obtaining data for research on this matter is extremely difficult as the business community fears the criticism that academia may direct towards them. The public sector refuses to talk about it to researchers due to confidentiality and the private sector is terrified of admitting this issue exists, let alone assisting in researching it in a constructive manner.

What has emerged from the research is that, whilst identity crime continues to gather pace, as evidenced by Wall (2013a) who emphasises "the resilience of identity crimes and their likely evolution", the efforts of those agencies seeking to prevent it are struggling to make progress. At the heart of the problem is the lack of ownership of this crime by the

government, and businesses being more concerned about their bottom line. It needs to be recognised as a crime in its own right and not for its component parts, so that local, national and international co-operations can begin to accurately measure, forecast, communicate, mitigate and prevent it. As Evans (2011: 184) states when the problem of crime cannot be fully eradicated, or the political will to 'solve it' is not present, then the only way left is to manage it, which is the current status quo with identity related crimes.

Another key research finding highlighted that the government also needs to acknowledge that identity crime creates disruption, financial loss and emotional turmoil and is an enabler of far more serious crimes including terrorism and human trafficking. Therefore, to combat this, the government needs to take the lead in establishing an organisation whose sole task is to combat identity crime, which is clearly directed, adequately funded (not just for a short period), appropriately empowered and staffed with identity crime prevention professionals, and one that is not influenced by politics. Similarly, the research indicates that the private sector needs a professional institute to draw together the various industries across the wide commercial spectrum, as well as to provide much needed support to the SME community which is, arguably, the most vulnerable and is struggling with a lack of knowledge and resources to defend against identity crime. Both these government and private sector institutes require executive powers to force compliance so that progress can be made in understanding, measuring, defending against and prosecuting this crime. Furthermore, both public and private sectors need to be compelled to report cases of identity crime and law enforcement agencies need to use current and future powers and resources granted to them to vigorously prosecute it.

The world is becoming increasingly information reliant to the point that some argue that Google knows people better than they know themselves, and that this technological giant never forgets nor deletes (Goodman, 2015:78).Therefore, it is becoming increasingly important for the whole of society (government public and private sectors and individuals) to protect itself. The government must cease ignoring this issue, cease trying to pass responsibility for it to the private sector and they in turn must cease their efforts to pass it on to the individual who is, arguably, the most vulnerable and least equipped to deal with it.

Another theme emerging from the study was that, notwithstanding concerns on civil liberties, and personal safety, there is a pressing need for one custom-designed document to establish a person's identity which should contain biometric data. Currently, this is politically unacceptable in the UK, but since the Identity Cards Act, 2006 was repealed, little effort has been made to establish a compromise solution which addresses the needs of the identity

crime-fighting community whilst avoiding the pitfalls of the National Identity Register and of the compulsion to carry.

Central to the research findings was the importance of information-sharing (notwithstanding the difficulties created by incompatible definitions) at all levels, local national and international as well as awareness-raising across all sections of society (particularly the most vulnerable demographics). This needs commitment from the government and both the public and private sectors so that individuals are more able to protect themselves and less likely to become victims to identity crime.

The attitudes of respondents towards victims also emerged as a key theme from the study. Financial institutions have attempted to provide support for victims, but the process is still tortuous involving multiple organisations before reimbursement of losses and restoration of financial reputation can be accomplished. A simpler solution for victims should be one of the main foci of the government body charged with identity crime management and prevention. Additionally, whilst the financial institutions of the private sector currently accept the majority of the monetary losses incurred by individuals and businesses, there is a trend for them to seek to claim negligence on the part of the victim as a means to reject reimbursement

Findings both support and criticise the role of law enforcement agencies in the fight against identity crime. Once it has been firmly established as a crime in its own right, rather than a combination of other crime elements, law enforcement agencies need a more proactive strategy to identify, apprehend, prosecute and convict identity criminals. To achieve this, they need government support and funding, specialist identity crime fighting personnel and clear government direction on priorities at national and local level. A focus on actually reducing identity crime, rather than using analytical re-definitions to produce crime figures which appear to show it has been reduced, is long overdue. A review of existing laws which impinge negatively on combating identity crime needs to be carried out in order to close loopholes and improve defences. Furthermore, law enforcement agencies need to police and apply penalties to institutions, both private and public, for non-compliance with data protection legislation.

The role of cyber-crime was omnipresent in research findings as an enabler of sophisticated identity crime, often carried out by organised crime gangs, which is made more difficult by the transnational nature of the internet and the complexity of policing it across multiple borders and legislatures.

Finally, feedback on partnerships indicated that, although there remain certain limitations, partnerships, at local, national and international levels, played a valuable role in combating identity crime by improved communication and sharing of latest threats and best practices.

8. Bibliography/ Reference

Abubakar, A, Bagheri Zadeh, P., Janicke, H. and Howley, R. (2016) *Root Cause Analysis (RCA) As A Preliminary Tool Into The Investigation of Identity Theft,* Cybersecurity and Protection of Digital Services, International Conference.

Ackroyd, S. and Hughes,J. (1983) *Data Collection in Context*, London: longman.

Action Fraud, (2018) https://www.actionfraud.police.uk/ (Accessed:5th July 2018)

Allison, S.F.H., Schuch, A.M. and Lersch, K.M. (2005) Exploring the crime of identity theft: Prevalence, clearance rates, and victim/offender characteristics*, Journal of Criminal Justice*, Volume 33 :19-29.

All Parliamentary Group Report Into Identity Fraud (2007) available at: http://www.fhcreative.co.uk/idfraud/downloads/APPG_Identity_Fraud_Report (Accessed: 27th March 2008).

Anderson, R. (2013) *Risk and Privacy Implications of Consumer Payment Innovation in the Connected Age*, https://www.kansascityfed.org/publicat/pscp/2012/Anderson_final.pdf (Accessed: 2nd June, 2018)

Archer,N., Sproule, S., Yuan, Y., Guo, K. and Xiang, J. (2012) *Identity Theft and Fraud: Evaluating and Managing Risk*, University of Ottawa Press: Ottawa.

Benson, M. L. and Simpson, S.S.(2015) *Understanding white-collar crime: an opportunity perspective*,Routledge: New York.

Berg, S. (2008) Preventing Identity Theft through Information Technology, *Crime Prevention Studies,* Volume 23: 151-167.

Bishop, J. (2018) 380,000 passengers affected by malicious British Airways hack, https://www.forbes.com/sites/bishopjordan/2018/09/09/british-airways-hacked/#65994dd367ae (Accessed:11th September 2018).

Blaxter, L., Hughes, C. and Tight, M. (2002) *How to research,* 2nd edition, Buckingham: Open University Press.

Blumstein, A, Cohen, J., Roth, J.A. and Visher, C.A. (1986) *Criminal careers and "career criminals*", Volume 2. Panel on Research on Career Criminals, Committee on Research on Law Enforcement and the Administration of Justice, Commission on Behavioral and Social Sciences and Education, National Research Council. Washington, DC: National Academy Press.

Braithwaite, J. and Geis, G. (1982) On Theory and Action for Corporate Crime Control, *Crime and Delinquency* Volume 28: 292-314.

Broadie, C. (2016) Tesco bank hacked, https://www.moneysavingexpert.com/news/2016/11/tesco-bank-vows-to-refund-customers-affected-by-hack---check-if-your-current-accounts-been-compromised/ (Accessed:3rd September 2018)

Burke, R.H. (2006) *An introduction to criminological theory*, Cullompton: Willan.

Burns, T. and Stalker, G. M. (1961), *The Management of Innovation*, Tavistock, London.

Camp, L.J. (2007) *Economics of Identity Theft: Avoidance, Causes and Possible Cures,* New York: Springer Science and Business Media.

Card World (April 2009) publication, http://www.cardwatch.org.uk/ (Accessed:27th April 2010).

Cashell, B., Jackson, W.D., Jickling, M. and Webel,B. (2004) *The Economic Impact of Cyber-attacks*, Order Code RL32331,Government and Finance Division, Congressional Research Service, Library of Congress.

Cassim, F. (2015) Protecting Personal Information in the Era of Identity Theft: Just How Safe is our Personal Information from Identity Thieves, *P.E.R.*, Volume 18 No 2.

Ceccato, V.and Benson, M. L. (2016). Tax Evasion in Sweden 2002–2013: Interpreting Changes in the Rot/Rut Deduction System and Predicting Future Trends. Crime, *Law and Social Change*, Volume 66: 217–232.

Cendrowski, H., Martin, J.P. and Petro, L.W. (2007) *The Handbook of Fraud Deterrence, Identity Theft*, John Wiley & Sons Inc, Hoboken, New Jersey.

Cho, Y. and Lee, S. (2016) *Detection and Response of Identity Theft within a Company Utilizing Location Information*, Institute of Electrical and Electronics Engineers Inc, published Apr 19.

CIFAS (2019) Cifas research reveals sharp rise in middle-aged money mules, https://www.cifas.org.uk/newsroom/money-mule-activity-over-40 (Accessed: 1st August 2020).

CIFAS , http://www.cifas.org.uk/ (Accessed:21st February 2019).

Clark, R.V. (1999) *Hot product: Understanding, anticipating and reducing the demand for stolen goods.* Police Research Series, Paper 98. London, UK: Home Office.

Clarke, R.V.(1983) Situational crime prevention: Its theoretical basis and practical scope. In *Crime and justice: An annual review of research*, 4, ed. Michael Tonry and Norvel Morris, 225. Chicago: University of Chicago Press.

Clinard, M.B. and Quinney, R. (1973) *Criminal behaviour systems and typology, Holt, Rinehart and Winston: Austin.*

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, 588-608.

Cohen, L. E., Kluegel, J. R., & Land, K. (1981). Social inequality and predatory criminal victimization: An exposition and test of a formal theory. *American Sociological Review*, Volume 46: 505–524.

Companies House, http://www.companieshouse.gov.uk/infoAndGuide/proofFaqsWebFiling.shtml (Accessed:10th August 2019).

Copes, H. and Vieraitis, L.M. (2012) *Identity Thieves: Motives and Methods*, North eastern University press: Lebanon.

Copes, H., Vieraitis, L.M., Cardwell, S.M. and Vasquez, A. (2013) Accounting for identity Theft: The Roles of Lifestyle and Enactment, *Journal of Contemporary Criminal Justice* Volume 29, issue 3: 351-368.

Cornish, D. B., & Clark, R. V. (1986) Social change and crime rate trends: A routine activities approach. *American Sociological Review*, Volume 44: 588-607.

Cremers, C., Rasmussen, K.B., Schmidt, B. and Capkun, S, (2012) *Distance Hijacking Attacks on Distance Bounding Protocols,* 2012 IEEE Symposium on Security and Privacy, San Francisco, CA, 2012, pp. 113-127, doi: 10.1109/SP.2012.17.

Cressey, D. R. (1969) *Theft of the Nation*. New York: Harper & Row.

Croall, H. (1992) *White Collar and Corporate Crime, Crime and Society in Britain*, London: Longman.

Croall, H. (2001) *Understanding white Collar Crime,* Open University Press: Buckingham.

Crawford, A. (1998a) Crime prevention and community safety: Politics, policies and practices, Harlow: Longman.

Crawford, A. (1999) *The Local Governance of Crime: Appeals to community and partnerships,* Oxford University Press: Oxford.

Crow, I. and Semmens, N. (2008) *Researching Criminology*, Open University Press: Berkshire.

Dadkhah, M., Lagzian, M. and Barchardt, G. (2017) Identity theft in the academic world leads to junk science, *Science and Engineering Ethics*, Volume 24, 287-290.

Damodaram, R. (2016) Study on phishing attacks and antiphishing tools, *International Research Journal of Engineering and Technology (IRJET)*, Volume: 03 Issue: 01:700-705.

Davis, C.A. (2001) *Women who kill: Profiles of female serial killers*, London: Allison and Busby Limited.

Dearden, T. E. (2017) An Assessment of Adults' Views on White-Collar Crime, *Journal of Financial Crime*, volume 24, issue 2: 309–321.

De Lisi, M. (2005) *Career criminals in society*, California: Sage Publications, Inc.

Directive (2016) EU 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1–30, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC (Accessed: 13th September 2020).

Document 1 – EU activities against cybercrime – ID theft/fraud, a presentation at EU commission meeting (Obtained from participant 8).

Document 6 – Expert meeting in identity theft, minutes of an internal meeting (Obtained from participant 8).

Document 8 – Identity fraud, minutes of an internal meeting (Obtained from participant 8).

Document 9- MO: The Fraudster's Modus Operandi: A white paper from 192.com business services (Obtained from participant 15).

Document 11 –UK Card Fraud Conference, Internal presentation March 2009 (obtained from participant 15).

Document 12 – Security and Risk Services Best Practices Series, June 2008 (Obtained from participant 15).

Document 13 – Resist and repel: The Experian Insider Fraud Dossier (obtained from participant 8).

Document 14 – European ATM Security Report, 2005 (Obtained from participant 11).

Document 15 – Incident Summary: Payment Processor (Heartland) Breach February 2009 (Obtained from participant 15).

Document 16 – Security Assessment, Internal report September 2009.

Don Gibbons (1973) *Crime and Criminal Careers* ,Englewood Cliffs, NJ: Prentice Hall.

Douglas, M. and Wildavsky, A. (1982) *Risk and culture*, University of California press.

Durkheim, E. (1938) *The Rules of Sociological Method,* New York: The Free Press.

Edelstein, A. (2016) Rethinking Conceptual Definitions of the Criminal Career and Serial Criminality, *Trauma, Violence and Abuse*, Volume 17, issue 1: 62-71.

Edwards A and Hughes G (2009) 'The Preventative Turn and the Promotion of Safer Communities in England and Wales: Political Inventiveness and Governmental Instabilities', in Crawford A (ed) Crime Prevention Policies in Comparative Perspective, Willan Publishing, Devon.

Emigh, A. (2006) The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond, *Journal of Digital Forensic Practice*, Volume 1, No 3:245-260, DOI: 10.1080/15567280601049985.

Evans, K. (2011) *Crime prevention: A critical introduction*, London: Sage.

Farnsworth, M. (1989) Theory Integration Versus Model building, in S.F. Messner, M.D. Krohn and A.E. Liska (eds), *Theoretical Integration in the study of Deviance and Crime.* Albany, NY: State U

Farrington, D.P.(1997) Evaluating a community crime prevention program, *Evaluation*, Volume 3, issue 2: 157-173

Felson, M. and Clarke R.V. (1998) *Opportunity makes the thief: practical theory for crime prevention.* Police Research Series, London.

Foley, L. (2003) Enhancing Law Enforcement, Identity Theft Communication, *British Journal of Criminology*, Volume 37, issue 2 :165–183.

Fortes, N. and Rita, P. (2016) Privacy concerns and online purchasing behaviour: towards an integrated model*. European Research on Management and Business Economics,* 22(3), 167- 176, http://dx.doi.org/10.1016/j.iedeed.2016.04.002.

Foucault, M. (1984) *What is an Author? in P. Rainow (ed), The Foucault Reader, Harmondsworth,* Penguin: London.

Fraud Act 2006, http://www.opsi.gov.uk/acts/acts2006/ukpga_20060035_en_1 (Accessed: 5th April 2010).

Fraud Focus (February 2010) http://www.attorneygeneral.gov.uk/nfa/WhatAreWeSaying/Documents/Fraud%20Focus_Ed_5_ED_FEB_2010.pdf (Accessed:20th March 2010).

Fraud Focus (October 2010) http://www.homeoffice.gov.uk/publications/agencies-public-bodies/nfa/fraud-focus-newsletter/fraud-focus-oct10?view=Binary (Accessed:11th April 2010).

Fraud Indicator 2016, http://www.port.ac.uk/media/contacts-and-departments/icjs/ccfs/Annual-Fraud-Indicator-2016.pdf (Accessed:14th February 2017).

Fraud Review (2007), www.attorneygeneral.gov.uk/Fraud%20Review/Terms%20of%20NFSA.pdf (Accessed:21st March 2017).

Fraud the facts (2009), APACS, the UK payments association, Mercury House, Triton Court, 14 Finsbury Square, London, EC2A 1LQ.

Fraud the facts (2019), https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202019%20-%20FINAL%20ONLINE.pdf (Accessed: 4th March 2020)

Freilich, J. D., & Newman, G. R. (2017). Situational crime prevention. In *Oxford research encyclopedia of criminology and criminal justice, https://oxfordre.com/criminology/criminology/view/10.1093/acrefore/9780190264079.001.0001/acrefore-9780190264079-e-3 (Accessed: 1st November 2020)*

Frevel, B. and Rogers, C. (2016) Community Partnerships (UK) vs Crime Prevention (GER): Differences and Similarities, The Police Journal: Theory, Practice and Principles, Volunme 89(2):133-150.

Fuss, R. and Hecker, A. (2008), Pro_ling White-Collar Crime: Evidence from German-Speaking Countries, *Corporate Ownership and Control,* Volume 5, No. 4 (Summer), 149-161, Niversity of New York Press.

Golladay, K.A. (2017) Reporting behaviors of identity theft victims: an empirical test of Black's theory of law, *Journal of Financial Crime*, Vol. 24, No 1:101-117.

Garland, D. (1990) *Punishment and Modern Society: A study in social theory*, Oxford: Clarendon.

Garland, D. (2001a) *The culture of control: Crime and social order in contemporary society,* Oxford: Clarendon.

Geis, G. and Jesilow, P. (eds) (1993) White-collar crime, *Special Issue of The Annals of the American Academy of Political and Social Science*, 525 January.

Gerard G.J., Hillison W., Pacini C. (2004) Identify Theft: An Organization's Responsibilities, http://ruby.fgcu.edu/courses/cpacini/ courses (Accessed:26th May 2012).

Gilbert, N. (2005) *Researching Social Life*, Sage Publications Ltd.

Gibbons. K. (2019) Action Fraud ignored dossier detailing Bitcoin scam https://www.thetimes.co.uk/article/action-fraud-ignored-dossier-detailing-bitcoin-scam-n7s92d25l# (Accessed: 20th December 2019).

Gilling, D. (2005) Partnership and crime prevention, *Handbook of crime prevention and community safety,* Tilley, N. Davon: Willan.

Glasser, B. (1978) *Theoretical Sensitivity*, California: Sociology Press.

Goodman, M. (2015) *Future Crimes*, Transworld Publishers: London.

Gordan, M. (2006) Reporting Breaches: When should companies go public following a security breach?, *Computer Fraud & Security*, Volume 2006, Issue 9: 16-18.

Graves, P.E. and Sexton, R.L. (2016) Optimal Public Policy Against Identity Theft, *The American Economist*, Volume 62, Issue 2: 217-221.

Green, G.S. (1990) *Occupational Crime*, Chicago: Nelson Hall.

Green, G.S. (1997) *Occupational Crime*, Nelson Hall Inc, New York.

Goel, R.V. (2018) Identity theft in the internet age: Evidence from the U.S. states, Manage Decis Econ. 2019;40:169-175. https://doi.org/10.1002/mde.2991

Gottfredson, M. and Hirschi, T. (1990) *A General Theory of Crime*, Stanford, CA: Stanford University Press.

Gottschalk, P. (2017) White-collar crime: Detection and neutralization in religious organizations, *International Journal of Police Science and Management*, Volume 19, Issue 2: 120-126.

Hamadi, R. (2004) *Identity Theft, Kent*: Mackays of Chatham Ltd.

Hammesrley, M. and Atkinson, P. (1983) *Ethnography: principles in practice*, London: Tavistock.

Harrell, E. (2015) *Victims of Identity Theft, 2014,* Bureau of Justice Statistics, NCJ 248991.

Hatch, M. (2001) Electronic commerce in 21st century: Article the privatisation of big brother: Protecting sensitive personal information from commercial interests in the 21st century, *William Mitchell Law Review*, 27, 1447.

Helser, S. (2015) *FIT: Identity Theft Education*, IEEE International Symposium on Technology in Society (ISTAS) Proceedings.

Hemphill, T.A. (2001) Identity Theft: A Cost of Business, *Business and Society Review*, Volume 106, Issue 1: 51-63.

Hinde, S. (2005) Identity theft: theft, loss and giveaways, *Computer Fraud & Security*, Volume 2005, Issue 5: 18-20.

HM Government (2018) The Future Relationship Between the United Kingdom and the European Union, White-paper, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/786626/The_Future_Relationship_between_the_United_Kingdom_and_the_European_Union_120319.pdf (Accessed:2nd September 2020).

Hoare & Wood (2007) Plastic card and identity fraud. In J. Fkatekley (Ed.), Mobile phone theft, plastic card and identity fraud: Findings from the 2005/06 British Crime Survey (Supplementary Volume 2). Retrieved February 21, 2009 from http://rds.homeoffice.gov.uk/rds/pdfs07/hosb1007.pdf.

Holt, T. J, Bosslar, A.M and Siegfried-Spellar, K.C. (2018) *Cybercrime and Digital Forensics. An Introduction,* 2nd edition. Routledge. Abingdon.

Home Office Identity Fraud Steering Committee (2008) Identity Crime Definitions, http://www.identity-theft.org.uk/definition.html (Accesses:17th March 2008).

Horning, D.N.M. (1970) Blue Collar Theft: Conceptions of Property, Attitudes toward Pilfering, and Work Group Norms in a Modern Industrial Plant.' In EO.

Huisman, W. and Erp, J. (2013). Opportunities for Environmental Crime: A Test of Situational Crime Prevention Theory. *British Journal of Criminology*, Volume 53, Issue 6: 1178-1200.

Hunt, M. (2017) Preventing Wireless Data Breaches in Retail, https://silo.tips/download/white-paper-preventing-wireless-data-breaches-in-retail (Accessed: 12th September 2020).

Identity cards are to be scrapped, (2008) http://www.homeoffice.gove.uk/media-centre/news/identity-cards-scrapped (Accessed:15th September 2017).

Identity Fraud Steering Group, www.identity-fraud.org.uk (Accessed: 6th June 2009).

Identity force (2018) Real identity theft stories case #11, https://www.identityforce.com/blog/real-identity-theft-stories-part-11-child-id-theft (Accessed: 15th July 2020)

Identity Theft Resources Centre (2003) Identity Theft: The Aftermath 2003, September 23, http://www.idtheftcenter.org/idaftermath.pdf, (Accessed: 20th May 2008).

IDTRC (2017), ' At Mid-Year, U.S. Data Breaches Increase at Record Pace', *Identity Theft Resource Centre Press Release,* https://www.idtheftcenter.org/press-release/2017-mid-year-data-breach-report-press-release.

Information Commissioners Office (ICO), https://ico.org.uk/ (Accessed:12th September 2018).

Insurance Information Institute (2020) Facts + statistics: identity fraud and cybercrime, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (Accessed: 4th July 2020).

Irshad, S. and Soomro, T.R. (2018) Identity Theft and Social Media, International Journal of Computer Science and Network Security, Vol.18, No.1:43-55).

Jacobson,M. and Ramzan, Z. (2008) *Crime ware: understanding new attacks and defences and defences,* Safari Technical Books: California.

Jackson, C., Boneh, D. and Mitchell, J. (2007)*Transaction generators: Root kits for the web.* In: Proceedings of the 2nd USENIX Workshop on Hot Topics in Security, https://www.usenix.org/legacy/events/hotsec07/tech/full_papers/jackson/jackson.pdf (Accessed: 1st October, 2020)

Javelin (2009) 2009 Identity Fraud Survey Report: Consumer Version, Pleasanton, CA: Javelin Strategy and Research.

Jordan, G., Leskovar,R. and Maric, M. (2018) Impact of fear of identity theft and perceived risk on online purchase intention, *Organizacija*, Volume 51, issue 2: 46-155.

Jupp, V. (2001) 'Triangulation', in E. McLaughlin and J. Manice (eds), *The Sage Dictionary of Criminology.* London:Sage.

Jupp, V. & Davies, P. & Francis, P. (2000) *Doing Criminological Research*, SAGE Publication: London.

Kerbsbach, K. (2004) 'Bank Court Losses as Fraud Numbers Climb', US Banker, April 2004, The Thompson Corporation; http://www.usbanker.com/article.html?id=20040415VUYIODHE, (Accessed: 22nd March, 2008).

Kirk, D. (2014) Identifying Identity Theft*, The Journal of Criminal Law*, Volume 78, Issue 6: 448-450.

Kirwan, G. and Power, A. (2013) *Cybercrime: The Psychology of Online Offenders*, Cambridge University Press: Cambridge.

Koops, B. and Leenes, R. (2006) Identity theft, identity fraud and/or identity-related crime: Definitions matter. *Datenschutz und Datensicherheit* - DuD, Volume 30, 553-556.

Lacey, D., Zaiss, J. and Barber, K.S. (2016) Understanding Victim-enabled Identity Theft: Perpetrator and Victim Perspectives, *Privacy, Security and Trust* (PST), 14th Annual Conference.

Laney, D. (2012) To Facebook you are worth $80.95, CIO Journal (blog), *Wall Street Journal*, May 3, 2012.

Lavorgna, A. (2020) *Cybercrimes: Critical Issues in a Global Context*, MacMillian: London.

Leyden, J (2001) *Identity Thefts from the Rich and Famous,* https://www.theregister.com/2001/03/20/identity_thefts_from_the_rich/ (Accessed 6th July 2020)

Lim, Y.J., Osman, A., Salahuddin, S.N., Eomle, A.R. and Abdullah, S. (2016) Factors influencing online shopping behaviour: the mediating role of purchase intention. *Procedia Economi9cs and Finance*, 35, 401-410, http://dx.doi.org/10.1016/S2212-5671(16)00050-2.

Link Website (2011) http://www.link.co.uk/media/newsreleases/pages/linksupportsphdatcentralstmartins.aspx (Accessed:20th April 2012)

LoPucki, L.M, (2001) Human Identification Theory and the Identity Theft Problem, *Texas Law Review*, Volume 80:89-135.

Mann, K. (1989) "Sanctioning White-collar Offenders" paper presented to the School of Criminal Justice, Rutgers the State University of New Jersey, February.

May, T. (1993) *Social Research- Issues, Methods and Process*, Open University Press: Buckingham.

Maxwell, J.A.(1996) *Qualitative Research Design: An Interpretive Approach*, London: Sage Publication.

M. McCune, J., Perrig, A. and Reiter, M.K. (2009) Safe passage for passwords and other sensitive data, In Giovanni Vigna, editor, Proceedings of NDSS 2009. The Internet Society, February 2009, https://netsec.ethz.ch/publications/papers/mccune_perrig_reiter_ndss09.pdf (Accessed: 12th September 2020).

McNally, M. (2008) Charting the Conceptual Landscape of Identity Theft, in *Perspectives on Identity Theft,* Volume 23: 33-53 edited by M.McNally and G.Newman, Crime Prevention.

McNally, M.M. and Newman, G.R. (2010) *Perspectives on Identity Theft*, London:Rienner.

Merton, R.K. (1949) Social Structure and Anomie: Revisions and extensions, in Anshen. (ed) *The Family*, New York: Harper Brothers.

Miles, M.B. and Huberman, A.M. (1994) *Qualitative Data Analysis: an Ethnographic Sourcebook* (2nd edn), London: Sage.

Monahan, T. (2009) Identity theft vulnerabilities: Neoliberal governance through crime construction, *Theoretical Criminology*, Volume 13, issue 2: 155-176.

Morgan-Bentley, P. and Good, A. (2019) Action Fraud: victims misled and moched as police fail to investigate, www.thetimes.co.uk/article/action-fraud-investigation-victims-misled-and-mocked-as-police-fail-to-investigate-wlh8c6rs6 (Accessed:19th August 2019)

Murdock, S.J., Drimer, S., Anderson, R. and Bond, M. (2010) Chip and PIN is Broken, IEEE Symposium on Security and Privacy, https://www.cl.cam.ac.uk/research/security/banking/nopin/oakland10chipbroken.pdf (Accessed: 1st July 2011).

Murdock, S.J. and Anderson, R. (2010) Verified by Visa and MasterCard SecureCode: or How Not to Design Authentication, https://www.cl.cam.ac.uk/~rja14/Papers/fc10vbvsecurecode.pdf (Accessed: 4th July 2011).

National Crime Prevention Programme (2004) ID Theft: A Kit to Prevent and Respond to Identity Theft, February 2004, Commonwealth of Australia.

National Fraud Authority (2012) *Annual Fraud Indicator*, National Fraud Authority, March, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/118530/annual-fraud-indicator-2012.pdf (Accessed:15th January 2011).

National Fraud Authority Business Plan 2010/11, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/118513/business-plan-2011-12.pdf (Accessed:15th January 2011).

National Statistics (2012*) 2010/11 Scottish Crime and Justice Survey: Main Findings*, National Statistics/Scottish Government, http://www.scotland.gov.uk/Resource/Doc/361684/0122316.pdf (Accessed:14th April 2019)

ONS (2018b) Crime in England and Wales, https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables (Accesses:7th June 2020)

Nettler, G. (1974) Embezzlement without Problems, *British Journal of Criminology, Volume* 14: 70-77.

Newburn, T. (2007) *Criminology*, Devon: Willan Publishing.

New Estimate of Cost of Identity Fraud to the UK Economy (2006-7) http://www.identitytheft.org.uk/cms/assets/cost_of_identity_fraud_to_the_uk_economy_2006-07.pdf (Accesses:5th February 2009)

Newman, G. (2004) Identity Theft, Problem-oriented Guides for Police, *Problem-Specific Guides Series* No. 24. Washington, DC:U.S. Department of Justice.

Newman, G. (2009) Identity theft and opportunity, *Perspectives on identity theft*, McNally, M.M. and Newman, G.R.,London: Lynne Reinner.

Newman, W.L. (1997) *Social Research Methods- Qualitative and Quantitative Approaches* (3rd edn), London: Allyn and Bacon.

Newman, G.R. and R.V.Clark (2003) *Superhighway robbery: Preventing e-commerce crime*, London; Willan.

Online Business Dictionary, http://www.businessdictionary.com/ (Accessed: 9th July 2012).

Onyesolu, M. O., & Okpala, A. C. (2017). Improving security using a three-tier authentication for automated teller machine (ATM). *International Journal of Computer Network and Information Security*, 9(10), 50. doi:http://dx.doi.org/10.5815/ijcnis.2017.10.06

Osborne, H. (2017) Wonga data breach could affect nearly 250,000 UK customers, https://www.theguardian.com/business/2017/apr/09/wonga-data-breach-could-affect-250000-uk-customers (Accessed:17th September 2018)

Passas, N. (2009) Anomie and Corporate Deviance in Whyte, D. (ed.), *Crimes of the Powerful: A Reader*, Maidenhead: Open University Press.

Perl, M. W. (2003) It's not always about the money: Why the state identify theft laws fail to adequately address criminal record identity theft, *Journal of Criminal Law and Criminology*, Volume 94, No 1:169- 208.

Pontell, H.N., Brown, G.C., & Tosouni, A. (2008). Stolen identities: A victim survey. In M. McNally & G. Newman (Eds.), *Perspectives on identity theft* (pp. 57-86). New York: Criminal Justice Press.

Poore, R.S. (2001) Identity Theft: Who Are Anyway*?, Information Security Journal*: A Global Perspective, Volume 10, No 3: 1-6.

Porter, M. (1994) Second Hand Ethnography': Some Problems in Analysing Feminist Project, in A. Bryman and R.G. Burgess (eds) *Analysing Qualitative Data,* London: Routledge.

Punch, M. (1996) *Dirty Business*, London: Sage.

Reyns, B. W. and Henson, B. (2016) The Theft with a Thousand Faces and the Victim with None: Identifying Determinants for Online Identity Theft Victimization with Routine Activity Theory*, International Journal of Offender Therapy and Comparative Criminology*, Volume 60, Issue 10: 1119-1139.

Robin,G.D. (1974) White – Collar Crime and Employee Theft, *Criminal Justice*, Volume 20, Issue 3: 251.

Rost, M.,Meints, M. and Hanson, D (2005) "Authentisierung in sozialysystemen- Identity Theft Strukturell Betrachtet Datenschutz und Datenscherheit 4/ 2005 PP. 216-2018, Wiesbaden April.

Ruggiero, V. (2015) *Power and Crime,* Routledge: New York.

Ruggiero, V. (2017) *Dirty Money: On Financial Delinquency*, Oxford University Press: Oxford.

Sampson, R. and Laub, J.H. (2016) Turning Points and the Future of Life-Course, *Criminology* , Volume 53, Issue 3.

Scheerhout, J. (2014) The fraudster who lived the high life thanks to identity theft, http://www.manchestereveningnews.co.uk/news/greater-manchester-news/jailed-fraudster-who-lived-high-8114301 (Accessed:12th November 2017)

Scott, J. (1990) *A Matter of Record: Documentary sources in social research,* Cambridge: Polity Press.

Security Report Online Identity Theft, (2006), http://www.btplc.com/onlineidtheft/onlineidtheft.pdf (Accessed:25th May 2005).

Shah, M.H., Ahmed, J. and Soomro, Z.A. (2016) Investigating the identity theft prevention strategies in M-Commerce, Internationa Conferences ITS, ICEdu Tech and STE 2016.

Shah, M., Maitto, A. Jones, P. and Yusuf, Y. (2019) An investigation into agile learning processes and knowledge sharing practices to prevent identity theft in the online retail organisations, *Journal of Knowledge Management*, Volume 23, Issue 9, 1857-1884.

Shapiro, S. (1990) "Collaring the Crime, Not the Criminal: Reconsidering the Concept of White Collar Crime," *American Sociological Review,* Volume 55: 346-65.

Sharp, T., Shreve- Neiger, A., Fremouw, W., Kane, J., and Hutton, S. (2004) Exploring the Psychological and Somatic Impact of Identity Theft, *Journal of Forensic Science*, Volume 49, No1.

Shover, N. & Cullen, F.T. (2008) Studying and teaching white-collar crime: populist and patrician perspectives. *Journal of Criminal Justice Education*, Volume 19: 155-174.

Skidmore, M.; Ram, J.; Goldstraw-white, J.; Barrety, C.; Barleaza, S.; Mur, R. and Gill, M. (2018) More than just a number: improving the police response to victims of frsud, file:///C:/Users/aidaf/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/more_than_just_a_number_exec_summary%20(1).pdf (Accessed:10th August 2019).

Slapper, G. and Tombs, S. (1999) *Corporate Crime*, Harlow: Longman.

Smigel, E. (1956). Public Attitudes Toward Stealing as Related to the Size of the Victim Organization, *American Sociological Review* 21(June): 320-27.

Smith, R. (2010) Identity theft and fraud, pp. 273-301 in Y. Jewkes and M. Yar (eds) *Handbook of Internet Crime*, Cullompton: Willan.

Soomro, Z.A. Shah, M.H., and Ahmed, J (2016) Information security management needs more holistic approach: A literature review. International Journal of Information Management, Vol.36, No2, 215-225. Http://dx.doi.org/10.1016/j.ijinformgt.2015.11.009.

South, N. (1998a). A green field for criminology? A proposal for a perspective. *Theoretical Criminology,* 2(2), 211–233.

Strauss, A.L and Corbin, J. (1998) *Basics of Qualitative Research – Techniques and Procedures for Developing Grounded Theory* (2nd edn), London: Sage.

Sutherland, E. H. (1940) White-collar Criminality, *American Sociological Review*, Volume 5: 1-12.

Sutherland, E. H. (1949) White – Collar Criminality, *American Sociological Review*, Vol 5, No.1: 1-12.

Sutherland, E. H. (1983) *White Collar Crime: The Uncut Version*, New Haven, CT: Yale University Press.

Sykes,G. and Matza, D. (1957) Techniques of Neutralization: A theory of delinquency. *American Sociological Review*, Volume 22:664-670.

Synovate. (2003) Federal Trade Commission: Identity theft survey report, http://www.ftc.gov/os/2003/09/synovatereport.pdf (Accessed:19th Marth, 2008)

Tappan, P.W. (1947) Who is the criminal? *American Sociological Review*, Volume 12, No 1:96-102.

Tatft, D.R. and England, R.W (1964) *Criminology,* New York: McMillan.

The Associated Press, (2018) *Reno man guilty in $3.5 million ID theft scheme,* https://www.seattletimes.com/nation-world/reno-man-guilty-in-3-5-million-id-theft-scheme/ (Accessed: 15 July 2020)

The new GDPR rules enforced from 25th May 2018, http://www.itpro.co.uk/general-data-protection-regulation-gdpr/31025/gdpr-fines-how-high-are-they-and-how-can-you-avoid (Accessed:14th July 2018).

The UK Cyber Security Strategy 2011-2016, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf (Accessed:26th February 2017).

The UK Cyber Security Strategy 2011-2016, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf (Accessed:12th March 2020).

Tilley, N. (2002) Introduction: analysis for crime prevention, in N. Tilley (ed) *Analysis for crime prevention*, Crime Prevention Studies Series, Vol 13.

Toft, .B. and Reynolds, S. (1994) *Learning From Disasters: A Management Approach,* Oxford: Butterworth-Heinemann.

Trahan, A. (2011). Filling in the gaps in culture-based theories of organizational crime. *Journal of Theoretical and Philosophical Criminology*, Volume 3, Issue 1: 89–109.

Tuffcub (2017) UK Retailer CEX Suffers Data Breach, 2 Million Accounts Accounts Affected, http://www.thesixthaxis.com/2017/08/29/uk-retailer-cex-suffers-data-breach-2-million-accounts-accounts-affected/ (Accessed:9th September 2018).

United Nations declaration on victims (1991), https://www.unicef-irc.org/portfolios/documents/472_un-declaration-crime.htm (Accessed:6th June 2012).

United Nations Handbook on Identity-Related Crime (2010) https://www.unodc.org/documents/treaties/UNCAC/Publications/Handbook_on_ID_Crime/10-57802_ebooke.pdf Accessed:12th July 2017) .

US Identity Theft and Assumption Deterrence Act (1998), https://www.ftc.gov/node/119459 (Accessed:12th July 2012)

Villar-Rodriguez, E., Del Ser, J., Torre-Bastida, A.I., Bilbao, M.N. and Salcedo-Sanz, S. (2016) A novel machine learning approach to the detection of identity theft in social networks based on emulated attack instances and support vector machines, Concurrency Computat: Pract. Exper: 2016;28:1385-1395.

Vins, B., Tigchelaar, J. and Linden, T. (2008) Describing Identity Fraud: Towards a Common Definition, *Scripted*, Volume 5, Issue 3.

Visa Global Security Summit Summery Report (2011) http://www.visasecuritysummit.com/media/2011SecuritySummitSummary.pdfissues (Accessed: 3rd July 2012).

Vold, G, and Bernard, T.J. (1986)*Theoretical criminology*, 3rd ed., Oxford University Press: New York.

Vuckovic, Z., Vukmirovic, D., Milenkovic, M.J., Ristic, S., and Prljic, K. (2018) Analyzing of e-commerce user behaviour to detect identity theft, PhysicaA, 511:331-335.

Wall, D. (2007) Cybercrime, Polity Press: Cambridge. White and Fisher (2008), Assessing Our Knowledge of Identity Theft: The Challenges to Effective Prevention and Control Efforts, *Criminal Justice Policy Review*, Volume 19, Issue 1: 3-24.

Wall, D.S. (2010a) Micro-Frauds: Virtual Robberies, Stings and Scams in the Information Age**,** pp. 68-85 in T. Holt, T., and B.S chell (eds) *Corportae Hacking and Technology-Driven Crime: Social Dynamics and Implications*, Hershey, PA (USA): IGI Global.

Wall, D.S. (2010b) 'The Organization of Cybercrime and Organized Cybercrime', pp, 53-68 in M. Bellini, P. Brunst, and J. Jaenke (2010) (eds*) Current issues in IT security, Freiburg: MaxPlanck-Instituts für ausländisches und internationales Strafrecht*.

Wall, D.S. (2013a) *Identity related crime in the UK*, paper DR19 Future of identity series, London: government Office for Science Foresight initiative project.

Wall, D.S. (2013b) *The future challenges of identity crime in the UK*, paper DR20 Future of identity series, London: government Office for Science Foresight initiative project.

Wall, D.S. (2018) How Big Data Feeds Big Crime, *Global History: A Journal of Contemporary World Affairs*, P:29-35.

Walton, R. (2005) Identity Infrastructure: security considerations, *Computer Fraud & Security*, Vol 2005, Issue8.

Walsh, G., Hille, P. and Cleveland, M. (2016) *Fearing online identity theft: A segmentation study of online customers,* ECIS proceedings conference.

Wheeler, S. Weisburd, D. and Bode, N. (1982) Sentencing the White-Collar Offender: Rhetoric and Reality, *American Sociological Review* Volume 47, Issue 5:641-51.

Wheeler, S., Weisburd, D., Waring, E. and Bode, N. (1991) *Crimes of the Middle vlasses: White-collar offenders in the Federal Courts*. New Haven, CT: Yale University Press.

White, M.D. and Fisher, C. (2008) Assessing Our Knowledge of Identity Theft: The Challenges to Effective Prevention and Control Efforts, *Criminal Justice Policy Review*, V 19, No 1, 3-24.

Williams, F.P. and McShane, M. D.(2010) *Criminological Theory*, 5th Edition University of Houston: Downtown.

Winch, J. (2013) 'Our £130,000 bill from identity theft', http://www.telegraph.co.uk/finance/personalfinance/money-saving-tips/10388791/Our-130000-bill-from-identity-theft.html (Accessed:5th June 2017)

Wolfgang, M.E., Figlio, R. M. and Sellin, T. (1972) *Delinquency in a Birth Cohort*. Chicago: University of Chicago Press.

Wright, A. (2006) *Organised Crime*, Cullompton: Willan.

Whitty, MT, Buchanan, T (2012) The online dating romance scam: A serious crime. Cyberpsychology, *Behavior, and Social Networking* 15(3): 181–183.

Willison, R.(2008) Applying situational crime prevention to the information systems context, *Crime Prevention Studies*, Volume 23, 169-192.

Wortley, R. (2010) Critiques of situational crime prevention. In B. Fisher & S. Lab (eds) *Encyclopedia of Victimology and Crime Prevention,* Thousand Oaks, CA: Sage.

Yang, Y., Manoharan, M. and Barber, S. (2014) Modelling and Analysis of Identity Threat Behaviours Throught Text Mining of Identity Theft Stories, IEEE Joint Intelligence and Security Informatics Conference.

Yar, M. and Steinmetz, K.F. (2019) *Cybercrime and society*, London: Sage.

Young, J. (1992) Ten points of realism, in Young, J. and Matthews, R. (eds) *Rethinking Criminology: The realist debate*, London: Sage.

Young, E. (2005) BBA Annual Fraud Conference, http://www.fsa.gov.uk/pages/Library/Communication/Speeches/2005/0627_ey.shtml (Accessed: 27th March, 2008).

9. Appendix

9.1. Situational crime prevention techniques table

Increase the effort	**Increase the risks**	**Reduce the rewards**	**Reduce provocations**	**Remove excuses**
Target harden	Extend guardianship	Conceal targets	Reduce frustrations and stress	Set rules
Control access	Assist natural surveillance	Remove targets	Avoid disputes	Post instructions
Screen exits	Reduce anonymity	Identify property	Reduce temptation and arousal	Alert conscience
Deflect offenders	Use place managers	Disrupt markets	Neutralise peer pressure	Assist compliance
Control tools/ weapons	Strengthen formal surveillance	Deny benefits	Discourage imitation	Control drugs and alcohol

9.2. Table of techniques utilized by the finance sector to tackle identity crimes

Type of control	Relevant theory
Customer authentication	
Chip and PIN	Target hardening (Increase the effort)
Two factor authentication	Target hardening (Increase the effort)
Dynamic authentication	Target hardening (Increase the effort)
Risk based approach to authentication	Risk management
Dynamic one time passwords	Target hardening (increase the effort)
ID&V / KYC/ False credentials	
Identity documents checking solutions	Access control (Increase the effort)
JMLSG AML guidelines	Guidelines
Layered control checks and sampling	Target hardening (Increase the effort)
Electronic KYC(Know Your Customer)	Intelligence/ data mining based
Hunter-CIFAS-DETECT-SIRA	Intelligence/data mining based
Shared secrets	Data sharing
Use of partial static data	Target hardening (Increase the effort)
Dynamic data	Target hardening (Increase the effort)
Pattern authentication	Intelligence/data mining based
PVC-Passport Verification System	Target hardening (Increase the effort)
Chip based authentication for two factor	Target hardening (Increase the effort)
Data compromise	
PCI-DSS	Guidelines
Exception reporting- unusual activity	Intelligence/data mining based
Incident management	Incident management
Card reissuing	Controlling tools (Increase the effort)
Status coding of accounts at risk for	Intelligence/data mining based

monitoring purposes	
Ongoing monitoring of at risk cards at the end of their life e.g. expiry data	Intelligence/ data mining based
Access controls	Access control (Increase the effort)
Segregation of duties	Reduce temptation/arousal (Reduce provocations)
Firewalls	Target hardening (Increase the effort)
Physical protection	Target hardening (Increase the effort)
FSA- regulatory controls	Regulatory guidance
Collaborations with various organisations and stakeholders	Partnership approach
Remote purchase fraud and online banking	
Malware monitoring	Strengthening formal surveillance (Increase the risk)
E-crime data sharing across communities	Data sharing
Card schemes	Regulatory
Protection of customer PC	Target hardening (Increase the effort)
Padlock symbol – https:/	Awareness raising
Customer vulnerability	
Card activations calls/internet-use two factor authentication or high level of password ID	Control tools (Increase the effort)
Universal ID policy and rigour for all channels recognising risks by channel	Access control (Increase the effort)
Card Watch materials – PR releases – PR Calendar _ Media campaigns	Awareness raising
Use of external data sources e.g. IP addresses in controls	Data sharing
Secure mailings for card delivery	Target hardening (Increase the effort)
Quantity out of pattern expenditure	Intelligence/data mining based

Reporting of loss – encourage customer vigilance at all times	Education/behavioural change
Be card smart online	Education/behavioural change
Crimestoppers- encourage reporting crimes	Law enforcement/intelligence
Consumer education through various channels	Education/behavioural change
Uptake of anti-virus software increase	Access control (Increase the effort)
Acknowledgment of measures required by partners/ISP providers, Google etc	Partnership approach
Staff and insiders	
CRB checks	Access control (Increase the effort)
Control checks-policy-role based access controls	Access control (increase the effort)
Enforced leave-2 weeks consecutive	Set rules (Remove excuses)
Call monitoring	Surveillance (Increase the risk)
Audit control checking	Surveillance (increase the risk)
Credit checks	Proactive
Whistle-blowing volumes	Natural surveillance (Increase the risks)
Monitoring engines	Surveillance (Increase risk)
CIFAS staff fraud database	Data sharing
Card ID theft (Account takeover)	
Transaction monitoring for card re-order, change of details or balance transfer	Surveillance (Increase the risk)
Contact customer using new/old details where change made	Proactive
Data sharing of balance transfer beneficiary and transfer details	Data sharing
Balance transfer through BACS gives three days to identify	Proactive
Indemnity process Compensation from charges or losses/	Unique to financial identity crimes

exemption from liability	
First party fraud and mules	
Information sharing mule database	Data sharing
Indemnity process/ interbank enquiries	Data sharing
Transaction profiling payments	Intelligence/data mining based
FISS	Data sharing
Hunter	Data sharing
Detect	Data sharing
100% online authorisation	Access control (Increase the effort)
Account monitoring	Surveillance (Increase the risk)
Behavioural scoring	Intelligence/ data mining based
Counterfeit cards	
DDA cards and the mandate in place by card schemes	Target hardening (Increase the effort)
Scanning for off-line authorised transactions	Proactive- monitoring
Zero floor limits	Target hardening (Increase the effort)
Use of industry Hot Card Files	Data sharing
Detection software –Hybrid systems combining the Neural Network models and Rule based systems	Surveillance (Increase the risk)
Cross border card fraud	
Issuer rules for cards used at overseas ATM's	Regulatory
Card scheme reporting and alert system e.g. Visa GFIS	Intelligence/ data mining based
ATM profiling schemes Monitoring the ATM to see the fraud attacks quicker	Proactive – monitoring
Issuer optimisation and use of iCVV	Target hardening (Increase the effort)

Mobile services and payments	
Authentications	Target hardening (Increase the effort)
Third party and agency services	
Audit trails	Surveillance (increase the risk)
Existing SLAs and contracts	Regulatory
Rigorous due diligence	Proactive
Alternative risk based strategies	Risk management
Alternative regulatory bodies	Regulatory
Scrutiny of broker and solicitor	Proactive
PCI DSS third party agent registration programme	Regulations
Existing card scheme registration programs for third party service providers	Proactive
FSA register of financial services practitioners	Proactive
Remote purchase fraud	
3D secure	Target hardening (Increase the effort)
Address verification service	Intelligence/ data mining based
Card security code CVV/CVC	Target hardening (Increase the effort)
Profiling systems – e-vision	Intelligence/ data mining based
In or out of wallet challenge Out-of-wallet checks are intended to validate the consumer's identity by asking them questions that are derived from his/her past credit or public records, most typically using credit reports. Generally includes three to ten questions in a multiple-choice format.	Target hardening (Increase the effort)
IP Geolocation information This is a service provided by third parties to e-merchants and works on helping the merchant with the location of the customer. There is a mis-conception that if you know where the IP address is, you know where	Target hardening (Increase the effort)

the customer is- but in reality this could be very different.	
Order velocity monitoring: Velocity monitoring is a technique used in the banking industry to detect potential fraudulent use of a debit card by analyzing sudden and dramatic changes in debit card usage.	Proactive- monitoring
External passive verification sources	Target hardening (Increase the effort)
Hot lists, sometimes referred to as negative lists are utilized to reject orders from customers that have had charge-backs on previous orders.	Proactive- monitoring
Counterfeit card fraud	
Transaction monitoring	Surveillance (Increase the risk)
Payment profiling	Intelligence/ datamining based
Maestro CVV/AVS checks	Target hardening (Increase the effort)
Risk based strategies	Risk management
Call centre =social engineering	
Authentication process	Target hardening (Increase the effort)
Regular training	Training
Track and monitor calls	Surveillance (Increase the risk)
Frequency of contacts by account	Proactive monitoring
Cashing out	
Strategic fraud and security guidance in the design of new payment systems	Guidelines
Fraud detection systems	Intelligence/ data mining based
ATM	
Country hot spots	Intelligence/ data mining based
iCVV rollout	Target hardening (Increase the effort)
Card protection kits (CPKs)	Target hardening (Increase the effort)
CCTV	Surveillance (Increase the risk)

Signage/messages	Educational
Safe zones	Deflect offenders (Increase the effort)
Jitter software Jitter technology uses a stop-start, or jitter motion, when a card is inserted in the ATM. The irregular motion distorts the magnetic stripe details on the card, so if a skimming device has been placed on an ATM, the jitter feature makes the copied information unusable.	Deny benefits (Reduce the rewards)
ATM usage limits- volume and value, chip non-chip, country	Target hardening (Increase the effort)
Working in liaison with Crimestoppers and offering a reward of up to £25,000 for information on cash machine fraud	Proactive
Funding a 4 year bursary PhD course supported by Central Saint Martins' award winning Design Against Crime Research Centre (DACRC) The PhD student will consider how design and innovation may reduce ATM crime and improve the customer experience by addressing customer communication, design improvements within the wider build environment and the interaction design of ATM software.	Proactive
LINK first worked with DACRC in 2011 when the company was involved in an industry sponsored design project with CSM's BA Product Design students. The brief was to design new and cost-effective solutions to tackle ATM crime. The results were exciting and innovative, prompting LINK to consider the extension of this early research with a full-time PhD into the subject.	Proactive
Card not received fraud	

Risk based delivery strategy	Risk management
Industry data sharing on high risk post codes	Data sharing
Card activation	Control tools (Increase the effort)
Separate PIN mailer	Control tools (Increase the effort)
Data sharing with Royal Mail black data	Data sharing
Staff training, education and awareness	
Minimum training is a control and a gap	Training
Fraud CBT-computer based training – modular	Training
Publications	Training
Fraud awareness –promotions-fraud awareness week	Training
CCTV (monitoring staff at all times)	Surveillance (Increase the risk)
Monitoring and recording phone conversations and computer logins	Surveillance (Increase the risk)
Cheque fraud	
Security features on cheques	Target hardening (Increase the effort)
Cheques printer accreditation scheme	Control tools (Increase the effort)
Limited supplies to print/equipment materials etc	Control tools (Increase the effort)
Minimum security standards	Target hardening (Increase the effort)
Staff training and awareness	Training
Systems to check cheques	Proactive
Account profiling	Intelligence/ data mining based
Rules on cheque stockpiling	Set rules (remove excuses)
Rules on distribution	Set rules (remove excuses)

9.3. Recommendation to further utilize SCP techniques in the finance sector

Theory	Sub theory	Applicability
Increase the effort	Target harden	End to end encryption of data
	Control access	Access control needs to be biometric rather than passwords which are becoming increasingly outdated and vulnerable to compromise No data (by the way of a small storage unit or a laptop) should be allowed to leave the company premises
	Screen exits	Far tougher screening for those employees who have access to consumer data Making the offender work much harder to steal the data
	Deflect offenders	Harder for people to access data Specially designed tests for those employees who work with data Specifically designed education for those employees who work consumer data
	Control tool/weapons	More controls on specific tools that facilitate production of other tools to commit financial crime (such as certain electronics like PEDs, cards, etc)
Increase the risks	Extend guardianship	Increase the role of the police and their responsibility in dealing with identity related financial crime Board level data protection director who could be an IT specialist or just a resource dedicated to oversee secure handling of data and preventing compromises
	Reduce anonymity	Within organisations there needs to be a system where every time someone searches for data the system will flag it up. It is best that the employees are told about it. This will have a impact on averting internal staff data theft. To have better processes inside the organisation so that in case of a breach the company can track the source of it.
	Strengthen formal surveillance	Regular surveillance of employee social media accounts accessed in the workplace for signs of collusion with fraudsters
Reduce the rewards	Conceal targets	An end-to-end solution

	Remove targets	Not to store consumer data anywhere or under any circumstances
	Identify property	To have a system where all stolen identities are flagged up when used
	Disrupt markets	It is very well known that the identity data stolen by various organised groups end up on the internet for sale. The banking industry should exploit the use of this strategy to disrupt such operations on the internet.
	Deny benefits	Data needs to be made useless for hackers and criminals such as better authentication/encryption processes This is an area that is the most challenging to the finance industry. As this is an industry wide issue/challenge the first line of efforts needs to be focused on researching the best authentication methods available. Experts should be consulted so that if changes need to be made to the available solutions to make them more effective these can be implemented quickly. It is known that fraudsters target those that have weaker systems in place. So if an effective solution is adopted/ implemented industry wide, there will be no weak link in the chain to be targeted by fraudsters. The industry is well acquainted with using standards. Standards could be developed in authentication to assist them in the process. Establishing the benefits of these defences so that they can be used in business cases presented to non-fraud decision makers within these institutions.
Reduce provocations	Reduce frustration and stress	This can work very well in relation to internal fraud where staff due to work related stress may be driven towards data theft or may be more easily convinced to participate with organised gangs.
	Avoid disputes	This could have an impact on internal fraud. A disgruntled employee may commit fraud as revenge against his/her employer. Such disputes should be resolved amicably. Good clear human resources policies that would cover grievance procedures, escalation procedures, fair internal tribunal (with independent parties outside the organisation) would help in such circumstances.
	Reduce temptation and arousal	Important information which is inadequately guarded increases temptation To make sure that there are systems in place both in computing and procedures to offset such arousals.

		This could be considered in three different stages: 1. Accessing data 2. Use of that data 3. The correct and complete closure of that data within an agreed timeframe
	Neutralize peer pressure	For internal employees- widely publicise to the entire staff when a colleague has been apprehended for stealing data.. This will have a positive impact on thwarting those who might consider crime under pressure from colleagues or criminals.
	Discourage imitation	Same as above
Remove excuses	Set rules	This is very important for helping to tackle the insider element of identity related crimes. All organisations small and large need to have such rules in place.
	Post instructions	And such rules need to be openly and frequently communicated to staff
	Alert conscience	This can be utilized in a number of situations and places: • At ATMs • On screen prompts before the final stage of an online transaction
	Control drugs and alcohol	This could have an impact when dealing with employees who under the influence of alcohol or drugs may be tempted to steal data. Some may even do this to feed an addiction. At the beginning of the employment stage, tests could be carried out to make sure that the person being employed is free of such addictions.

9.4 Interview questions

1. How is identity crime perceived in your organisation?
   At what level in your organisation in this issue managed?

2. Are you affected by identity crime?
   How do you measure it?

3. How do you define identity crime?
   What does identity crime consist of? How is identity crime committed against your organisation?

4. Who are the victims of identity crime?
   To what extent are they victimised? How are they victimised? Are there any procedures to help them recover?

5. Who are the offenders?
   How do they obtain the necessary information to commit the crime? What methods do they use to commit the fraud?

6. What objectives do you employ with regards to identity crime?
   Which risk based approach do you take (transfer, tolerance or specific strategy)? How do you set these objectives? Who sets the objectives?

7. How do you detect identity crime?
   How do you develop these methods? What percentage of detected id crime gets investigated?

8. What prevention and mitigation measures do you have in place?
   How do you develop these prevention methods? Who develops them?

9. Do you work with other organisations or institutions to combat the issue?
   If yes, which organisations do you work with? In what context do you work with these organisations? Has these collaborations being effective?

10. What else needs to be done to tackle the issue?