

Durham University

MSc Criminology and Criminal Justice Dissertation



Online and Offline Correlates of Card-not-present Fraud Victimisation in the UK

In Partial Fulfillment
of the requirements for the Degree of
Master of Sciences in Criminology and Criminal Justice

School of Applied Social Sciences

Supervisor: Dr Christopher Lawless

Naci Akdemir

ABSTRACT

This study addresses the relatively unexplored issue of correlates of the card-not-present fraud and the effect of fear of card-not-present fraud on behavioural adaptation and preventive measures. Recent studies have suggested that the lifestyle and online activities of Internet users plays an important role in their own victimization. However, little is known about the online and offline correlates of CNP fraud victimization. This study applies the Life-style Routine Activities approach as the theoretical framework. Using Crime Survey England and Wales (2013-2014), binary logistic regression analyses suggest that identity theft is the most significant precursor to CNP fraud victimisation. Risky online behaviours appeared to be associated with increased risk of victimisation. Results pertaining to the effect of fear of CNP fraud victimisation and past CNP fraud victimisation experience suggest that these two factors have significant impact on both behavioural adaptation and increased preventive measures. Overall, these findings appear to support the proposition of victim precipitation in CNP fraud victimisation. This study has an impact to the knowledge and understanding of card-not-present fraud victimization for policy makers and law enforcement bodies as well as for credit card users.

ACKNOWLEDGEMENTS

I would like to express my utmost gratitude to Professor David Wall for providing his expertise and guidance throughout the process of this dissertation. He is always been a source of great inspiration for me. I would also like to express my most sincere gratitude to my supervisor, Dr. Christopher Lawless. Without his endless support and invaluable feedback, I feel as though this dissertation could have never been completed. Additionally, I would like to express my appreciation to Professor Maggie O'Neil for her continuous encouragement and precious advice. Her support has benefited this dissertation greatly. Finally, I would like to thank to Dr. Vikki Boliver for her support and sharing her expertise on the statistical methodology.

I am also very grateful to the Turkish Gendarmerie General Command for their support and accrediting me as a candidate to pursue this postgraduate study.

Most importantly, I would like to thank to my wife Eda, my son Atakan and my daughter Elanaz for their endless love and support throughout all of my endeavors.

This dissertation has been dedicated to the loving memory of my mother, who passed away while this dissertation was being crafted.

CONTENTS

ABSTRACT	ii
ACKNOWLEDGEMENTS	iii
CONTENTS	iv-vii
LIST OF TABLES	vii-x
LIST OF FIGURES	xi
1 Introduction	
1.1 Introduction	1
1.2 Structure of Dissertation	4
2 Background	
2.1 Introduction	5
2.2 Cybercrime	5
2.2.1 Definition of Cybercrime	5
2.2.2 Classification of Cybercrimes	6
2.3 Card-not-present Fraud	6
2.3.1 Typology of Card-not-present Fraud	8
2.4 Identity Theft	10
2.4.1 Identity Theft in Cyberspace	11
2.4.2 Identity Theft in “Meatspace”	12
2.5 Fear of Online Crime	14
2.5 Theoretical Framework	14

3	Review of Literature	
3.1	Introduction	19
3.2	Online Victimisation	19
3.2.1	Computer Content Crimes	20
3.2.2	Computer Integrity Crimes	20
3.2.3	Computer Assisted Crimes	21
3.3	Demographic Characteristics of Victims	21
3.4	Offline Fraud Victimisation	22
3.5	Online Fraud Victimisation	23
3.6	Fear Of Online Crime	25
3.7	Aims of the Dissertation and Hypotheses	27
3.7.1	Aims	27
3.7.2	Hypothesis	27
4	Methodology	
4.1	Introduction	29
4.2	Method	29
4.3	Statistical Methods Employed	30
4.3.1	Univariate Analyses	30
4.3.2	Bivariate Analyses	31
4.3.3	Multivariate Analyses	31
4.4	Data	33
4.5	Hypotheses to be tested	34
4.6	Analysis Plan	34
4.7	Analytic Procedure	34
4.7.1	Understanding the Nature of Card-not-present Fraud	34

4.7.2	Exploring Correlates of Card-not-present Fraud	35
4.7.2.1	Online Correlates	35
4.7.2.2	Offline Correlates	36
4.7.3	The Effect of Fear of CNP Fraud and Past Victimization	36
4.8	Measurement	37
5	Results	
5.1	Introduction	38
5.2	The Online and Offline Correlates of Card-not-present Fraud	38
5.2.1	Online Correlates	38
5.2.1.1	Exposure to Motivated Offender	38
5.2.1.2	Target Suitability	43
5.2.1.3	Absence of Capable Guardianship	45
5.2.1.4	Full Model	48
5.2.2	Online Identity Theft	50
5.2.3	Offline Correlates of Card-not-present Fraud Victimization	54
5.3	The Impact of The Fear of Crime and Past CNP Fraud Victimization	57
5.3.1	The Impact of The Fear of Crime and Past CNP Fraud Victimization on Online and Offline Behaviors	57
5.3.2	The Impact of The Fear of Crime and Past CNP Fraud Victimization on Guardianship Measures	59
6	Discussion	
6.1	Introduction	61
6.2	Nature of Card-not-present Fraud Victimization	61
6.3	Online and Offline Correlates of Card-not-present Fraud	62
6.4	The Relation Between Online Activities, Identity Theft and CNP Fraud Victimization	64
6.5	Offline Correlates of Card-not-present Fraud	66

6.6	The Effect of Fear of CNP Fraud Victimisation and Past Victimisation on Behavioural Adaptation	67
6.7	The Effect of Fear of CNP Fraud Victimisation and Past Victimisation on Guardianship Measures	68
7	Conclusions	
7.1	Conclusions and Policy Implications	71
7.2	Limitations and Recommendations for Future Studies	72
8	Appendices	
	Appendix A	74
	Appendix B	94
9	References	99

LIST OF TABLES

Number		Page
Table 5.1	Using Internet for Financial Activities	39
Table 5.2	Using Internet for Leisure/Social Activities	40
Table 5.3	Internet Related Factors	41
Table 5.4	Logistic Regressions for Exposure to Motivated Offender	42
Table 5.5	Bivariate Target Suitability	44
Table 5.6	Binary Logistic Regression Model for Target Suitability	45
Table 5.7	Bivariate Digital Guardianship	46
Table 5.8	Bivariate Personal Guardianship	47
Table 5.9	Binary Logistic Regression for Guardianship	48
Table 5.10	Binary Logistic Regression for all Online Components	50
Table 5.11	Binary Logistic Regression for all Online Components with Control Variables	50
Table 5.12	Relation Between Online Activities and Online Identity Theft	52
Table 5.13	The Relation Between Online Activities and Online Identity Theft	53
Table 5.14	Relation Between Online Identity Theft and Card-not-present Fraud Victimisation	54
Table 5.15	Offline Correlates of CNP Fraud	55
Table 5.16	Binary Logistic Regression Model for Offline Correlates of CNP Fraud	56
Table 5.17	Binary Logistic Regression Model with Control Variables for Offline Correlates of CNP Fraud	56
Table 5.18	Logistic Regression Model for The Effect of Fear of CNP Fraud Victimisation and Past Victimisation on Behaviours	58

Table 5.19	Binary Logistic Regression Model for Online Guardianship	60
Table 5.20	Binary Logistic Regression Model for Offline Guardianship	60
Table A.1	Dependent Variables for Online Correlates of Card-not-present Fraud	75
Table A.2	Independent Variables for Exposure to Motivated Offender	77
Table A.3	Independent Variables for Target Suitability	79
Table A.4	Independent Variables for Absence of a Capable Guardianship	81
Table A.5	Control Variables	82
Table A.6	Dependent Variables for Online Identity Theft	86
Table A.7	Independent Variables for Online Identity Theft	83
Table A.8	Control Variables for Online Identity Theft	84
Table A.9	Independent Variables for Online Identity Theft	85
Table A.10	Independent Variables for Offline Correlates of CNP Fraud	86
Table A.11	Dependent Variables for Fear of CNP Fraud and Previous CNP Fraud Victimisation-Behaviours	88
Table A.12	Independent Variables for Fear of CNP Fraud and Previous CNP Fraud Victimisation-Behaviours	89
Table A.13	Control Variables for Fear of CNP Fraud and Previous CNP Fraud Victimisation-Behaviours	90
Table A.14	Dependent Variables for Fear of CNP Fraud and Previous CNP Fraud Victimisation-Guardianship	92
Table A.15	Independent Variables for Fear of CNP Fraud and Previous CNP Fraud Victimisation-Guardianship	93
Table A.16	Independent Variables for Fear of CNP Fraud and Previous CNP Fraud Victimisation-Guardianship	93
Table B.1	CNP Fraud Victimisation Rates	94
Table B.2	Amount of Money Lost	95
Table B.3	Demographics of the Credit Card Users	96
Table B.4	Reporting Behaviour of Card-not-present Fraud Victims	97

Table B.5	Emotional Effect of CNP Fraud	98
Table B.6	Fear of CNP Fraud Victimisation	98



LIST OF FIGURES**Number**

1	Card-not-present Fraud Losses	2
2	Comparison of Plastic Card Usage and CNP Fraud Victimization	2
3	Comparison of CNP Fraud and Counterfeit Fraud	3
4	Online Market in European Union	7
5	E-commerce Sales in the UK	8
6	Card-not-present Fraud Process	10
7	Counterfeit Card Fraud Losses on UK-issued Cards	13
8	Hypotheses	28

CHAPTER 1**Introduction****1.1 Introduction**

It is a cliché; though true, to say that the Internet has affected every aspect of our lives. As Bargh and McKenna (2004, p.574) argue, the Internet has become a “natural background” of our daily routines. The Internet, which is global, informational and networked (Wall, 2007), has not only transformed the way we live, but it has also transformed the way we are victimized (Yar, 2006; Wall, 2010). The transformative effect of the Internet has given birth to a new genre of crimes such as phishing, spamming, hacking and cracking; yet, it has also transformed the nature of conventional crimes such as card-not-present fraud (Smith, 2000; Grabosky and Smith, 2001; Wall, 2007). However, little is known about card-not-present fraud and it is not clear what online and offline factors cause card-not-present fraud victimization of individuals.

Card-not-present fraud, which can be defined as unauthorized use of payment cards in the absence of physical payment card (Montague, 2010), has adverse effects at the individual and macro level, namely banks, financial institutions (Lawrence and Tar, 2010; Becker et al., 2014). Card-not-present fraud related losses in UK are more than doubled from 30% in 2004 to 69% in 2014 and losses rose from 150.8 million £ to 331.5 million £ for the same period (Figure 1a and 1b). Although the number of credit cards increased steadily, the number of victims showed fluctuations over the same period, which implies that the increase in the number of credit cards does not account for the increase in the victimization rate (Figure 2). On the other hand, as The Figure 3 illustrates, whereas card-not-present fraud (remote purchase fraud) victimization increased nearly 16%, counterfeit (skimmed/cloned) card fraud victimization decreased approximately 73% from 2008 to 2014. The possible explanation of these changes will be discussed in Chapter 2. As statistics illustrate, card-not-present fraud is

a growing issue and many credit card users suffer its financial and emotional effects (Button et al., 2009a).

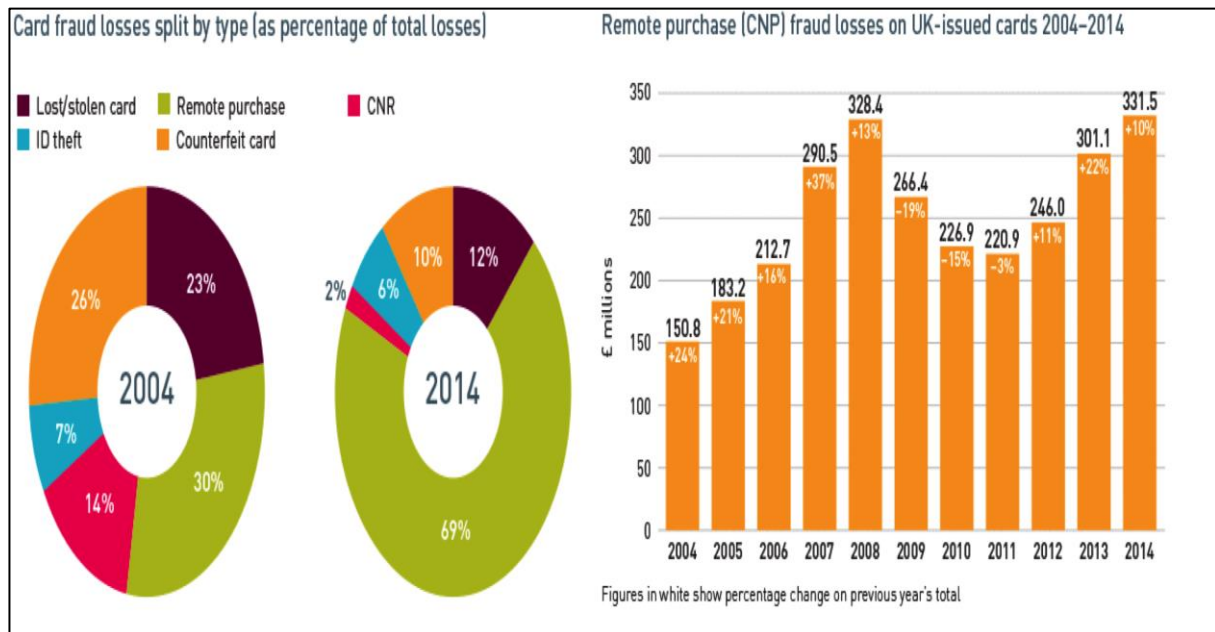


Figure 1a: Losses in percentages
(Source: UK Cards Association)

Figure 1b: Losses in numbers

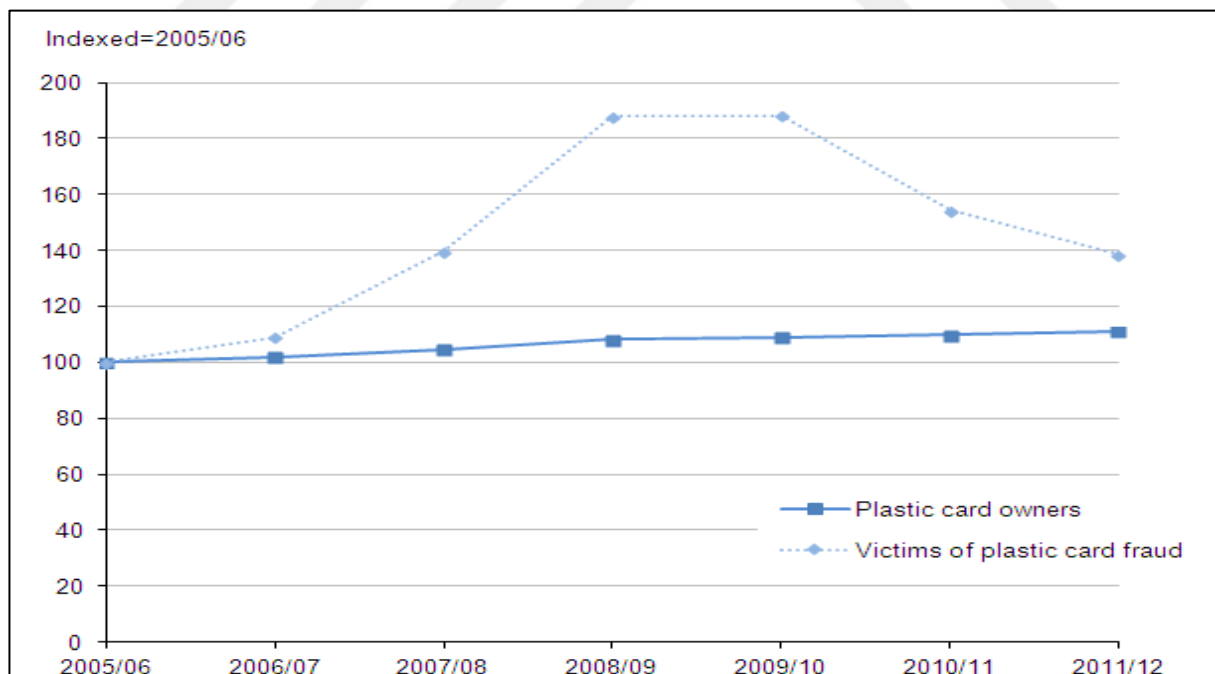


Figure 2: Comparison of Plastic Card Usage and CNP Fraud Victimization
(Source: Office for National Statistics, Plastic Card Fraud Report, 2013)

Card fraud type	2008	2009	2010	2011	2012	2013	2014
Remote purchase fraud	875,086	824,736	733,145	709,402	750,200	951,998	1,019,146
Counterfeit (skimmed/cloned) fraud	371,442	177,430	96,861	81,112	98,322	101,109	99,279

Figure 3: Comparison of CNP Fraud and Counterfeit Fraud
(Source: UK Cards Association)

The fear of card-not-present fraud can be regarded as a significant issue. One dimension of the emotional impact of card-not-present fraud is named as the fear of card-not-present fraud. Croall and Levi (1999) argue that the emotional effects of fraud victimisation might sometimes be more severe than violent crimes. Embarrassment, self-blame and anger are the most common emotions that fraud victims suffer (Mayhew, 1993; Titus and Gover, 2001). Past fear of crime studies, which will be examined in Chapter 3, indicate that fear of crime causes some behavioural adaptations such as not going out jogging after dark or protective responses such as buying a gun, putting alarms (Miller, 2002; Casten and Payne, 2008; Brant, 2009; Sreetheran and van den Bosh (2015).

Although criminologists' interest in fear of online crime has increased recently, empirical studies are limited to relation between fear of crime, perceived risk of victimisation and past victimisation (Reisig et al., 2009; van Wilsem, 2011; Henson et al., 2013); yet, Reyns (2013) researched the relation between identity theft and perceived risk of victimisation. Unfortunately, what is not yet clear is the impact of fear of card-not-present fraud and past CNP fraud victimization on individuals' online and offline behaviours and protective and preventive behaviours, namely guardianship measures.

Although Wolfgang conducted the first victimisation studies in the 1950s (Wolfgang, 1957 and 1958), it was after the introduction of two ground-breaking victimisation theories, Lifestyle-exposure (Hindelang et al., 1978) and Routine Activities Theory (Cohen and Felson, 1979) that victimisation and the role of the victim in the occurrence of crime received

considerable attention (Meier and Miethe, 1993). The intention of two aforementioned theories is to offer a systematic approach to explain victimisation rather than putting blame on victims. Later, Clarke (1995) proposed a situational crime prevention approach, which is informed mainly by Routine Activities Theory. The situational crime prevention approach proposes that crimes can be prevented or reduced should the conditions and opportunities that lead to victimisation be controlled or reduced (Clarke 1995; 1997). The idea of “highly specific forms of crime” is at the heart of this perspective (Clarke, 1995, p.93). This means that the success of this approach lies in focusing on specifications of every type of crime individually. For instance, rather than studying correlates of cybercrime, examining card-not-present fraud. Clarke (1997) and Newman and Clarke (2013) argue that situational crime prevention approach is applicable to cybercrimes and card-not-present fraud can be prevented should the opportunities be blocked. This dissertation will therefore adopt a situational crime prevention method informed by Lifestyle-Routine Activities Theory (LRAT), in order to find out online and offline activities that lead card-not-present fraud victimisation.

1.2 Structure of Dissertation

Together with this introductory chapter, this dissertation is composed of seven chapters. The second chapter begins by defining cybercrimes and card-not-present fraud and continues with explaining the process of victimisation and concludes with discussing theoretical dimensions of this dissertation. The third chapter is concerned with review of literature and the fourth chapter deals with the methodology adopted for this dissertation. The fifth section presents the results of the analyses conducted to test the hypotheses. The sixth chapter bears a discussion of the findings in the light of Life-style Routine Activities Theory. Finally, the conclusion chapter provides a summary of this dissertation and policy implications of the findings as well as limitations. This chapter finishes with recommendations for future research in this area.

CHAPTER 2**Background****2.1 Introduction**

Although the Internet was created for communication between researchers and military bodies (Leiner et.al, 2009), its commercial use after 1990s was a real breakthrough (Mowery and Simcoe, 2002). However, this feature of the Internet is not free from its secondary effects, such as facilitating card-not-present fraud, which will be discussed in this chapter. Firstly, the definition and classification of Cybercrimes will be given. Secondly, the typology and process of card-not-present fraud will be presented before demonstrating the relationship between Identity theft and card-not-present fraud. And then, fear of online crime will be defined and the effect of fear of online crime on victimisation will be discussed. Finally, the theoretical framework of this dissertation will be explained.

2.2. Cybercrime**2.2.1 Definition of Cybercrime**

Finding a conceptual or working definition of cybercrime is one of the debates in cybercrime literature. The main drive behind producing a working definition of cybercrime lies in the intention of controlling criminal activities in cyberspace (Wall, 2007; Yar, 2006). Law, technology and social norms are three perspectives used by scholars or institutions to define cybercrime. Whereas some scholars stress the illegality of activities (Brenner, 2010; Akdeniz, 2000; Rho, 2007), others emphasize the role of computer and Internet technology (Shiple and Bowker, 2013; Clough, 2010; Kowalski, 2002) in the occurrence of crime. Other scholars (Thomas and Loader, 2000a; Wall, 2007) include illicit activities in their definitions of cybercrime. Kshetri's (2009, p.1; 2010, p.3) broad definition appears to be the most exhaustive one. He defines cybercrime as "a criminal activity in which computers or

computer networks are the principal means of committing an offense or violating laws, rules, or regulations”.

2.2.2 Classification of Cybercrimes

There seems to be a general agreement about the classification of cybercrime around categorization of the Council of Europe's convention on Cybercrime (The Council of Europe ETS.No.185, 2001). Scholars such as Yar (2006), Wall (2007) and Brenner (2010) seem to be inspired by this classification when categorizing cybercrimes:

1. **Computer Integrity Crimes:** This category encompasses crimes that are related to illegal access to computers or use of personal data (e.g. hacking)
2. **Computer-Assisted Crimes:** This category includes crimes that are committed with the help of computers or Internet Technologies (e.g. Frauds)
3. **Computer Content Crimes:** This category covers crimes related to dissemination of obscene materials (e.g. child pornography).

The Literature Review Chapter will be framed according to this classification of cybercrimes.

2.3 Card-not-present Fraud

E-commerce, which is the trade of goods, products and services over the Internet (Turban et al., 2015), is one of the fastest growing industries in the world (Shabir et al., 2014). Emarketer (2014) estimates that e-commerce sales have reached \$ 1.316 trillion and this was accounted for 5.9% of total trade worldwide in 2014. It is forecasted that e-commerce sale will make up 8.8% of total sales in 2018 (Emarketer, 2014). The UK has the biggest market share in the e-commerce sector in the European Union. E-commerce sales in UK constitute 20% of business turnover (Office for National Statistics Statistical Bulletin, 2014), which

account for £557 billion in 2013. As Figure 5 indicates, there is an increasing trend in e-commerce sales in UK, an increase of £ 222 billion (%66) in the last five years.

The prevalence of e-commerce has boosted the popularity of credit card usage dramatically (Schneider, 2011; Turban et.al, 2015). Over the past ten years, credit cards have become most preferred payment method. Credit card payments accounted for 75% of all spending of the retail sector in the UK, which makes the UK biggest credit card payment market in the European Union (Curphey, 2015) (Figure 4). Online usage of credit cards has risen 66.1% when compared to 2008, reaching £68.4 billion in 2012. Interestingly, this increase in online credit card usage is analogous to the increase in figures of e-commerce for the same period, which was described above. This similarity seems to confirm the effect of e-commerce on popularity of credit cards. However, this growth in e-commerce and credit card sector is not free from problems. Card-not-present fraud has become an important issue in e-commerce.

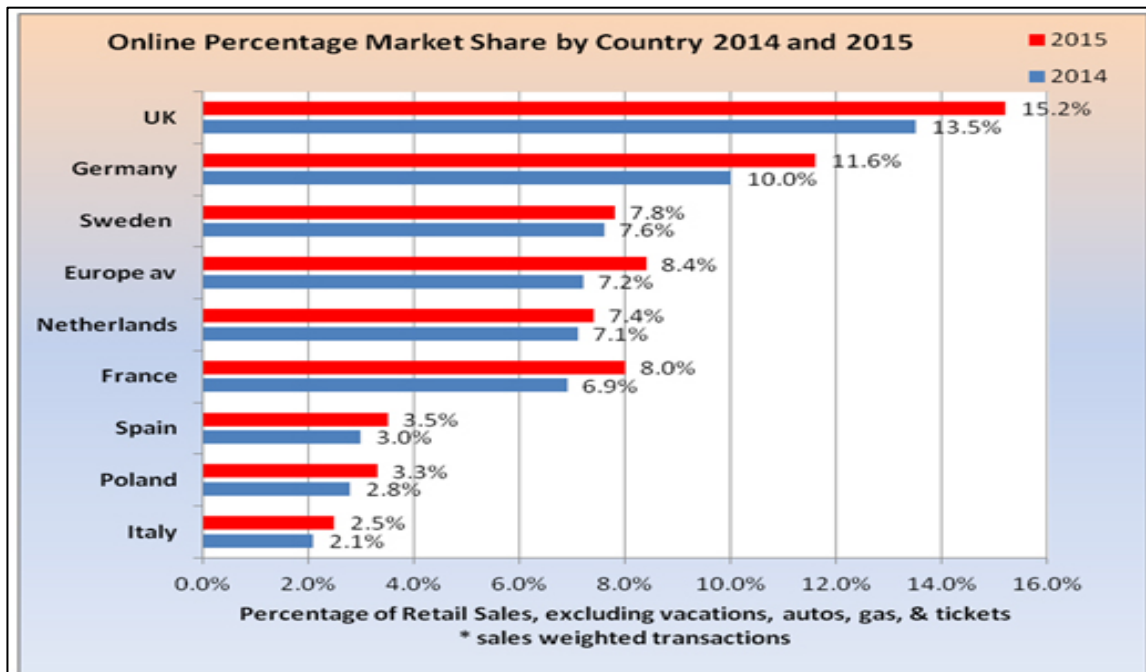
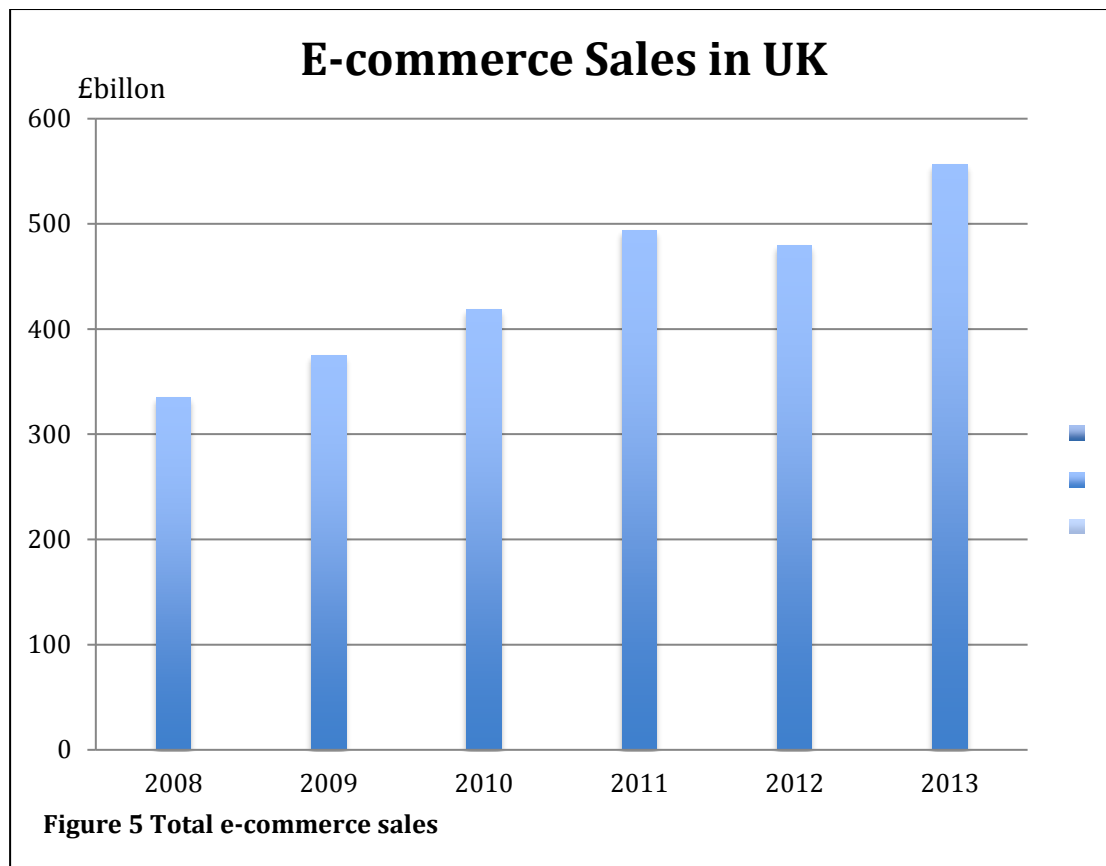


Figure 4: Online Market in European Union
(Source: Centre for Retail Search)



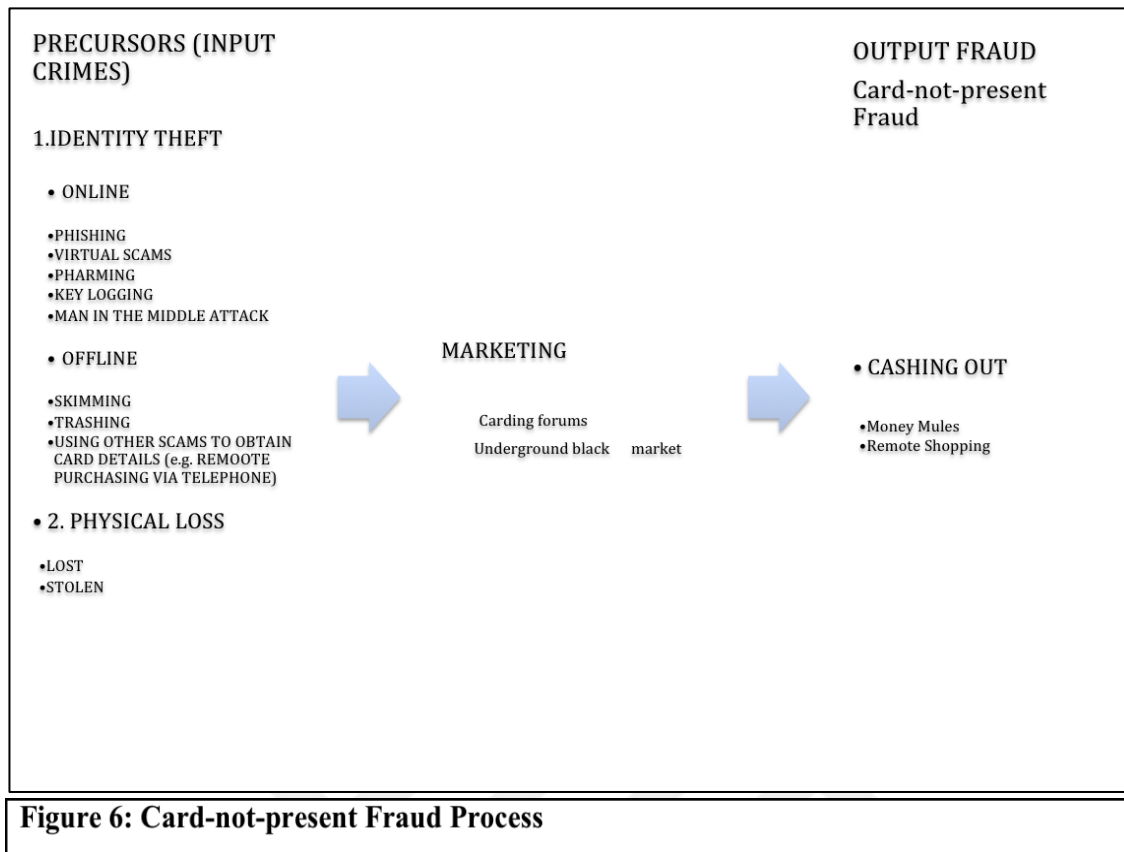
2.3.1 Typology of Card-not-present Fraud

Card-not-present fraud has two distinct attributes, being a hybrid and output crime. Wall (2007) classifies frauds as a hybrid or second-generation cybercrime as frauds can be committed in both cyberspace and real world. Following this line of logic, card-not-present fraud may be regarded as a hybrid cybercrime as the perpetrators can use stolen credit card information via the Internet or telephone. Wall (2007) conceptualizes three generations of cybercrimes. Whereas first generation cybercrimes act as a secondary or tertiary tools to assist conventional crimes such as bank robbery, second generation cybercrimes create new opportunities for perpetrators (e.g. enabling fraudsters access personal information of a person who lives in another country). The third generation cybercrimes are those that could only be committed in cyberspace, for instance, spamming can online be committed via networked technologies. Based on this classification, card-not-present fraud can be considered as a second-generation cybercrime since the Internet created many opportunities for fraudsters

such stealing card details via infected computers or selling stolen credit card detail in online black markets (Thomas et al, 2014; Bulakh and Gupta, 2015). Secondly, card-not-present fraud may be considered as an output cybercrime since it requires the use of illegally obtained credit card details over the Internet or telephone, which is a process that it will be discussed below.

Card-not-present fraud, rather than being a result of one single event, is an outcome or the last stage of a process (Howard, 2009). As can be seen in Figure 6, the process begins with input activity, such as identity theft, or physically loss of cards and ends with card-not-present fraud, which encompass cashing out the money or goods. The first stage of this process is the main focus of this study since victims' actions or lifestyle may facilitate the fraudulent process, which is named as victim precipitation (Smith and Bouffard, 2014). This stage is made up of two main input crimes, or illegal activities: identity theft and physical loss of credit card. Since the physical loss of card, either stolen or lost, has nothing to do with cybercrime or victim precipitation identity theft, which can be defined as "misuse of another individual's personal information to commit fraud" (Copes and Vieraitis, 2009, p.565) will be examined in details.

Identity theft is the key factor in understanding the role of victim precipitation in card-not-present fraud. Identity theft is a multi-faceted generic or umbrella term that covers the different meaning of identity (Wall, 2013; Smith, 2010). However, discussing these different aspects is beyond the scope this study (see Wall, 2013; Smith, 2010; Finch, 2009; Sproule and Archer, 2007 for detailed discussion of different aspects of identity theft and identity fraud).



2.4 Identity Theft

Identity theft is a rapidly growing issue and it not only endangers e-commerce but it also poses a barrier for online credit usage (Roberts et al., 2013). According to The Bureau of Justice Statistics (BJS) Bulletin (2012) approximately 6% of adults experienced identity theft and unauthorised access or use of personal financial details, which accounts for 85% of these incidents in the US in 2012. The situation is not different in the UK, where 8.8 % of adults were the victims of identity theft in 2012 (National Fraud Authority, 2013).

Cybercriminals direct their attacks to two main sources, namely companies or institutions that hold costumers' financial details and individuals, to acquire financial details of credit card users. The increasing popularity of alternative payment methods such as e-wallet, where credit card or debit card details are registered in private companies' databases, boosted the fraudsters' interest in these companies' databases as well as banks' records

(Schneider, 2010; Turban et al., 2015). Sony PlayStation (Reuters, 2011), Citibank (BBC, 2011) and JP Morgan Chase (The guardian, 2014) attacks occurred in 2011 are the most notorious examples of cyber-attacks, which targeted institutions rather than individuals.

With regards to individuals, identity theft may occur in both worlds (Schell and Martin, 2004). Whereas phishing, pharming, key logging, man in the middle attack and virtual scams are the most common methods of identity theft on the online environment, skimming, trashing and using other scams are the most favoured techniques used in the real world.

2.4.1 Identity Theft in Cyberspace

Phishing, pharming and man-in-the-middle attacks share the same logic: diverting Internet users to bogus websites. Yet, their methods differ. Phishing, a hacker terminology coined in 1990s, heavily depends on email users' response to fraudulent emails (Symantec, 2014). Whereas phishing uses logos, names of financial institutions to persuade email users to click on the link provided by fraudsters (Jagatic et al., 2007), pharming depends on clandestinely installed malicious software or virus to divert users to bogus website (Pathak et al., 2015). Hence, phishing heavily depends on social engineering to deceive email users (Wall, 2013; Whitman and Mattord, 2011). Burgard and Schlmebach (2013, p.114) argue that it is people's "private interest" such as free software, which makes them a suitable prey for fraudsters. The Pharmers usually use freely distributed software (Brody et al., 2007) or software updates and patches, which is called "Trojanized Software Update" (Symantec, 2015, p.6) to infect computers. The recent IBM report (IBM Security Intelligence Report, 2015) indicates that "inadvertent actors" play an important role in data breaches.

On the other hand, man-in-the middle attack, the most sophisticated form of identity theft, uses both phishing and pharming to acquire financial information. However, man-in-the

middle attack is slightly different from pharming, since whereas pharming requires Internet users to enter financial details into bogus website, man-in-the-middle-attack may also include real-time interception of personal data that are entered in the real website (Hong, 2012).

Virtual Scams, which attract Internet users' attention with offers or discounts, is another method used to obtain credit card details (Wall, 2010). For instance, fraudsters create a website that offers a cheap holiday or discount (Moore, 2015) or build a gaming website which sells popular game characters (Narcisse, 2015) to either obtain credit card details or infect machines with malware. The literature implies that most of the online identity theft techniques rely on Internet users' reckless online actions. Hence, this study will endeavour to explore online behaviours that facilitate CNP fraud victimisation.

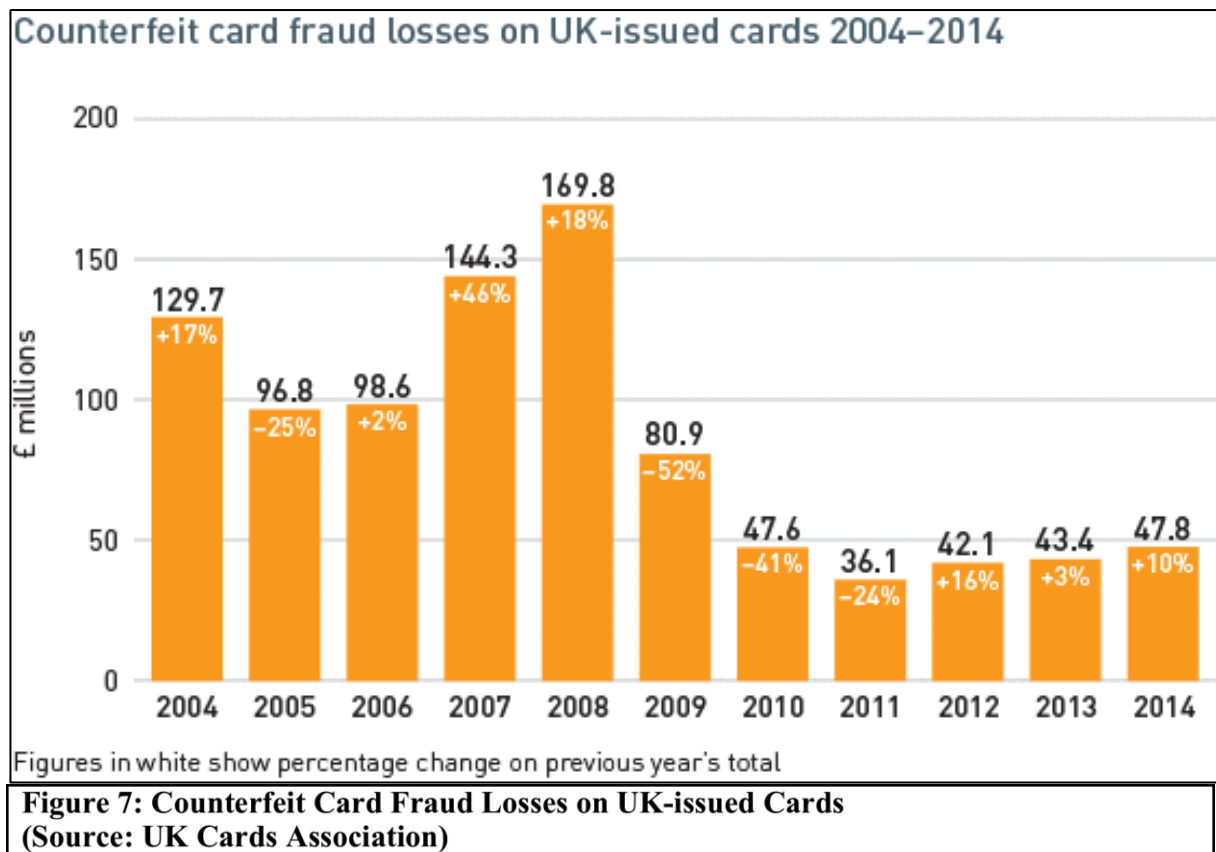
2.4.2 Identity Theft in “Meatspace¹”

Skimming, trashing and using other scams as facilitator are the most favoured offline methods that fraudsters use to obtain credit card details. Skimming, a method that involves cloning data on the magnetic strip and capturing PIN number (Bhatla, 2003), was once the most preferred method to capture credit card details, however, the introduction of the EMV standard (Europay, MasterCard, Visa) (EMV) or Chip and PIN decreased the popularity of this technique severely (Wall, 2010; Kosse, 2013; Valentine, 2013). The UK Cards Association's latest report (The UK Cards Association Report, 2014) supports this proposition of decrease (Figure 7).

Terrestrial scams are also used to gain credit card information by fraudsters (Judge et al., 2005). Empirical research confirms this proposition of facilitation: Telemarketing fraud (PolICASTRO and Payne, 2014; Holtfreter et al., 2015) and free prize scam (Titus, 1995) are examples of this kind of facilitation. Advance fee fraud, which is known as Nigerian 419

¹ Meatspace, which refers to the real world, is coined by Pease (2001, p.24)

since the Nigerian Penal Code of fraud is 419 (Dyrud, 2005), is one of the most frequently used scams. Fraudsters contact people usually via email to propose a high return a result of help to move the large sum of money from abroad (Tive, 2006). Fraudsters began their scam with asking a small amount of money or financial details for transferring money and the process end with a huge sum of lost money.



To sum up, identity theft appears to be the most significant input crime for card-not-present fraud. As Clarke (1995, 1997) and Clark and Newman (2013) advice dealing with crime specific conditions would enable us to perceive the nature of crimes under examination. Thus, revealing the role of identity theft would help us to explore online and offline correlates of card-not-present fraud.

2.5 Fear of Online Crime

Fear of crime, which encompasses “feelings, thoughts, and behaviours, all of which are focused on the subjectively conceived threat of criminal victimization” (Jackson and Gouseti, 2014, p. 1), bears diverse range of meanings. As Warr (1984) argues, this diversity sometimes creates confusion among researchers, which can be seen from their operationalization of fear of crime. In order to prevent this confusion, Ferraro (1995) highlights a distinction between fear of crime and perceived risk of victimisation. Whereas fear of crime involves emotional reactions to fear, the latter encompasses cognitive assessments of chance of being victimised (Ferraro 1995; Hale, 1996). This means that fear of crime has some emotional effects such as anxiety and isolation (Bernard, 1992; Skogan, 1986a); however, perceived risk of victimisation does not necessarily have an impact on people’s reactions (Renfigo and Bolton, 2012). This dissertation will follow Ferraro’s (1995) distinction and apply fear of crime measures to investigate the effect of fear of card-not-present fraud victimisation on individuals’ behaviours and protective actions.

2.6 Theoretical Framework

Two victimisation theories, Lifestyle Routine Activity Theory (Cohen and Felson, 1979; Hindelang et al., 1978) and Low-self-control, have largely been applied to recent victimisation studies as a theoretical framework (Van Wilsem, 2013; McNeely, 2014). Opportunity theories, namely Routine Activity Theory and Lifestyle-Exposure theory, shifted the attention from the offending behaviour to victims’ lifestyle and routine activities, which proposed to prepare suitable conditions for crime. This approach was a real challenge for criminologist who sought remedy in examining the offending behaviour (Meier and Miethe, 1993). Routine Activities perspective postulates that the motivated offender, the suitable target and the absence of capable guardian are three minimal elements for a crime to occur

(Hindelang et al., 1978; Cohen and Felson, 1979). These elements, which are explained below, are necessary conditions for a crime to occur; hence controlling these conditions may prevent victimisation (Miethe and Meier, 1990; Mustaine and Tewksbury, 1998).

Exposure and Proximity to Motivated Offender: Whereas exposure refers to “physical visibility and accessibility” of victims, proximity refers to “physical distance” between motivated offender and victims (Cohen et al., 1981, p.507). Due to the nature of the cyberspace, victims do not expose themselves to the perpetrators physically and there is no physical distance between offenders and victims in the online environment. However, victims are in close proximity to offenders’ tools rather than physical existence (Bossler and Holt, 2011), hence, the proximity to the motivated offender is zero in the Cyberspace (Yar, 2005). Whereas victims expose themselves in conventional street crimes, victims usually expose their personal information to the perpetrators in cyberspace. The Internet users online behaviours and life-styles increase the exposure to the motivated offender and put themselves in closer proximity to motivated offenders’ tools (Pratt et al., 2010; Reyns 2011; Holt and Bossler, 2013; van Wilsem 2013).

Suitable Target: Cohen and Felson (1979) argue that some specific features of a target value, inertia, visibility and accessibility, known as VIVA, increase the target attractiveness. Later Clarke (1999) based on these characteristics of a target, created a model called CRAVED, concealable, removable, available, valuable, enjoyable and disposable. Clarke (1999, p.V) dubbed the targets that have these qualifications as “hot products”, which are the items that are mostly preferred by thieves. These hot products can be cars, jewellery or money in the real world; however, the hot product of cyberspace is information such as credit card numbers (Newman and Clarke, 2013). Since the target attractiveness of personal information is high in online environment, fraudsters seek suitable targets in cyberspace and

Internet users' some of online behaviours and online life-style increase target suitability (Holt and Bossler, 2013).

Absence of a Capable Guardian: Cohen et al (1981) define guardianship as the capability of the persons or things to prevent crime. Whereas the guardians in the real world can be police officers, family members or alarms, the guardians in cyberspace are anti-virus programs, firewalls, or personal security measures such as checking the security signs of a website.

Lifestyle Exposure Theory (Hindelang et al., 1978) assumes that changes in crime rate may be attributed to the victims' demographics, which causes differences in lifestyles (Sampson and Wooldredge, 1987; Miethe et al., 1987). Risky lifestyles lead individuals to engage in activities that increase the risk of victimisation. Later, Cohen et al (1981) implicitly combined two theories in their research and since then these two theories have been used in tandem. Lifestyle Routine Activities theory has been applied to explain different kinds of victimisation: violent victimisation (Bouchard et al., 2012; Bunch et al., 2012), sexual assault (Fisher et al., 2010;) burglary victimisation (Cohen and Cantor, 1981; Kennedy and Forde; 1990; Miethe and McDowall, 1993) are only a few examples of the huge amount of victimisation studies that applied LRAT as theoretical framework.

It was Grabosky (2001) and Pease (2001) who firstly proposed that Routine Activities Theory might be applicable to online crimes (See Yar (2005) and Tillyer and Eck (2009) for opposing views). Since then LRAT perspective has been widely used in cybercrime studies; however, recently some scholars (Bossler and Holt, 2010; Holtfreter et al., 2008) use Low Self-Control Theory (Gottfredson and Hirschi, 1990) as theoretical framework in cyber victimisation studies. Gottfredson and Hirschi (1990) argue that low self-control may increase the likelihood of engaging with criminogenic activities due to impulsive decisions. Although this theory was not proposed to explain victimisation, Schreck (1999) was the first to apply

this approach to victimisation studies. Schreck (1999) claims that low self-control can account for victimisation, since victims and offenders share some common traits. Although cyber offending studies such as cyber piracy, hacking have found empirical support (Higgins and Makin, 2004; Holt and Bossler, 2012; Bossler and Burruss, 2010; Malin and Fowers, 2009), victimisation studies (Averdijk and Loeber, 2012; Bossler and Holt, 2010) have found partial support for applicability of low self-control to victimisation.

Low self-control may sometimes be a cause of victimisation; however, it fails to account for victimisation in general. One major drawback of this approach is that it confines causes of victimization to only low self-control, yet, there should be other factors that facilitate victimisation. Another problem with this approach is that it fails to take the effect of lifestyle and daily activities into account.

On the other hand, Lifestyle Routine Activities Theory provides a more systematic approach for victimisation studies. Its situational crime prevention perspective may also enable us find out necessary conditions for card-not-present fraud victimisation, which may provide valuable information for policy makers and policing bodies. Therefore, this dissertation will adopt Lifestyle-Routine Activities Approach as a theoretical framework.

Overall, Cohen and Felson (1979) and Hindelang (1981) argue that individuals' lifestyles and routine actions increase the risk of victimisation. Situational Crime Prevention Approach (Clarke, 1995) proposes that "opportunity-reducing measures" (Clarke, 1997, p.4) would decrease the risk of victimisation by controlling conditions. However, to implement these measures, opportunities that prepare suitable conditions for a crime should be detected according to each specific type of crime (Felson and Clarke, 1998). Hence, it is important to determine which online and offline behaviours contribute to victims' precipitation. The Internet is used for a variety of reasons (shopping, online banking, communication and leisure) and many different devices are used to access the Internet (e.g. laptop, desktop,

handheld computer and smartphone and mobile phone). The security measures taken by Internet users are also important factors in the occurrence of cybercrimes. When all of these factors come together they may prepare suitable conditions for card-not-present fraud. The perpetrators also use terrestrial scams to gain credit card details. Responding terrestrial scams such as Nigerian 419 may also facilitate card-not-present fraud victimisation. Based on these considerations, the main focus of this dissertation is to find out online and offline factors that contribute to victimisation.



CHAPTER 3**The Review of Literature****3.1 Introduction**

This section will review the cybercrime literature critically. The first part of the review will deal with online victimisation studies. Offline fraud victimisation studies will be presented in the second part and then online fraud victimisation studies will be discussed in the third section. Fear of online crime studies will be reviewed in the fourth part before discussing the effects of actions in both domains on victimisation in the fifth part.

3.2 Online Victimization

Cybercrimes are generally divided into three categories, computer content crimes, computer integrity crimes and computer assisted crimes (Wall, 2007; Brenner, 2010). Past online victimisation studies will be reviewed according to this classification.

Ngo and Paternoster (2011) and Choi (2008, 2011) researched different types of online victimisation in one study. These studies found that whereas the risky online life style increased the risk of victimisation, legitimate online activities had no effect on victimisation. Results pertaining to guardianship measures were rather contradictory. While Choi (2008, 2011) found that using computer software decreases the risk of victimisation, Ngo and Paternoster (2011) and Holt and Bossler (2013) found that using computer software increases the risk of victimisation. These inconsistent results may be attributed to design of researches, which examine different types of online crime with the same independent variables. Studying distinct crimes with same predictive online behaviours may have decreased the exploratory power of two aforementioned researches.

3.2.1 Computer Content Crimes

Extant researches indicate that physical and personal guardianship measures have different impact on preventing computer content crime victimisation. Whereas physical guardianship measures such as anti-virus software, have no effect on preventing online harassment or cyber-bullying victimisation (Marcum (2008, 2011; Marcum et al., 2010), the existence of a teacher or peer while using the Internet was found to decrease the risk of receiving online sexual harassment (Marcum 2008, 2011). Yet, Reyns et al (2011) found that using a profile tracker increases the risk of victimisation. These studies appear to suggest that whereas social guardianship efforts are effective in preventing interpersonal cybercrimes, digital guardianship measures do not have an effect on preventing such online crimes (van Wilsem, 2013). Both legitimate online activities such as sharing photos on online social media, updating status on social media frequently (Reyns et al., 2011), shopping online and using chat rooms (Marcum et al., 2010) and deviant online behaviours such as harassing others or illegal download increased the risk of computer content crime victimisation.

3.2.2 Computer Integrity Crimes

Bossler and Holt (2009, 2011) and Holt and Bossler (2013) studied the effect of the online lifestyle on malware infection. Whereas legitimate online activities such as shopping online, playing video games or using social media had no significant effect on malware victimisation; deviant online behaviours, namely pirating software or illegal downloading, were strongly associated with malware infection.

However, their results pertaining to guardianship were somewhat contradictory. Bossler and Holt (2009, 2011) found that neither personal guardianship such as computer skills and careful password management nor physical guardianship such as the anti-virus program significantly correlated with malware victimisation; yet, Holt and Bossler (2013)

found that physical guardianship, using anti-virus software decreased the risk of victimisation but personal guardianship, such as the high level of Internet skills, was negatively associated with victimisation.

3.2.3 Computer Assisted Crimes

Hutchings and Hayes (2009) researched phishing victimisation and Reynolds (2013) studied identity theft victimisation. Reynolds (2013) used data of British Crime Survey 2008/2009, but due to the unavailability of Internet security questions, he only studied the effects of online behaviour on identity theft. His research revealed that online legitimate behaviours such as shopping online, using the Internet for banking/managing finances and using e-mails/instant messaging as well as illegitimate online behaviour, downloading music or movies, were emerged to increase the risk of identity theft victimisation.

Hutchings and Hayes (2009) found similar results, which indicate that legitimate online behaviours increase the risk of victimisation. However, they found that using physical guardianship measures such as phishing filters and firewalls increased the risk of phishing victimisation. This unexpected result may be attributed to the fact that security software sometimes creates the false sense of security (Ngo and Paternoster, 2011), which may lead Internet users to engage in more risky online activities.

3.3 Demographic Characteristics of Victims

Research findings related to demographics of online victims are rather contradictory. Reynolds (2013) found that those who were married have a paid job and have income higher than £50,000, were at the increased risk of being the victim of the identity theft. Age is positively correlated with victimisation, which means that older people are at more risk of identity theft. Bossler and Holt (2009, 2011) found that having a job and being female increased the

likelihood of being victim of malware infection; however, Holt and Bossler (2013) found that only being female was associated with malware infection victimisation. On the other hand, the study conducted by van Wilsem (2013) indicates that single and young people were more likely to be the victim of the online sexual harassment.

Overall, the findings of past online victimisation studies have shown that whereas proximity to the motivated offender and being a suitable target increased the risk of the victimisation regardless of the type of the online crime, guardianship element of theory yielded mixed results. This inconsistency may be attributed to the fact that each type of crime has its own characteristics, which may require a different kind of guardianship measures. Hence, situational crime prevention perspective proposes to focus on crime specific conditions to better understand the factors related to crime under examination (Clarke, 1997).

3.4 Offline Fraud Victimisation

Most of the offline victimisation studies aimed to find out demographic characteristics and reporting behaviour of fraud victims (Mason and Benson, 1996; Van Wyk and Mason, 2001; Holtfreter et.al, 2006; Policastro and Payne, 2014) but (Van Wyk and Benson, 1997; Schoepfer and Piquero, 2010).

Age emerged as one of the most common demographic characteristics of offline fraud victims. Contrary to public perception, age was negatively associated with fraud victimisation (Van Wyk and Benson, 1997; Titus et.al, 1995; Van Wky and Mason, 2001; Holtfreter, 2006; Schoepfer and Piquero, 2010); however, Mason and Benson (1996) and Policastro and Payne (2014) found no relation between age and fraud victimisation.

Risky financial actions (Van Wyk and Benson, 1997) and risky behaviour such as responding to an email to be eligible for a free prize, sharing PIN numbers with family

members over the telephone were associated with fraud victimization (Schoepfer and Piquero, 2010).

It is found that reporting rates of fraud were lower than other crime reporting rates (Copes et al., 2001, Button et al., 2009a). Several under-reporting reasons identified in literature: feeling of self-blame (Mason and Bason, 1996), embarrassment (Reed, 2005), the small amount of financial loss (Copes et al., 2001; McGuire and Dowling, 2013a) and distrust to authorities (Reisig and Holtfreter, 2007) are the most common reasons of under-reporting. The findings about the relation between reporting behaviour and demographics are somewhat contradictory. Whereas Schoepfer and Piquero (2010) found that males are more likely to report victimization, Van Wky and Mason (2001) and Mason and Bason (1996) found no relation between reporting behaviour and demographics.

3.5 Online Fraud Victimization

Online fraud victimisation (Holtfreter et al., 2008; Pratt et al., 2010, Button et al., 2014), credit card theft victimisation (Reisig et.al (2009), online advertisement fraud (Garg and Nilizadeh, 2013) online dating scams (Rege (2009) and online consumer fraud victimisation (van Wilsem, 2011) are the types of online frauds to be discussed.

Several online victimisation studies thus far have linked victims' precipitation with online fraud victimisation (Reisig et al., 2009; Holtfreter et al., 2008; Pratt et al., 2010; Wilsem; 2011 Button et al., 2014). Spending more time on the Internet to shop goods, checking online forums and having profiles on different social media websites (van Wilsem, 2011), remote online purchasing (Holtfreter et al., 2008), the amount of time spent online and shopping online (Pratt et al., (2010), responding dating scams (Rege, 2009) were increased the risk of online fraud victimisation.

Previous research has indicated that various demographic indicators have a significant impact on online fraud victimization. Age (van Wilsem, 2011; Pratt et al, 2010), gender (Holtfreter et al., 2008; Garg and Nilizadeh, 2013), marital status (Pratt et. al, 2010), educational level (Pratt et. al, 2010; van Wilsem, 2011; Garg and Nilizadeh, 2013), ethnicity (Pratt et. al, 2010; Garg and Nilizadeh, 2013) and employment status (Pratt et al, 2010) were correlates of online fraud victimisation. Whereas age was negatively correlated other demographics were positively correlated with victimisation. Schoepfer and Piquero (2010) found that age was a negative predictor of credit card fraud, which means that young people are at the increased risk of being the victim of credit card fraud.

Although some fraud victimisation studies researched credit card fraud victimisation within the general context of fraud victimisation (Schoepfer and Piquero, 2010; Bossler and Holt, 2010) only Reisig et al (2009) studied credit card fraud victimisation in separate research. Reisig et.al (2009) studied the effect of impulsivity and perceived risk of credit card theft victimisation on online behaviours. They conducted a telephone survey in Florida with 573 adult participants. Online purchasing and the amount of time spent online were the online behaviours that were under examination. They have found that those with the high level of perceived risk of victimisation avoided online purchasing and they decreased the time spent online. Yet, impulsive respondents did not alter their online behaviours. Individuals who belong to an ethnic minority and with lower SES were more prone to have high levels of risk perception.

The research revealed significant results about the effect of perceived risk of credit card fraud on online behaviours; however, they limited their research to two kinds of online behaviours, online purchasing and amount of time spent online. Moreover, they did not study the correlates of credit card theft victimisation.

3.6 Fear of Online Crime

The impact of fear of crime and past victimisation on behavioural adaptation and coping strategies is one of the most researched areas among criminologists (Hale, 1996; Renfigo and Bolton, 2012; Henson; 2013). Past research has found that previous victimisation has considerable effect on victims' behaviours (Rountree and Land, 1996, Dugan, 1999; Gale and Coupe, 2005; Warr, 2000). Whereas some scholars (Averdijk, 2011; Skogan and Maxfield, 1981, Rountree and Land, 1996) argue that victimization causes behavioural responses, others (Ferraro, 1995; Gale and Coupe, 2005) argue that past victimization experiences increase protective and preventive actions.

The direction of the impact is also another facet of controversy. For example, while Averdijk (2011) found that past victimisation resulted with the injury decreased the frequency of going out, Davis et al (2002) found that physical assault increased risky behaviours. Fear of crime researches also yielded mixed results pertaining to behavioural changes and coping strategies (Liska et al, 1988; Markowitz et al, 2001; Yin, 1980).

With regards to fear of online crime, privacy (Rust et al., 2002; Miyazaki, 2008; Xu and Gupta, 2009), fear of identity theft (Zwick and Dholakia, 2004; Milne et al., 2004; Indermaur and Spiranovic, 2013; Hille et al., 2015) and fear of financial loss (Swinyard and Smith, 2003; Hassan et al., 2006; Chang and Wu, 2012 and Dai et al., 2014) are identified as the main concerns affecting Internet users shopping behaviour. Studies have found that these concerns decrease online shopping (Saban et al., 2002; Forsythe and Shi, 2003; Forsythe et al., 2006; Lu and Yu-Jen Su, 2009; Kukar-Kinney and Close; 2010).

The relation between perceived risk of victimisation and online behaviour is another area of interest (Lieberman and Stashevsky, 2002; Reisig et. al., 2006; D'Alessandro et al., 2012; Henson et al., 2013). Lieberman and Stashevsky (2002) interviewed 465 adult respondents and found that perceived risk of card-not-present fraud and revealing personal

information was two main factors that decreased financial use of the Internet. Similarly, D'Alessandro et al (2012) found that high levels of perceived risk decreased online gemstone trade in the US. Reisig et al (2006) conducted a telephone survey in Florida with 573 adult participants. They have found that those with the high level of perceived risk of victimisation adopted or altered their online behaviours, namely online purchasing and time spent online. They have also found that individuals who belong to an ethnic minority and with lower SES were more prone to have high levels of risk perception. Henson et al (2013) studied the relation between fear of online crime, perceived risk and online victimisation. Low levels of fear of online crime were observed among participants. Perceived risk emerged to be the significant indicator of online crime and past online crime was positively correlated with fear of online crime.

The literature review appears to suggest that despite social, psychological and financial impacts, online fraud victimisation is understudied when compared to other types of cybercrimes such as cyber bullying and malware infection (Reisig et al., 2009; Schoepfer and Piquero, 2009; Pratt et al., 2010).

Overall, recent studies have shown that Internet users online behaviours as well as the medium used to access the Internet may contribute to their online victimisation (Bossler and Holt, 2010; Pratt et al., 2010; Holt and Bossler, 2013). A great deal is known about the correlates of online victimisation, namely online fraud, malware infection and identity theft; however, much less is known about the correlates of card-not-present fraud. Unfortunately, no previous study has investigated this phenomenon individually. It is not clear either how credit card users' online lifestyle affects the risk of being a victim of card-not-present fraud or the effect of responding to terrestrial scams such as telemarketing fraud on CNP fraud victimisation.

On the other hand, research to date has tended to focus on the interaction between fear of crime, perceived risk of victimisation and past victimisation, no single research has studied whether fear of card-not-present fraud cause behavioural adaptations and preventive actions or not. This dissertation will attempt to address these gaps in the literature.

3.7 Aims of the Dissertation and Hypotheses

3.7.1 Aims

The aims of this study are two-fold:

1. To find out online and offline correlates of card-not-present fraud.
2. To examine the effect of fear of card-not-present fraud and recent card-not-present fraud on credit card users' online and offline preventive behaviours.

3.7.2 Hypotheses

1. Internet users' online lifestyle, such as using online banking or online shopping cause identity theft and identity theft leads to card-not-present fraud victimisation.
2. Fear of card-not-present fraud and recent card-not-present fraud victimisation not only cause behavioural adaptation but also preventive actions such as shopping from secure sites.

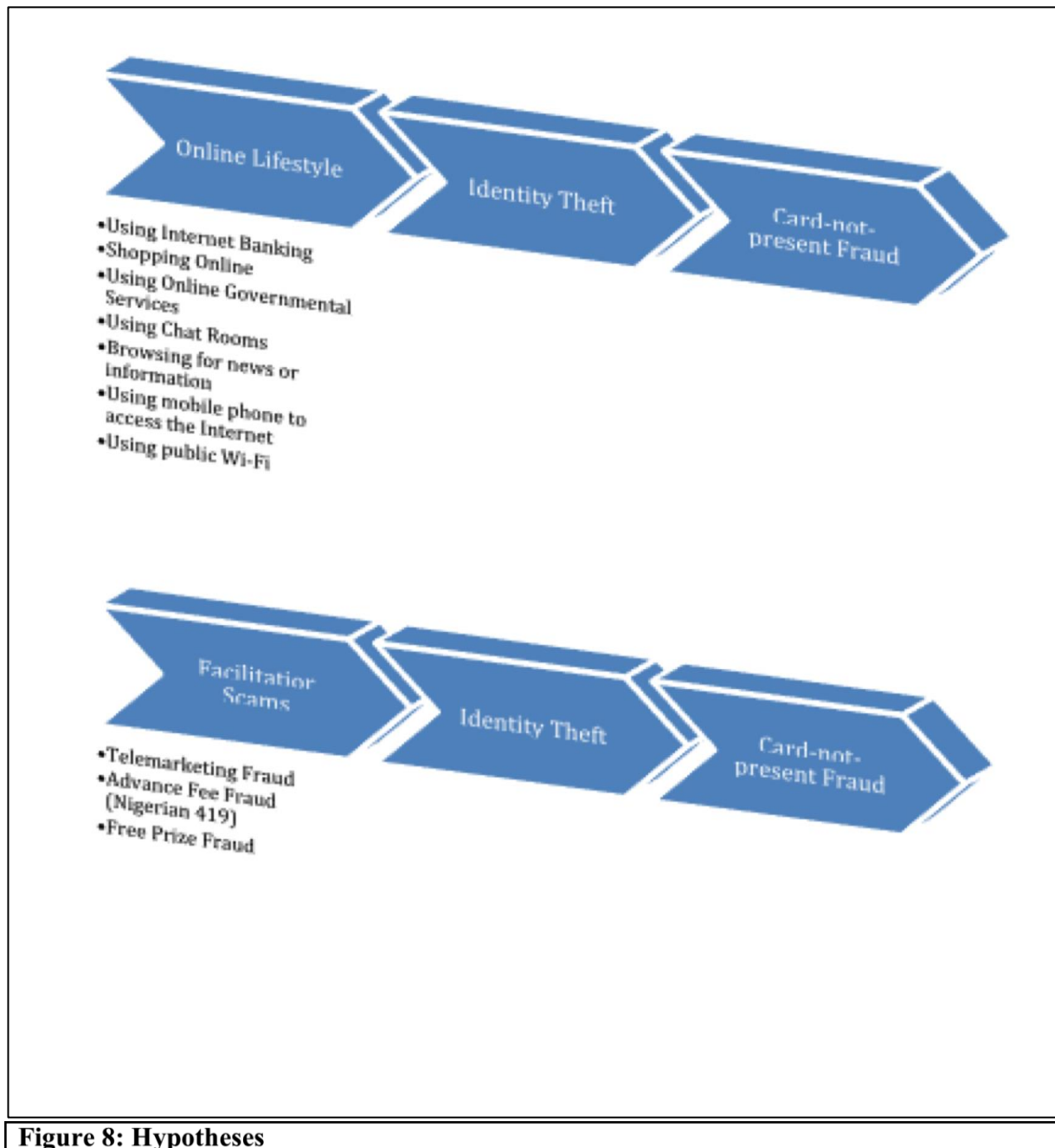


Figure 8: Hypotheses

4.1 Introduction

This dissertation adopted a secondary data analysis method to test the hypotheses related to online and offline correlates of card-not-present fraud and the effect of fear of card-not-present fraud on behavioural adaptation. Firstly, secondary data analysis method and statistical methods employed to test the hypotheses will be evaluated critically and then the data set of Crime Survey and Wales 2013/2014 will be explained before describing the analytic procedure followed to test the hypotheses and to find out online and offline correlates of card-not-present fraud. The operationalization of components of Life-style Routine Activities Theory will be explained in Appendix A.

4.2 Method

The secondary data analysis method can be defined as “... any further analysis of an existing dataset which presents interpretations, conclusions or knowledge additional to, or different from, those produced in the first report on the inquiry as a whole and its main results” Hakim (1982, p. 540). Crime Survey England and Wales 2013/2014 encompasses a wide range of questions pertaining to the online lifestyle, card-not-present fraud victimisation and fear of crime. Analysing these questions would shed light on our understanding of card-not-present fraud and fear of card-not-present fraud victimisation.

The secondary data analysis method offers many advantages to researchers. Firstly, accessing a nationwide highest quality survey is a great opportunity; it is obvious that producing such a data is beyond the ability of an individual researcher. Secondly, analysing secondary data not only allow researchers to test a theory, (Hakim, 1982) but it also enable scholars to build new theories (Zvekic and Del Frate, 1996). Moreover, Kesteren (2014)

argues that risk factors of crimes can be determined by analysing data from large victimisation surveys. Various statistical methods can also be employed owing to the rich content of national surveys (Rew et al, 2000). Economic and Social Research Council (ESRC) encourages social scientist to use secondary data in their researches (Gorard, 2002); however, the use of secondary data is widely neglected by social scientists (Irwin, 2013).

4.3 Statistical Methods Employed

Univariate, bivariate and multivariate analyses were conducted to explore the nature of card-not-present fraud victimisation as well as the online and offline correlates of card-not-present fraud and the effect of fear of card-not-present fraud on behavioural adaptations and guardianship measures. SPSS 20 statistical analysis software was used to analyse the dataset of Crime Survey England and Wales 2013/2014.

4.3.1 Univariate Analyses

Univariate analysis is a useful tool in describing the attributes of a phenomenon. Although Univariate analysis does not enable researchers to examine the relationship between two variables, examining the rates of dispersion still gives a preliminary idea about the nature of variables under examination (Maxfield and Babbie, 2015). Univariate analysis allows researchers to observe the dispersion of individuals on a single variable (Bryman and Cramer, 2001). Hence, univariate analyses were used to measure the extent of card-not-present fraud victimisation and financial losses as well as demographic characteristics of victims of card-not-present fraud. The percentages are used to explore and compare variables in the univariate analyses.

4.3.2 Bivariate Analyses

As the Univariate analyses are not sufficient to examine the relations between variables, bivariate analyses are conducted to explore the nature of relationships (Crow and Semmens, 2007). The relations between two variables are best displayed with Cross-tabulation, which visually illustrates the tendencies and relations in partial tables (Matthews and Ross, 2010). In other words, cross-tabulation or contingency tables are the most effective way of summarising the relations between two variables (Singh, 2007). When both of the variables are nominal variables, Pearson's Chi-square (X^2) is the most appropriate test to examine the existence of the relationship between two variables (Marlow, 2010). Since Pearson's Chi-square test measures the existence of the relation, Phi and Cramer's V tests are used to observe the strength and direction of the relation between two variables (Field, 2009).

4.3.3 Multivariate Analyses

Bivariate analyses are used to examine the relation between two variables however; card-not-present fraud is a complex phenomenon, which involves interaction of many variables. Multivariate analyses are used when researchers want to investigate the interaction between variables and build or test a model (Sapsford and Jupp, 2006). Life-style Routine Activities Theory proposes a model of victimisation, which is composed of three elements. Hence, using multivariate analyses would test the applicability of LRAT to card-not-present fraud as well as observing the effects of control variables such as age and gender on the occurrence of card-not-present fraud.

Qualitative Comparative Analysis (QCA) is another method that can be used to analyse models with binary dependent variables. Qualitative Comparative Analysis is a case-based method underpinned by the complex realist approach (Berg-Schlosser et al., 2009). QCA looks for necessary and sufficient conditions for a phenomenon to occur (Drass and

Miethe, 2001). Although Ragin (1999) developed QCA method to analyse small N-number cases, other scholars such as Grofman and Schneider (2009), applied this method to analyse large- N number cases such as surveys. However, this dissertation used Binary Logistic Regression Method due to following reasons:

Firstly, the QCA method requires familiarity with cases not only to interpret the results but also to resolve the contradictions that appear in ‘Truth Table’ (Schneider and Wagemann, 2010). When the QCA method is applied to the survey, every respondent was regarded as a case. However, large-N number surveys such as Crime Survey England and Wales contain many participants, which make it impossible to familiarize with every case (Greckhamer et al., 2013). Hence, interpreting the results and resolving the contradictions that emerge during analysis would be spurious.

Secondly, Vis (2012) does not recommend the use of QCA with relatively large number cases (more than 1000 cases) since the comparative power of the method decreases with the increased number of cases. On the other hand, binary logistic regression is a strong tool in building and testing models (Verma, 2012). Binary logistic regression is useful for exploratory studies since it yields the relations between outcome variable and several independent variables (Hosmer et al., 2013). It also allows researchers to observe the effect of control variables such as socio-demographics on outcome variable. Based on these considerations, this dissertation used the binary logistic regression method to run multivariate analyses. The use of the binary logistic regression is in accordance with the large body of cybercrime studies, which applied secondary data analysis method (e.g. Holtfreter et al., 2008; Pratt et al., 2010; Reyns et al., 2011; Reyns, 2013).

4.4 Data

Most of the cybercrime studies used college students as a sample universe (e.g. Ngo and Paternoster, 2011; Reyns et al., 2011; Holt and Bossler, 2013). However, using college student as a sample universe arises some problems. Firstly, generalizability of the research results in this kind of sampling is questionable. Secondly, most of the university students have the high level of computer skills, which is found to be an effective personal guardianship measure in preventing cybercrime (van Wilsem, 2013) but (Bossler et al., 2012). Hence, findings based on such population would be misleading since LRAT perspective suggests that the existence of a capable guardianship may reduce the risk of victimisation. Based on these considerations this dissertation used Crime Survey England and Wales (CSEW) 2013/2014, which uses residents of England and Wales as a sample universe.

Crime Survey England and Wales, British Crime Survey previously, measures the nature and extent of crime in England and Wales since 1982 (Office for National Statistics, 2015). It was conducted with 2 years intervals until 2001 and then it has been carried out annually (Jansson, 2007). The main aim of this survey is to observe crime trends and examine risk factors for each type of crime in England and Wales (ONS, Information Paper, 2015). This face-to-face-survey asks questions related to attendees' crime experiences occurred in the last 12 months as well as their attitudes, perceptions about crime trends (ONS Bulletin, 2014). Survey adopts a multistage cluster sampling (Maxfield and Babbie, 2015) method and uses Postcode Address File (PAF) to select the respondents randomly (ONS, Information Paper, 2015).

CSEW 2013/2014 invited 50,000 adults who live in England and Wales and 35,000 adults participated in the survey (CSEW Technical Report, 2014). Questionnaire format includes follow-up modules and self-completion modules, which ask questions to sub-samples as well as all participants. This means that all questions were not asked to all

participants. For instance, whereas mass marketing fraud questions were asked to all participants, online security questions were asked to 25% random sample of respondents and plastic card fraud questions were asked to 75% random sample of attendees (CSEW Technical Report, 2014).

4.5 Hypotheses to be tested

1. Internet users' online lifestyle such as using online banking or online shopping cause identity theft and identity theft leads to card-not-present fraud victimisation.
2. Fear of card-not-present fraud and recent card-not-present fraud victimisation not only cause behavioural adaptation but also preventive actions such as shopping from secure sites.

4.6 Analysis Plan

The analytic procedure was carried out in three phases. The first part explored the nature of card-not-present fraud victimisation and characteristics of victims, which will be presented in Appendix B. The second part of analysis aimed to test the first hypothesis and to investigate online and offline correlates of card-not-present fraud. The second hypothesis was tested in the third part of analysis.

4.7 Analytic Procedure

4.7.1 Understanding the Nature of Card-not-present Fraud:

The first phase of analyses aimed to examine different aspects of card-not-present fraud by conducting univariate analyses. The card-not-present victimisation rate, the amount of financial loss, demographic characteristics of victims, reporting behaviour of victims and the emotional effect of CNP fraud and fear of fraud were analysed to depict the nature of

card-not-present fraud. Descriptive Statistics/Frequencies command of SPSS 20 was used to analyse all of the above-mentioned analyses.

4.7.2 Exploring Correlates of Card-not-present Fraud:

4.7.2.1 Online Correlates

It is hypothesised that credit card users' online behaviours lead to identity theft and identity theft cause card-not-present fraud victimisation. Hence, it is argued that there is an indirect relation between credit card users' online behaviours and victimisation, where identity theft act as a bridge. In order to test this assumption the analyses conducted in two phases.

The first part analysed the relation between online activities and card-not-present fraud victimisation to find out the correlates of card-not-present fraud victimisation. Firstly, the three components of Life-style Routine Activities Theory were analysed separately. Whereas bivariate analyses were conducted to examine the relations between online activities and card-not-present fraud victimisation, binary logistic regression models were formed to explore the causal relations between online activities and victimisation.

Secondly, three components of theory put into one logistic regression model to test the theory as a model. Then control variables were added to the model to examine the effect of socio-demographic characteristics of CNP fraud victimisation.

The second phase analysed the relation between identity theft and card-not-present fraud. Hence, it would be possible to observe the direct and indirect relation between online activities and CNP victimisation. Firstly, all independent variables, which were used to test the components of LRAT, were put in a model to test the relation between online activities

and identity theft. Secondly, identity theft and control variables were put into a model to test the relation between identity theft and card-not-present fraud victimisation.

4.7.2.2 Offline Correlates

Responding to fraudulent communications and sending or transferring money as requested by fraudsters hypothesised to be offline factors that lead identity theft, which is a precursor to card-not-present fraud. Firstly, bivariate analyses were conducted to observe the relations between each independent variable and dependent variable. Cross-tabulation, Pearson's Chi-square and Phi and Cramer's V tests were conducted to examine relations between two variables. Secondly, the full model was tested with binary logistic regression analysis.

4.7.3 The effect of Fear of CNP fraud and Past Victimisation on Behavioural Adaptation and Guardianship Measures

It is hypothesised that the credit card users who have fear of card-not-present fraud would change their online and online behaviours and they would increase their security measures and previous card-not-present fraud victimisation would cause behavioural changes and increase the guardianship measures of credit card users. To test these hypotheses, analyses were conducted in two phases.

Two binary logistic regression models were built to assess the impact of fear of CNP fraud and previous CNP fraud victimisation on behavioural adaptations in the first phase. And then, five binary logistic regression models were formed to examine the impact of independent variables on online guardianship measures and four binary logistic regression models were built to examine the impact of independent variables on offline guardianship measures.

4.8 Measurement

Bivariate Analysis: The bivariate analyses included cross-tabulation, Pearson's Chi-square test and Phi and Cramer's V test. The cross-tabulation or contingency table displayed relations visually while representing the trends in percentages. The significance level for the Chi-square test was set as 0.5 to determine the existence of the relation between two variables. Phi and Cramer's V tests were used to explore the strength of the relation between variables.

Multivariate Analysis: The multivariate analyses included logistic regression analyses. Backward Wald method was used to obtain the most parsimonious model in the result section. The effect of the independent variables were assessed by the use significance level (Sig.) and Odds Ratio (Exp(B)). Significance level 0.05 was set to decide the statistical significance of independent variable's contribution to the model. Whereas values of Odds Ratio bigger than 1 indicates increased the likelihood, values smaller than 1 indicates decreased the likelihood.

Control Variables: Socio-demographic characteristics such as education level, gender, age, and income are the most common control variables in the social sciences (Aneshensel, 2012) and many scholars (Policastro and Payne, 2014; Reyns et al., 2011) use control variables in their studies to rule out spuriousness (Spector and Brannick, 2011) and improve statistical power of analysis (Becker, 2005).

5.1 Introduction

The results of analyses will be presented in three sections. Firstly, the nature of card-not-present fraud will be presented and then online and offline correlates of Card-not-present fraud will be examined before presenting the effect of fear of card-not-present fraud on both online, offline behaviours and guardianship methods.

5.2 The Online and Offline Correlates of Card-not-present Fraud

This part of analysis was conducted to find out the online and offline correlates of card-not-present fraud and test the first hypothesis, which propose that online activities of credit card users cause identity theft and identity theft eventually leads card-not-present fraud victimization.

5.2.1 Online Correlates

5.2.1.1 Exposure to Motivated Offender

Bivariate and multivariate analyses were conducted to investigate the presence of the association between exposure to motivated offender element of Routine Activities and card-not-present fraud victimisation. Variables were categorized into three groups since it is assumed that using the Internet for financial activities would increase the risk of victimisation.

Bivariate Analysis

As table 5.1, 5.2 and 5.3 demonstrate, *using online banking or managing finances* ($\chi^2=12.976$, $p<0.01$), *online shopping* ($\chi^2=13.991$, $p<0.001$) *using online government services*

($\chi^2=19.844$, $p<0.001$), *playing online games or attending quizzes and competitions* ($\chi^2=7.829$, $p<0.05$), *using Internet in the last 12 months* ($\chi^2=29.820$, $p<0.001$), *using Internet frequently* ($\chi^2=8.398$, $p<0.05$), *experiencing a computer virus* ($\chi^2=9.029$, $p<0.05$) and *experiencing an unauthorised access to personal data* ($\chi^2=260.286$, $p<0.001$) appeared to be significantly associated with card-not-present fraud. However, Phi & Cramer's tests indicate that whereas the relation between experiencing an unauthorised access to personal data and card-not-present fraud was moderately strong ($\phi=0.203$), the relations between other variables and victimisation were very weak since Phi (ϕ) values were very close to zero.

Exposure to Motivated Offender						
Using Internet for Financial Activities	Crosstab			Chi-Square Tests		Phi & Cramer's V
		Victimisation		χ^2	P	ϕ
		Yes	No			
Online banking or managing finances	Yes	5.0%	95.0%	12.976	.000	.045
	No	3.1%	96.9%			
Buying goods or services	Yes	4.8%	95.2%	13.991	.000	.047
	No	2.4%	97.6%			
Online government services	Yes	5.3%	94.7%	19.844	.000	.056
	No	3.0%	97.0%			
Table 5.1: Using Internet for Financial Activities						

Exposure to Motivated Offender						
Using Internet for Leisure/Social Activities	Crosstab			Chi-Square Tests		Phi & Cramer's V
		Victimisation		χ^2	P	ϕ
		Yes	No			
Social networking or blogging	Yes	4.6%	95.4%	.765	.382	.011
	No	4.1%	95.9%			
E-mail, instant messaging, chat rooms	Yes	4.5%	95.5%	1.930	.165	.017
	No	3.5%	96.5%			
Browsing for news or information	Yes	4.5%	95.5%	1.734	.188	.017
	No	3.7%	96.3%			
Playing online games/doing quizzes/competitions	Yes	5.4%	94.6%	7.829	.005	.035
	No	3.9%	96.1%			
Table 5.2: Using Internet for Leisure/Social Activities						

Exposure to Motivated Offender						
Internet Related Factors	Crosstab			Chi-Square Tests		Phi & Cramer's V
		Victimisation		χ^2	P	ϕ
		Yes	No			
Used internet at home or elsewhere in last 12 months	Yes	4.4%	95.6%	29.820	.000	.062
	No	1.4%	98.6%			
Used Internet Frequently	Yes	4.9%	95.1%	8.398	.004	.036
	No	3.3%	96.7%			
Experienced a computer virus	Yes	5.8%	94.2%	9.029 ^a	.003	.038
	No	3.9%	96.1%			
Experienced an unauthorised access to/use of personal data	Yes	18.9%	81.1%	260.286 ^a	.000	.203
	No	3.2%	96.8%			
Table 5.3: Internet Related Factors						

Binary Logistic Regression:

As the model in table 5.4 demonstrates, two risky online financial activities, one online leisure activity and one the Internet related activity emerged as the statistically significant predictor of card-not-present fraud. *Buying goods or services online* increased the risk of victimisation by 57% ($b=0.452$, $p<0.05$, $\text{Exp}(B)=1.571$). This result is consistent with previous research (Holtfreter et al., 2008; Pratt et al., 2010; Reyns, 2013). Also *using online government services* increase the likelihood of victimization by %50 ($b=0.406$, $p<0.05$, $\text{Exp}(B)=1.500$). Additionally, those respondents who used the Internet for *playing online*

games were about 31 per cent more likely to be victim of card-not-present fraud ($b=0.273$, $p<0.05$, $\text{Exp}(B)=1.314$). Lastly, credit card users who reported experiencing an unauthorized access to/use of personal data were at increased risk compared to those who did not experience online identity theft ($b=1.897$, $p<0.001$, $\text{Exp}(B)=6.668$). Those who experienced online identity theft were 560 per cent more likely to be victimized.

Exposure to Motivated Offender						
Using Internet for Financial Activities		B	Sig.	Exp(B)	95% C.I. for EXP(B)	
					Lower	Upper
Online banking or managing finances	eusint3a(1)	.230	.159	1.258	.914	1.733
Buying goods or services	eusint3b(1)	.452	.040	1.571	1.020	2.420
Online government services	eusint3c(1)	.406	.009	1.500	1.108	2.031
Using Internet for Leisure/Social Activities						
Social networking or blogging	eusint3d(1)	-.108	.433	.898	.686	1.175
E-mail, instant messaging, chat rooms	eusint3e(1)	-.146	.497	.864	.567	1.318
Browsing for news or information	eusint3f(1)	-.076	.679	.926	.645	1.331
Playing online games/doing quizzes/competitions	eusint3g(1)	.273	.041	1.314	1.011	1.707
Internet Related Factors						
Used internet at home or elsewhere in last 12 months	Internetuse(1)	.194	.188	1.214	.910	1.619
Experienced a computer virus	eexpinta(1)	.173	.216	1.189	.904	1.564
Experienced an unauthorised access to/use of personal data (e.g. e-mail account/bank account)	eexpintc(1)	1.897	.000	6.668	5.048	8.808
Table 5.4: Logistic Regression for Exposure to Motivated Offender						

5.2.1.2 Target Suitability

It is assumed that devices used to access the Internet increase the risk of victimization. Hence, devices are categorized into two groups, high-risk and low-risk devices to test this assumption.

Bivariate Analyses:

As table 5.5 illustrates, *using laptop away from domestic place such as home and work or school/college* ($\chi^2=6.110$, $p<0.05$), *using handheld computers such as Ipad or tablet to access the Internet* ($\chi^2=13.924$, $p<0.001$), *using mobile phone to access the Internet* ($\chi^2=16.514$, $p<0.001$), *using digital TV to access the Internet* ($\chi^2=0.015$, $p<0.05$) appeared to be significantly associated with card-not-present fraud. However, Phi & Cramer's test indicate that these relations between independent variables and victimisation were very weak since Phi (ϕ) values were very close to zero.

Target Suitability/Devices Used to Access the Internet						
High Risk Devices	Crosstab			Chi-Square Tests		Phi & Cramer's V
		Victimisation		χ^2	P	ϕ
		Yes	No			
Laptop away from home and work or school/college	Yes	4.7%	95.3%	6.110	.013	.031
	No	3.3%	96.7%			
Handheld computer (iPad, tablet, palmtop)	Yes	5.6%	94.4%	13.924	.000	.047
	No	3.6%	96.4%			
Mobile phone or Smartphone	Yes	5.2%	94.8%	16.514	.000	.051
	No	3.0%	97.0%			
Public access computer (e.g. In a library, internet cafe)	Yes	4.8%	95.2%	.296	.586	.007
	No	4.3%	95.7%			
Low Risk Devices	Crosstab			Chi-Square Tests		Phi & Cramer's V
		Victimisation		χ^2	P	ϕ
		Yes	No			
Laptop, at home or work or school/college	Yes	4.9%	95.1%	1.855	.173	.017
	No	4.1%	95.9%			
Desktop computer (at home or work or school/college)	Yes	4.6%	95.4%	.951	.330	.012
	No	4.1%	95.9%			
Games console	Yes	4.8%	95.2%	.506	.477	.009
	No	4.3%	95.7%			
Digital TV	Yes	5.8%	94.2%	.015	.019	.031
	No	4.1%	95.9%			
Table 5.5: Bivariate Target Suitability						

Binary Logistic Regression Model:

As it was assumed, high-risk devices appeared to increase the risk of victimisation significantly (Table 5.6). Whereas *using handheld computer to access the Internet* increased the risk of victimization by 37% ($\chi^2=0.319$, $p<0.05$), *using mobile or smartphone to access the Internet* increased the risk of victimisation by %53 ($\chi^2=0.426$, $p<0.05$). Low-risk devices, however, were not statistically significantly associated with victimisation.

Target Suitability/Devices Used to Access the Internet						
High Risk Devices		B	Sig.	Exp(B)	95% C.I. for EXP(B)	
					Lower	Upper
Laptop away from home and work or school/college	intrus2c(1)	-.092	.533	.913	.684	1.217
Handheld computer	intrus2e(1)	.319	.019	1.375	1.053	1.797
Mobile phone or Smartphone	intrus2d(1)	.426	.005	1.532	1.136	2.066
Public access computer (e.g. In a library, internet cafe)	intrus2h(1)	-.056	.784	.946	.634	1.410
Low Risk Devices						
Laptop, at home or work or school/college	intrus2b(1)	.275	.098	1.316	.951	1.823
Desktop computer(at home or work or school/college)	intrus2a(1)	.054	.686	1.056	.811	1.374
Games console	intrus2f(1)	-.198	.293	.821	.568	1.186
Digital TV	intrus2g(1)	.171	.308	1.186	.854	1.647
	Constant	-3.731	.000	.024		
Table 5.6: Binary Logistic Regression Model for Target Suitability						

5.2.1.3 Absence of Capable Guardianship:

Bivariate Analyses:

Tables 5.7 and 5.8 illustrate that downloading *software updates and patches whenever prompted* ($\chi^2 = 7.482$, $p<0.05$), *checking signs that a site is secure when buying online* ($\chi^2=5.571$, $p<0.05$), *protecting home wireless connection (Wi-Fi) with password* ($\chi^2=7.489$, $p<0.05$), *deleting suspicious emails without opening them* ($\chi^2=6.406$, $p<0.05$), *being cautious*

using public Wi-Fi/insecure Wi-Fi ($\chi^2=9.624$, $p<0.05$), only using credit cards ($\chi^2=4.106$, $p<0.05$), using a different password for each different online account ($\chi^2=9.532$, $p<0.05$) were statistically significantly associated with card-not-present fraud. Yet, Phi & Cramer's test indicate that these relations between independent variables and victimisation were very weak since Phi (ϕ) values were very close to zero.

GUARDIANSHIP						
Digital	Crosstab			Chi-Square Tests		Phi & Cramer's V
		Victimisation		χ^2	P	ϕ
		Yes	No			
Install anti virus or other security software	Yes	4.4%	95.6%	.186	.666	.005
	No	4.1%	95.9%			
Install a firewall on your computer	Yes	4.4%	95.6%	.113	.736	.004
	No	4.3%	95.7%			
Download software updates and patches whenever prompted	Yes	5.1%	94.9%	7.482	.006	.034
	No	3.7%	96.3%			

Table 5.7: Bivariate Digital Guardianship

GUARDIANSHIP						
Personal	Crosstab			Chi-Square Tests		Phi & Cramer's V
		Victimisation		χ^2	P	ϕ
		Yes	No			
Check for signs that a site is secure when buying online (closed padlock sign/https website address)	Yes	4.9%	95.1%	5.571	.018	.030
	No	3.7%	96.3%			
Protect your home wireless connection (wi-fi) with a password	Yes	5.0%	95.0%	7.849	.005	.035
	No	3.5%	96.5%			
Delete suspicious emails without opening them	Yes	4.8%	95.2%	6.406	.011	.032
	No	3.3%	96.7%			
Log out of websites when you are finished	Yes	4.5%	95.5%	.296	.586	.007
	No	4.2%	95.8%			
Be cautious using public wi-fi / insecure wi-fi	Yes	5.5%	94.5%	9.624	.002	.039
	No	3.8%	96.2%			
Only use credit cards (not debit or charge cards)	Yes	5.3%	94.7%	4.106	.043	.025
	No	4.1%	95.9%			
Use complex passwords (contain letters, numbers and symbols)	Yes	4.7%	95.3%	2.578	.108	.020
	No	3.8%	96.2%			
Use a different password for each different online account	Yes	5.3%	94.7%	9.352	.002	.038
	No	3.7%	96.3%			
Table 5.8: Bivariate Personal Guardianship						

Binary Logistic Regression Model:

Table 5.9 demonstrates that only *using a different password for each different online account* was statistically significantly associated with card-not-present fraud victimization ($\chi^2=0.280$, $p<0.05$). This means that credit card users who used a different password for each online account were about 32% more likely be victim of card-not-present fraud ($\text{Exp}(B)=1.323$).

Absence of a Capable Guardian						
		B	Sig.	Exp(B)	95% C.I. for EXP(B)	
Digital					Lower	Upper
Install anti virus or other security software	eprode3a(1)	-.094	.624	.910	.625	1.326
Install a firewall on your computer	eprode3b(1)	-.199	.191	.820	.608	1.105
Download software updates and patches whenever prompted	eprode3c(1)	.219	.157	1.244	.919	1.685
Personal						
Use complex passwords (contain letters, numbers and symbols)	eprode3d(1)	-.078	.635	.925	.669	1.278
Use a different password for each different online account	eprode3e(1)	.280	.039	1.323	1.014	1.726
Check for signs that a site is secure when buying online	eprode3f(1)	.039	.798	1.040	.769	1.406
Protect your home wireless connection (wi-fi) with a password	eprode3g(1)	.179	.261	1.197	.875	1.636
Delete suspicious emails without opening them	eprode3h(1)	.215	.250	1.240	.860	1.788
Log out of websites when you are finished	eprode3i(1)	-.240	.119	.786	.581	1.064
Be cautious using public wi-fi / insecure wi-fi	eprode3j(1)	.217	.132	1.242	.937	1.647
Only use credit cards (not debit or charge cards)	eprode3k(1)	.154	.286	1.166	.880	1.545
	Constant	-3.325	.000	.036		
Table 5.9: Binary Logistic Regression for Guardianship						

5.2.1.4 Full Model

Binary Logistic Regression Model for All Online Factors:

Up to now, three components of theory were examined separately. However, as theory proposes, the convergence of these three components creates victimization. Hence, variables were put together to test the performance of full model.

Two binary logistics regression models were constructed. The first model included all components of theory to examine the combined effect of interaction between three variables.

The second model was built with inclusion of control variables, age, gender, running own business and having own business and ethnicity.

According to model 1 in table 5.10, two ‘exposure to the motivated offender’ variables, three ‘target suitability’ variables and one guardianship variable emerged to be the statistically significant indicator of card-not-present fraud. Whereas respondents who used *online governmental services* ($\chi^2=0.329$, $p<0.05$, $\text{Exp}(B)=1.376$), *used mobile phone or smartphone to access the Internet* ($\chi^2=4.106$, $p<0.05$, $\text{Exp}(B)=1.400$), *used a handheld computer to access the Internet* ($\chi^2=4.106$, $p<0.1$, $\text{Exp}(B)=1.275$), and *experienced unauthorized access to/use of personal data* ($\chi^2=1.867$, $p<0.001$, $\text{Exp}(B)=6.467$) were at increased risk of victimisation, those who *used social networking or blogging* were less likely to be victimised ($\chi^2=4.106$, $p<0.05$, $\text{Exp}(B)=0.753$). Although it is a security measure, *using a different password for each online account* emerged as risk increasing factor ($\chi^2=0.229$, $p<0.1$, $\text{Exp}(B)=1.257$).

As model 2 in table 5.11 demonstrates, three of these variables remained after control variables were added to the model. None of the control variables were statistically significantly associated with victimisation. Credit card users who *used mobile phones to access the Internet* were nearly 90% more likely to be victimised than those who did not used mobile devices to access the Internet ($\text{Exp}(B)=1.896$). But, credit card users who experienced *online identity theft (unauthorised access to/use of personal information)* faced the biggest threat. Experiencing online identity theft appeared to increase the likelihood of victimisation by about 600% ($\text{Exp}(B)=6.999$). Lastly, those who *used the Internet for networking or blogging* were nearly 40% less likely to be victimised ($\text{Exp}(B)=0.619$).

FULL MODEL-ONLINE FACTORS						
		B	Sig.	Exp(B)	95% C.I. for EXP(B)	
					Lower	Upper
Use a different password for each different online account	eprode3e(1)	.229	.072	1.257	.979	1.614
Online government services	eusint3c	.319	.025	1.376	1.041	1.820
Social networking or blogging	eusint3d	-.284	.042	.753	.573	.990
Mobile phone or Smartphone	intrus2d	.337	.032	1.400	1.029	1.906
Handheld computer	intrus2e	.243	.073	1.275	.977	1.664
Experienced unauthorized access to/use of personal data	eexpintc	1.867	.000	6.467	4.896	8.542
	Constant	-3.873	.000	.021		

Table 5.10: Binary Logistic Regression for all Online Components

FULL MODEL-ONLINE FACTORS WITH CONTROL VARIABLES						
		B	Sig.	Exp(B)	95% C.I. for EXP(B)	
					Lower	Upper
Social networking or blogging	eusint3d	-.480	.051	.619	.382	1.002
Mobile phone or Smartphone	intrus2d	.640	.009	1.896	1.172	3.068
Experienced unauthorized access to/use of personal data	eexpintc	1.946	.000	6.999	4.182	11.714
	Constant	-3.873	.000	.021		

Table 5.11: Binary Logistic Regression for all Online Components with Control Variables

5.2.2 Online Identity Theft

The Relation between Online Activities, Online Identity Theft and Card-not-present Fraud Victimization:

Binary logistic regression models were formed to test the first hypothesis proposing that there is a causal relation between credit card users' online activities and online identity theft, which eventually leads to card-not-present fraud victimisation.

As the first model in table 5.12 illustrates, five of the variables measuring online routine activities appeared to be significant predictors of online identity theft. *Using online banking or managing finances* ($\chi^2=0.450$, $p<0.01$), *buying goods or services* ($\chi^2=0.779$,

$p < 0.01$), *using online government services* ($\chi^2 = 0.381$, $p < 0.01$), *playing online games/doing quizzes and competitions* ($\chi^2 = 0.292$, $p < 0.05$), *experiencing a computer virus* ($\chi^2 = 0.701$, $p < 0.01$) emerged to be the statistically significant indicator of online identity theft.

According to the second model in table 5.13, three of these measures remained and three guardianship variables were added after the inclusion of control variable to the new model. First, respondents who *purchased items online* were nearly 135% more likely to be victim of online identity theft ($\text{Exp}(B) = 2.352$). *Using online government services* appeared to be another risk-increasing online activity. The respondents who used online government services were 83% more likely to be the victim of the online identity theft than those who did not use these services. Credit card users who reported *experiencing a computer virus* were also at increased risk compared to those who did face a computer virus. Experiencing a computer virus appeared to increase the risk of online identity theft by 100% ($\text{Exp}(B) = 2.015$).

On the other hand, guardianship measures, *using complex passwords for each online account* and *using complex passwords* increased the risk of identity theft by 47% and 70% respectively ($\text{Exp}(B) = 1.472$, $\text{Exp}(B) = 1.713$). This result is contrary to the Life-style Routine Activities Theory, which postulates that the presence of a capable guardianship decreases the risk of victimisation. But *protecting home wireless connection with a password* appeared to decrease the risk of victimisation by 38% ($\text{Exp}(B) = 0.628$). These guardianship results may indicate the effectiveness of guardianship measures play an important role in preventing identity theft.

Gender and age between 41 and 59 were statistically significantly associated with identity theft. Females were 47% less likely to be victimised than males ($\text{Exp}(B) = 0.538$). Respondents who aged between 41 and 59 years were 60% less likely to be victim of identity theft compared to those aged over 60 years.

With regards to relationship between online identity theft and card-not-present fraud, third model in table 5.14 demonstrates that online identity theft was a strong predictor of card-not-present fraud. Respondents who experienced online identity theft were 600% more likely to be victim of card-not-present fraud ($\text{Exp}(B)=7.009$) than those who did not face online identity theft.

Overall, these results appear to support the first hypothesis stating that credit card users' online activities increase the risk of online identity theft, which finally leads to card-not-present fraud. Hence, online identity theft is a precursor crime to card-not-present fraud.

Relation Between Online Activities and Online Identity Theft						
Using Internet for Financial Activities		B	Sig.	Exp(B)	95% C.I. for EXP(B)	
					Lower	Upper
Online banking or managing finances	eusint3a(1)	.450	.001	1.569	1.209	2.035
Buying goods or services	eusint3b(1)	.779	.000	2.178	1.473	3.221
Online government services	eusint3c(1)	.381	.001	1.463	1.157	1.850
Playing online games/doing quizzes/competitions	eusint3g(1)	.292	.003	1.340	1.103	1.627
Experienced a computer virus	eexpinta(1)	.701	.000	2.015	1.654	2.455
	Constant	-4.088	.000	.017		
Table 5.12: Relation Between Online Activities and Online Identity Theft						

Relation Between Online Activities and Online Identity Theft						
		B	Sig.	Exp(B)	95% C.I. for EXP(B)	
					Lower	Upper
Buying goods or services	eusint3b(1)	.855	.009	2.352	1.234	4.485
Online Government Services	eusint3c(1)	.609	.005	1.838	1.198	2.819
Use complex passwords (contain letters, numbers and symbols)	eprode3d(1)	.538	.026	1.713	1.065	2.753
Use a different password for each different online account	eprode3e(1)	.387	.059	1.472	.985	2.200
Protect your home wireless connection (wi-fi) with a password	eprode3g(1)	-.466	.032	.628	.410	.962
Experienced a Computer Virus	eexpinta(1)	.745	.000	2.106	1.405	3.156
Age of the Respondents	Recoded_age		.003			
	Recoded_age(1)	-.085	.797	.918	.481	1.754
	Recoded_age(2)	-.613	.072	.542	.278	1.056
	Recoded_age(3)	-.906	.004	.404	.218	.749
Gender of Respondents	recoded_sex(1)	-.619	.005	.538	.348	.833
	Constant	-3.231	.000	.040		
Table 5.13: The Relation Between Online Activities and Online Identity Theft						

Relation Between Online Identity Theft and Card-not-present Fraud Victimisation						
		B	Sig.	Exp(B)	95% C.I. for EXP(B)	
					Lower	Upper
Online Identity Theft	eexpintc(1)	1.947	.000	7.009	5.323	9.229
Age of the Respondents	Recoded_age		.794			
	Recoded_age(1)	-.028	.901	.972	.626	1.511
	Recoded_age(2)	-.128	.569	.880	.568	1.365
	Recoded_age(3)	-.186	.449	.830	.513	1.343
Gender of the Respondents	recoded_sex(1)	.120	.349	1.127	.877	1.448
Employment	recoded_work2(1)	.002	.987	1.002	.747	1.345
Having Any Qualification	educint(1)	-.012	.958	.988	.629	1.552
Ethnicity	ethgrp3a(1)	-.019	.929	.981	.649	1.484
	Constant	-3.368	.000	.034		
Table 5.14: Relation Between Online Identity Theft and Card-not-present Fraud Victimisation						

5.2.3 Offline Correlates of Card-not-present Fraud Victimization

Bivariate and multivariate analyses were conducted to examine the relationship between terrestrial input frauds (offline correlates) and card-not-present fraud victimization

Bivariate Analyses:

Responding to communication to help moving in large sum of money from abroad, which is known as Nigerian 419 advanced fee scams, ($\chi^2=3.639$, $p<0.05$) and responding to communication about an urgent request to help someone get out of some sort of financial trouble ($\chi^2=12.470$, $p<0.001$), were statistically significantly associated with card-not-present fraud (Table 5.15). Yet, Phi & Cramer's test indicate that these relations between independent variables and victimisation were very weak since Phi (ϕ) values were very close to zero.

Offline Correlates of Card-not-present Fraud						
	Crosstab			Chi-Square Tests		Phi & Cramer's V
		Victimisation		χ^2	P	ϕ
		Yes	No			
Responding communication about financial details	Yes	3.5%	96.5%	1.473	.225	-.021
	No	7.8%	92.2%			
Provided Bank Details	Yes	18.2%	81.8%	1.046	.307	.164
	No	7.1%	92.9%			
Sent off or transferred money as requested in response to a win in a lottery or other competition	Yes	16.7%	83.3%	1.019	.313	.028
	No	8.5%	91.5%			
Responding to communication about investment with a guaranteed high return	Yes	8.0%	92.0%	.064	.800	.004
	No	7.2%	92.8%			
Sent off or transferred money as requested in connection with a guaranteed high return investment	Yes	0.0%	100.0%	.846	.358	-.016
	No	7.8%	92.2%			
Responding to communication about help in moving large sums of money from abroad	Yes	12.8%	87.2%	3.639	.056	.019
	No	6.1%	93.9%			
Responding to communication about an urgent request to help someone get out of some sort of financial trouble	Yes	16.4%	83.6%	12.470	.000	.034
	No	6.0%	94.0%			
Table 5.15: Offline Correlates of CNP Fraud						

Binary Logistic Regression Model:

As the first model in table 5.16 illustrates, only one of the variables measuring risky offline activities was emerged as significant predictors of card-not-present fraud. *Responding an urgent request to help to someone get out of some sort of financial trouble* appeared to increase the risk of victimization about 370% ($\chi^2=3.639$, $p<0.05$, Exp (B)=4.671).

According to the second model in table 5.17, the impact of independent variable on dependent variable increased after the inclusion of control variable to the new model. First, credit card users who *responded an urgent request to help someone get out of some sort of financial trouble* were nearly 1380% more likely to be the victim of card-not-present fraud than those who did not respond such a communication (Exp(B)=14.818). Second, *running one's own business* appeared to be risk increasing demographic characteristics. The respondents who run own business were 640% more likely to be the victim of online card-not-present fraud than those who did not run own business (Exp(B)=7.409).

FULL MODEL-OFFLINE CORRELATES						
		B	Sig.	Exp(B)	95% C.I. for EXP(B)	
					Lower	Upper
Responding an urgent request to help someone get out of some sort of financial trouble	anyfraudf(1)	1.541	.032	4.671	1.144	19.071
	Constant	-2.235	.000	.107		

Table 5.16: Binary Logistic Regression Model for Offline Correlates of CNP Fraud

FULL MODEL-OFFLINE CORRELATES						
		B	Sig.	Exp(B)	95% C.I. for EXP(B)	
					Lower	Upper
Responding an urgent request to help someone get out of some sort of financial trouble	anyfraudf(1)	2.696	.010	14.818	1.902	115.436
Running own business	ownbus2(1)	2.003	.030	7.409	1.220	44.995
	Constant	-2.696	.000	.067		

Table 5.17: Binary Logistic Regression Model with Control Variables for Offline Correlates of CNP Fraud

5.3 The Impact of the Fear of Crime and Past CNP Fraud Victimization

5.3.1 The Impact of the Fear of Crime and Past CNP Fraud Victimization on the Online and Offline Behaviours

Fear of card-not-present fraud and past card-not-present fraud victimisation appeared to be statistically significant predictors of both online and offline behaviours (Table 5.18). As table 5.18 demonstrates, whereas credit card users who had the fear of card-not-present fraud victimisation were more likely to avoid purchasing items on Internet (Exp. (B)=1.104), victims of card-not-present fraud were more likely to continue purchasing items on Internet (Exp. (B)=0.746). Furthermore, victims of CNP fraud were more likely to engage in protective behaviours such as purchasing items from secure website (Exp. (B)=1.403) and only using a credit card rather than a debit card online (Exp. (B)=1.670) when compared to credit card users with fear of CNP fraud (Exp. (B)=1.322 and 1.317 respectively). These results indicates CNP fraud victims were more likely to not to quit purchasing items on the Internet but engage in more protective actions when compared to credit card users who had fear of crime.

On the other hand, credit card users who reported fear of card-not-present fraud and past CNP fraud victimisation were more likely to use only cash points that are inside (Exp. (B)=1.501 and Exp. (B)=1.195 respectively), but they did not stop using cash points (Exp. (B)=0.804 and Exp. (B)=0.741 respectively). However, credit card users who had fear of CNP fraud adjusted their offline behaviours more than victims of card-not-present fraud (Exp. (B)=1.501 and 1.195 respectively).

The results in table 5.18 indicate that female credit card users were more likely to quit purchasing items on the Internet than males (Exp. (B)=0.815), however, male credit card users were more likely to engage in protective behaviours such as purchasing items from

secure websites Exp. (B)=1.130) and only using a credit card rather than a debit card Exp. (B)=1.049). In regards to offline behaviours, females were more likely to adjust their offline behaviours than males (only use cash points that are inside (Exp. =0.645) and never use cash points (Exp. =0.734) (Table 5.24).

Age appeared to be the statistically significant indicator of behavioural adaptation. Credit card users who were over 60 years were more likely to change their online and offline behaviours compared to credit card users who were under 60 years.

THE EFFECT OF FEAR OF CNP FRAUD VICTIMISATION AND PAST VICTIMISATION ON BEHAVIOURS								
	ONLINE				OFFLINE			
	Avoid purchasing items on internet				Never use cash points			
	B	SE	Sig.	Exp(B)	B	SE	Sig.	Exp(B)
Fear of CNP Fraud	.099	.036	.006	1.104	-.218	.049	.000	.804
CNP Fraud Victimization	-.293	.098	.003	.746	-.300	.146	.040	.741
Gender	-.205	.036	.000	.815	-.309	.049	.000	.734
Age			.000				.000	
Under 25	-1.181	.084	.000	.307	-2.146	.153	.000	.117
Between 25-40	-1.373	.054	.000	.253	-2.518	.104	.000	.081
Between 41-59	-.800	.042	.000	.449	-1.548	.062	.000	.213
Table 5.18: Logistic Regression Model for The Effect of Fear of CNP Fraud Victimization and Past Victimization on Behaviours								

5.3.2 The Impact of the Fear of Crime and Past CNP Fraud Victimization on Guardianship Measures

Binary logistic regression models in tables 5.19 and 5.20 show that fear of card-not-present fraud and previous CNP fraud victimization cause an increase in preventive actions. For instance, while fear of CNP fraud causes a %32 increase in only purchasing items from secure website, previous CNP fraud victimization cause %40 increase in only purchasing items from secure website ($\text{Exp}(B)=1.322$ and 1.403 respectively).

Tables 5.19 and 5.20 indicate that whereas males were more likely to take more preventive actions than females in cyberspace, females were more likely to protect their personal data in the real world. For instance, using computer security measures ($\text{Exp}(B)=1.267$), have a separate card for online purchases ($\text{Exp}(B)=1.206$), but keep the record of PIN number separately from cards ($\text{Exp}(B)=0.896$) and shield PIN number in cash points/in shops ($\text{Exp}(B)=0.846$).

Age was also a significant predictor of changes for guardianship measures. However, guardianship patterns showed difference according to type of guardianship measures. For instance, whereas credit card users who were younger than 60 years old, increased the use of computer security measures, credit card users who were older than 60 years old preferred to keep PIN numbers separately from credit cards.

Overall, the results indicate that fear of CNP fraud victimization and past CNP fraud victimization had the impact on online and offline behaviours. This result is in line with Reisig et al. (2009). However, Forsythe and Shi (2003) found that perceived risk and victimization have no effect on online shopping behaviour.

BINARY LOGISTIC REGRESSION-ONLINE GUARDIANSHIP										
	Use computer security measures		Regularly check transactions on bank statements		Only purchase items from secure websites		Only use a credit card rather than a debit card online		Have a separate card for online purchases	
	Sig.	Exp(B)	Sig.	Exp(B)	Sig.	Exp(B)	Sig.	Exp(B)	Sig.	Exp(B)
Fear of CNP Fraud	.000	1.236	.000	1.326	.000	1.322	.000	1.317	.000	1.372
CNP Fraud Victimization	.000	1.498	.000	1.679	.000	1.403	.000	1.670	.103	1.206
Gender	.000	1.267	.099	.948	.000	1.130	.152	1.049	.000	1.241
Age	.000		.000		.000		.000		.000	
Under 25	.000	1.422	.000	.468	.000	2.402	.000	.289	.135	.827
Between 25-40	.000	2.466	.000	.735	.000	2.919	.003	.875	.005	1.231
Between 41-59	.000	2.679	.000	.847					.000	1.530
Table 5.19: Binary Logistic Regression Model for Online Guardianship										

BINARY LOGISTIC REGRESSION-OFFLINE GUARDIANSHIP								
	Keep record of PIN number separately from cards/no record of PIN numbers kept		Frequently change PIN number		Shield PIN number at cash points/in shops/etc.		Keep card in view when paying in restaurants, etc.	
	Sig.	Exp(B)	Sig.	Exp(B)	Sig.	Exp(B)	Sig.	Exp(B)
Fear of CNP Fraud	.000	1.142	.000	1.450	.000	1.462	.000	1.313
CNP Fraud Victimization	.129	1.099	.000	1.571	.032	1.159	.000	1.313
Gender	.000	.896	.000	1.223	.000	.846	.005	1.078
Age	.000		.000		.000		.000	
Under 25	.000	.455	.000	1.670	.462	1.041	.000	.596
Between 25-40	.000	.627	.000	1.459	.663	1.016	.000	.712
Between 41-59	.009	.920	.000	1.503	.000	1.263	.145	1.048
Table 5.20: Binary Logistic Regression Model for Offline Guardianship								

Chapter 6**Discussion****6.1 Introduction**

Despite a growing interest in cybercrime studies among scholars very little is known about the card not present fraud and its correlates (Holtfreter et al., 2008; Reisig et al., 2009). In order to address this gap in the literature, this dissertation aimed to find out the online and offline correlates of card-not-present fraud, examine the relation between online activities, identity theft and card-not-present fraud and explore the impact of fear of card-not-present fraud victimisation and past card-not-present fraud victimisation on behavioural adaptation and guardianship measures. Firstly, the most important findings with their possible explanations will be discussed and then limitations of this dissertation will be stated before presenting policy implications of this dissertation.

6.2 Nature of Card-not-present Fraud Victimisation

One of the aims of this dissertation was to depict the nature and extent of card-not-present fraud is not clear. Wall (2007; 2008/11; 2008b) and Yar (2005) imply that the public perception of cybercrime, which perceive cybercrime as a big threat, is somewhat constructed by the mass media. However, this study has found that the self-reported victimisation rate of card-not-present fraud is higher than other conventional crimes such as theft and burglary (Appendix B). The results indicate that despite the highest victimisation percentage, the financial impact of CNP on individuals is not so great. Most of the victims of CNP fraud reported the small amount of losses and 39% of them reported that they have received a refund. The fraudsters' tactic, which aims to steal small amount of money from many accounts rather than a great amount of money from one account, would be a possible explanation of these small amounts of financial losses (Wall, 2007; Tropina, 2014). Hence, the perpetrators may evade from prosecution since either victims do not inform authorities about

victimisation for the small amount of losses (Gheraouti, 2013) or theft of the small amount of money “punished as a misdemeanour” in many jurisdictions (Siegel, 2011, pp.664).

Results pertaining to the education level of victims raise issues worthy of further discussion. Credit card users who had higher levels of education reported higher percentages of victimisation. There appears to be a positive relation between education level and the risk of victimisation. This positive relation may be accounted for the financial ability of educated people and increased usage of financial service, which put them to close proximity to motivated offenders.

Lastly, victims of credit card fraud tend to report the victimisation to financial institutions such as banks, rather than policing bodies. This would be accounted for the desire to receive a refund for their losses, since banks tend to write-off victims’ losses to prevent defamation (Wall, 2007).

6.3 Online and Offline Correlates of Card-not-present Fraud

With regards to exposure to motivated offender, the LRAT perspective assumes that exposure to a motivated offender increases the risk of victimisation. Using the Internet for financial purposes is hypothesised to be riskier than using the Internet for leisure/social activities since credit card users reveal their credit card numbers and other personal information during online financial activities. Results appear to support this assumption of risky behaviours. ‘*Buying goods or services online*’ (Van Wilsem, 2011; Reyns, 2013), ‘*using online government services*’, ‘*playing online games or doing quizzes/competitions*’ and ‘*experiencing unauthorised access to/use of personal data*’ appeared the significant predictors of card-not-present fraud.

In regards to target suitability, it is assumed mobile devices bear some security breaches (Ben-Asher et al., 2013) and using these devices to access the Internet would

increase the risk of CNP fraud victimisation. The binary logistic regression model of target suitability indicates that *'using handheld computers such as Ipad or tablets'* and *'mobile phone or smartphone'* to access the Internet appear to be statistically significant predictors of CNP fraud. On the other hand, *'using laptop at home or desktop computer'* to access the Internet is not statistically significantly associated with CNP fraud. This result would be attributed to the security issues related to accessing the Internet. Internet users generally access the Internet via secure networks at home or at work; however, mobile phone users sometimes access the Internet via public hotspots, which shopping malls or other institutions offer for free. Fraudsters sometimes use these public Wi-Fi hotspots to gain personal information illegally (Phifer, 2009; Davi et al., 2012). The extensive use of android applications can be another possible explanation of this result. La Polla et al. (2013) argue that android markets are not closely and effectively supervised, which causes the intrusion of malware android applications (Becher et al., 2011).

The results pertaining to the absence of a capable guardian contradicts Life-style Routine Activities Theory, which assumes that both digital and personal guardianship measures would decrease the risk of victimisation. However, digital security methods and most of the personal security measures are not statistically significantly correlated with CNP fraud victimisation. *'Using different password for each different online account'*, which was the only statistically significant guardianship measure, appeared to increase the risk of CNP fraud victimisation. Previous studies have revealed contradictory results related to the guardianship element of LRAT. Similarly, Ngo and Paternoster (2011) and Holt and Bossler (2013) found that using security software increases the risk of victimisation. However, Holt and Bossler (2009) and Marcum (2008) found that digital guardianship (computer security) has no effect on cyber victimisation.

The final model that contains all elements of theory and demographics illustrates that *'using mobile phone or smartphone to access the Internet'* and *'experiencing unauthorised access to/use of personal data'* increased the risk of CNP fraud victimisation. Although partial models of components of the theory, which were discussed above, suggest that online activities such as online shopping and using online banking increase the risk of victimisation, these activities removed from the final model. This result would be attributed to weak relations between these activities and victimisation. As bivariate results indicate only identity theft was strongly associated with CNP fraud victimisation. As it will be discussed below, online activities were associated with online identity theft, which supports the first hypothesis stating that there is an indirect relation between online activities and CNP fraud victimisation and identity theft acts as a bridge.

6.4 The Relation between Online Activities, Identity Theft and CNP Fraud Victimisation

'Using online government services', 'buying goods or services', 'using online banking or managing finances', 'using complex passwords', 'using a different password for each different online account', 'protecting home wireless connection (Wi-Fi) with a password' and 'experiencing a computer virus' appeared to be significant predictors of Identity Theft. As it was assumed risky online activities (using online government services, buying goods or services online, using online banking or managing finances) increased the risk of victimisation. While buying goods or services increased the risk of victimisation by about 135% (Exp (B)=2.352), using online government services increased the likelihood of victimisation by 83% (Exp (B)=1.838). Reyns (2013) who analysed British Crime Survey England and Wales 2008/2009, found that using the Internet for banking and managing finances and shopping online increase the risk of Identity Theft victimisation. The results of

this dissertation and Reyns (2013) indicate that using online banking increases the risk of identity theft victimisation by around 50%; however, whereas this dissertation found that online shopping increase the risk of victimisation by about 135%, Reyns (2013) found that online purchasing increases the likelihood of victimisation by 30%. Hence, shopping online is riskier than 2008. This increase in the likelihood of victimisation caused by online purchasing may be attributed to the growth in e-commerce. According to Office for National Statistics report (2014) e-commerce sale increased from £335 billion to £492 between 2008 and 2012. Hence, the more Internet users expose their personal information, the more likely they would be the victims of Identity Fraud.

Using guardianship measures increased the chance of victimisation, which is contrary to LRAT perspective. Whereas those who use complex passwords were 71% more likely to be victimised, those who use different passwords for each different online account were 47% more likely to be victimised. On the other hand, protecting the home wireless connection decreased the risk of victimisation by approximately 38%, a result that lends support to LRAT. This result appears to account for the results of exposure to motivated offender and target suitability components of LRAT since using the insecure Internet connection increases the likelihood of exposure to motivated offender and target suitability, which increases the risk of victimisation.

Overall, Identity theft appeared to be the most important precursor to CNP fraud victimisation (Wall, 2013). The binary logistic regression model that test, the relation between online identity theft and card-not-present fraud indicates that experiencing online identity theft increase the risk of CNP fraud victimisation by 600%. The personal information gained by identity theft is used to commit CNP fraud (Archer et al., 2012; Roberts et al., 2013). This result appears to support the hypothesis, which assumes a relation between identity theft and CNP fraud victimisation.

With regards to theoretical implications of this dissertation, results appear to support Life-style Routine Activities Theory since online routine activities such as purchasing goods online, using online banking and using online banking emerged to increase the risk of victimisation. Hence, credit card users' online lifestyles prepare suitable conditions for victimisation. Results pertaining to guardianship measures require special attention: whereas 'using different passwords for each online account' and 'using complex passwords' appear to increase the risk of victimisation, 'protecting home wireless connection' emerged to decrease the risk of victimisation. These results would indicate that most of the security measures applied by credit card users are not '*capable guardians*'. Hence, implementing such security methods increase the risk of victimisation. As Ngo and Paternoster (2011) argues using ineffective security methods create a false sense of security, which leads engaging in riskier online activities that cause victimisation.

6.5 Offline Correlates of Card-not-present Fraud

It is hypothesised that responding to fraudulent request or sending/transferring money, as a response to such fraudulent requests would increase the risk of CNP fraud victimisation. '*Responding an urgent request to help someone get out of some sort of financial trouble*' appeared to be significant predictor of CNP fraud victimisation. Those who responded to such a request were about 360% more likely than those who did not respond to such a request to be victimised. This result partly support the assumption of facilitation since only one factor out of seven factors appeared to be statistical predictor of CNP fraud victimisation.

Overall, as it can be seen more online activities than offline activities are correlated with CNP fraud victimisation, which shows that although card-not-present fraud is committed in both domains, perpetrators prefer online methods to access personal information.

6.6 The Effect of Fear of CNP Fraud Victimisation and Past Victimisation on Behavioural Adaptation

With regards to online behavioural adaptations, whereas credit card users with fear of CNP fraud were more likely to avoid purchasing items on the Internet, credit card users who experienced CNP fraud victimisation were less likely to avoid online shopping. This means that fear of crime has a stronger impact than previous victimisation experience on behavioural adaptation in cyberspace. This result is consistent with previous studies demonstrating that persons with high-risk perception made fewer online purchases (Reisig et al., 2009; Forsythe and Shi, 2003).

Pertaining to offline behavioural adaptation, credit card users who have fear of CNP fraud and those who experienced CNP fraud victimisation were less likely to change offline behaviours. While those with fear of CNP fraud were 20%, respondents who experienced CNP fraud victimisation were 25% more likely avoid using cash points. Similarly, Rountree and Land (1996) also found that those with fear of crime and those faced burglary showed similar behavioural patterns. This result contradicts Ferraro' (1995) risk interpretation model, which proposes that fear of crime cause behavioural changes and other fear of crime studies demonstrating that past victimisation and fear of crime cause behavioural changes (Gala and Coupe, 2005; Averdijk, 2011; Rengifo and Bolton, 2012). Rengifo and Bolton (2012) found that people with high perception of risk are more likely to alter their leisure or voluntary activities. Averdijk (2011) found that previous violent victimisation was associated with less shopping and victimisation with injuries related with spending decreased the amount of time outside.

Females were more likely to change behaviours than males in both domains. Females were 30% more likely to avoid purchasing and 27 % more likely to stop using cash points than males. Gale and Coupe (2005) found that females who faced street robbery were more

inclined to change their behaviours than males after experiencing victimisation. People younger than 60 were less likely to change their behaviours in both worlds compared to people over 60. This result is in line with previous victimisation studies arguing that elderly people are more fearful than young people and they tend to avoid behaviours that may lead victimisation (Cook et al., 1981; Reisig et al., 2009) but Henson et al (2013) found that young people are more fearful of online crime than elderly people.

6.7 The Effect of Fear of CNP Fraud Victimisation and Past Victimisation on Guardianship Measures

With regards to online guardianship measures, both fear of CNP fraud and past CNP victimisation increased the guardianship measures. Odds Ratio values pertaining to analyses indicate that credit card users increase their guardianship measures between 20% and 67%. Interestingly, whereas fear of CNP fraud appeared to be statistically significant predictor of having a separate card for online purchases, previous CNP fraud victimisation did not emerge as a statistically significant indicator of this guardianship measure. This result appears to differentiate between the public perception of card-not-present fraud and the '*reality*' of card-not-present fraud. Many online security forums (e.g. stopidfrauds.com, nerdwallet.com) and banks (e.g. bank of America) suggest using a separate credit card to prevent CNP fraud victimisation. There appear to be a public misperception about the preventive effect of using separate card. Hence it is not surprising that those with fear of CNP fraud tend to use a separate credit card for online purchases. However, those who faced CNP fraud victimisation may have found this security measure to be ineffective based on their previous victimisation experiences.

When we compare the effect of fear of CNP and previous CNP victimisation experience on preventive actions, those who experienced CNP fraud were more likely to

increase their guardianship measures. For instance, whereas credit card users who had fear of crime were approximately 30% more likely to purchase items from secure websites, which means that those who experienced a victimisation are more cautious in the online environment.

Gender appeared to be only significant predictor of two online guardianship measures (using computer security measures and having a separate card for online purchases). Males are more likely to take preventive measures than females in cyberspace. In regards to age, there seems to be a trend. The older credit card users are, they are more likely to increase security measures such as using computer security measures, only purchasing items from secure websites and they are less likely to increase security measures such as regularly checking transactions on bank statements and only using a credit card rather than a debit card online.

The comparison of online guardianship results with the online behavioural adaptation results seems to suggest that credit card users who have fear of CNP fraud are more likely to change behaviours and less likely to take more preventive actions when compared to credit card users who have experienced CNP fraud victimisation. Following that line of logic, it would be argued that whereas fear of crime leads behavioural adaptations, previous victimisation causes increased preventive measures to avoid victimisation in cyberspace.

The comparison of the effect of fear of CNP fraud and previous CNP fraud victimisation on offline behaviours appear to indicate that whereas credit card users with both fear of crime and previous victimisation less likely to change their behaviours, they are more likely to increase offline guardianship measures. Hence, it can be argued that fear of CNP fraud and past victimisation experience have the effect on preventive measures rather than behavioural adaptation in real the word. These results appear to partially support the

second hypothesis stating that fear of CNP fraud and past victimisation cause both behavioural adaptations and increase in preventive measures.

With regards to offline guardianship measures, fear of CNP fraud and previous CNP fraud victimisation appeared to be significant predictors of offline guardianship measures. Credit card users with CNP fraud and those who experienced CNP fraud increased their offline security measures. Whereas females were more likely to keep the record of PIN number separately from cards and shield PIN number in cash points/in shops, males were more likely to frequently change PIN numbers and keep the card in view while using the card. The results related to age yields a similar trend with online guardianship measures. Whereas older people tend to frequently change PIN number and keep the card in view, younger people tend to keep the record of PIN number separately from the card.

7.1 Conclusions and Policy Implications

Life-style Routine Activities theory postulates that persons' routine activities and their life-styles create opportunities for motivated offenders. As a theoretical framework, LRAT provided a systematic approach to investigate correlates of card-not-present fraud. This dissertation has found a partial support for the application of LRAT perspective to cybercrimes. Whereas as credit card users legitimate online behaviours and devices used to access the Internet emerged to increase the risk of victimization, results pertaining to the guardianship measures indicate that not all online security measures capable guardians and implementing these preventive measures would boost the risk of victimization. Moreover, online identity theft appeared to be the strongest correlates of card-not-present fraud victimization and some legitimate online activities such as online purchasing emerged to be associated with online identity theft. Fear of CNP and previous CNP fraud victimization showed alternating impacts on online and offline behaviours. Whereas fear of crime caused behavioural adaptations, previous victimization leads more preventive actions in cyberspace.

This dissertation provided important insight for policy makers and law enforcement bodies policing card-not-present fraud. Firstly, Situational Crime Prevention Approach underscores the need for exploring crime specific correlates to prevent victimization. This dissertation has found out that some legitimate online activities such as using online banking or shopping online precipitate victimization. Banks and other e-commerce institutions would focus on developing new methods to prevent misuse of their systems by perpetrators. Secondly, fear of CNP fraud and previous victimization experience test results indicate that fear is more effective than previous victimization on preventive measures. Hence

governmental bodies as well as financial institutions could initiate public educational programs that increase public awareness about the risks of CNP fraud victimization. Lastly, results indicate that victims reported their victimization to banks or credit card companies rather than policing bodies such as police or Action Fraud. This may indicate the lack of public knowledge about activities and capabilities of policing bodies to combat CNP fraud victimization. Hence, these organizations would launch more programs to inform the public about their actions and capabilities in fighting CNP fraud victimization.

7.2 Limitations and Recommendations for Future Studies

This dissertation has several limitations that worth consideration. First, unfortunately Crime Survey England and Wales 2013/2014 does not contain questions related to deviant online behaviours such as illegal downloading, computer hacking, viewing adult sites and online gambling. Many cybercrime studies have identified deviant online behaviour as an important predictor of online victimisation (Choi, 2008; Holt and Bossler, 2009; Reyns et al., 2011). Including such questions into the forthcoming series of Crime Survey would help researchers to investigate the phenomenon of CNP fraud in depth. Second, Crime Survey England and Wales 2013/2014 is a cross-sectional survey, hence, this dissertation could measure the immediate effect of fear of CNP fraud and previous victimisation on behavioural adaptation and preventive actions. A longitudinal study would measure the long lasting effects of the fear of crime and previous victimisation experience. Third, this dissertation is only focused on card-not-present fraud victimisation; however, other online payment methods are gaining popularity (Wordpay Report, 2012). For instance, e-commerce companies such as Amazon.com, Yahoo and Apple offer an alternative payment method called E-wallet or digital wallet, which requires creating an account and loading your credit card details into that account, to prevent CNP fraud victimisation. Smartphone or mobile phone based payment methods are also becoming available to costumers (Andreev et al., 2012). Future studies may

attempt to find out the challenges caused by the usage of new online payment methods. Lastly, the results of this study indicate that although some credit card users have fear of card-not-present fraud victimization, they do not stop online purchasing, which can be considered as a sign of trust. This dissertation has not researched the relation between trust and online activities of Internet users. Future studies could also focus on the underlying causes of credit card users' trust in e-commerce and online payment methods as well as the relation between trust and the use of online payment methods.



APPENDIX A**OPERATIONALIZATION****Online Correlates of Card-not-present Fraud****Dependent Variables:**

Card-not-present Fraud (QCRDUSE): Respondents who approved that they own a credit card were asked if their credit cards have been used “without their permission or prior knowledge” (CSEW Questionnaire, p. 151). Although this question measures remote purchase or card-not-present fraud victimisation, the cause of their victimisation can not be totally attributed to respondents’ online or offline behaviours since there is a possibility that their credit card was lost or stolen before victimisation. Actually two other questions (QFRSTOL and QFRSTOL2) ask respondents if their credit cards or anything else were stolen before victimisation (CSEW Questionnaire, p. 152). In order to prevent confusion, the respondents who said YES to all three questions were excluded from the dependent variable by using recode into different variable command in SPSS software. The recoding done in the following way:

- a. Credit card used without permission/ prior knowledge and credit card NOT stolen before victimisation - coded as 1.
- b. Credit card used without permission/ prior knowledge and credit card stolen before victimisation - coded as 0.

Hence, I obtained a dependent variable that composed of respondents whose victimization may be facilitated by their own actions.

Online Identity Theft (EEXPINT C): Respondents who approved that they have used the Internet in the last 12 months were asked if they have experienced “unauthorised

access to/use of personal data (e.g. e-mail account/bank account)” in the last 12 months (CSEW Questionnaire, p. 143).

Dependent Variable			
Variable Name	Variable	Coding	Question
QCRDUSE	Card-not-present Fraud	NO=0 YES=1	In the last 12 months, that is since the first of [DATE], have any of your cards been used without your permission or prior knowledge to take money from your bank or building society accounts or to charge money to your credit or debit cards?

Table A.1: Dependent Variables for Online Correlates of Card-not-present Fraud

Independent Variables:

Exposure to Motivated Offender: Cohen et al. (1981) argue that the more persons are exposed to motivated offender, the more likely they become victim of a crime. Spending time out of home a night (Dugan and Apel, 2003; Miethe and Meier, 1990), associating with delinquent friends (Shreck and Fisher, 2004) are the terrestrial factors that increase the exposure to motivated offender. With regards to card-not-present fraud, experiencing a computer virus or unauthorised access to/use of personal data (van Wilsem 2013; Choi, 2008; Bossler and Holt, 2011) and the Internet users’ online activities or online life-style increase (Paternoster 2011; Holt and Bossler, 2013) increase the chance of exposure to motivated offender. The Crime Survey England and Wales 2013/2014 asks the reason of the Internet usage in the last 12 months in Online Security section of the survey (CSEW Questionnaire, p. 143) and measures the existence of 7 reasons. Another question asks if the respondents have experienced “a computer virus” or unauthorised access to/use of personal data (e.g. e-mail

account/bank account)” (CSEW Questionnaire, p. 143).

The variables that operationalize exposure to motivated offender component of the theory were grouped into three categories to better understand the effect of different kind of online activities on card-not-present fraud victimisation. Online activities were divided into two categories ‘*Using Internet for Financial Activities*’ and ‘*Using Internet for Leisure/Social Activities*’. Hence it can be observed if the online activities that may be considered as ‘*risky*’ and ‘*non-risky*’ increase risk of victimisation. The first group hypothesised to be risky since the Internet users reveal their personal information while using the Internet for that specific reason. For instance, the Internet users enter they credit card details while purchasing goods online. The third group ‘Internet Related Factors’ was composed of questions related to the Internet usage and computer integrity crimes. The computer integrity crimes increase the exposure to motivated offender by decreasing or stopping security measures of networked systems. Hence, these two illegal actions were operationalized as exposure to motivated offender measure.

EXPOSURE TO MOTIVATED OFFENDER			
Variable Name	Variable	Coding	Question
Using the Internet for Financial Activities			
EUSINT3A	Online banking or managing finances	NO=0 YES=1	Looking at this card which, if any, of the following things have you used the Internet for in the last 12 months?
EUSINT3B	Buying goods or services	NO=0 YES=1	
EUSINT3C	Online government services	NO=0 YES=1	
Using the Internet for Leisure/Social Activities			
EUSINT3D	Social networking or blogging	NO=0 YES=1	Looking at this card which, if any, of the following things have you used the Internet for in the last 12 months?
EUSINT3E	E-mail, instant messaging, chat rooms	NO=0 YES=1	
EUSINT3F	Browsing for news or information	NO=0 YES=1	
EUSINT3G	Playing online games/doing quizzes/competitions	NO=0 YES=1	
The Internet Related Factors			
INTERN1	Used internet at home or elsewhere in last 12 months	NO=0 YES=1	Have you used the Internet, at home or elsewhere, in the last 12 months?
EEXPINTA	Experienced a computer virus	NO=0 YES=1	In the last 12 months, have you personally experienced any of the things mentioned on this card while using the internet?
EEXPINTC	Experienced an unauthorised access to/use of personal data	NO=0 YES=1	

Table A.2:Independent Variables for Exposure to Motivated Offender

Suitable Target: The Internet users some online activities as well as devices they used to access the Internet may increase the risk of being card-not-present fraud victimisation due to some security deficiencies caused by the devices. For instance, perpetrators use public Wi-Fi or they establish bogus internet hot spots to steal information from the Internet users

(Cheng et al., 2013) and using a laptop away from home to access the Internet may require using an insecure public Wi-Fi, which prepares suitable conditions for perpetrators. Recent studies have revealed that smartphone or mobile phones and handheld computers such as tablets pose a great threat to their users due to breaches in their security methods (Tajpour et al., 2013; El-Din et al., 2015). Hence, using an inappropriate device to access the Internet may make us a suitable target for a hacker. In other words, the devices that use to access the Internet may increase target suitability. Crime Survey England and Wales 2013/2014 asks respondents which devices they have used to access the Internet in the last 12 months (CSEW Questionnaire, p. 142). Thus, this question is used to operationalize target suitability component of the LRAT.

The devices used to access the Internet were divided into two categories. The devices that considered having poor security measures against online threats were grouped into the '*High-risk Devices*' category. Other devices that considered having strong security measures or whose primary use is not to access the Internet were grouped into the '*Low-risk Devices*' category.

TARGET SUITABILITY/DEVICES USED TO ACCESS THE INTERNET			
Variable Name	Variable	Coding	Question
High Risk Devices			
INTRUS2C	Laptop away from home and work or school/college	NO=0 YES=1	Which of these have you used in the last 12 months to access the internet?
INTRUS2E	Handheld computer	NO=0 YES=1	
INTRUS2D	Mobile phone or Smartphone	NO=0 YES=1	
INTRUS2H	Public access computer (e.g. In a library, internet cafe)	NO=0 YES=1	
Low Risk Devices			
INTRUS2B	Laptop, at home or work or school/college	NO=0 YES=1	Which of these have you used in the last 12 months to access the internet?
INTRUS2A	Desktop computer (at home or work or school/college)	NO=0 YES=1	
INTRUS2F	Games console	NO=0 YES=1	
INTRUS2G	Digital TV	NO=0 YES=1	

Table A.3:Independent Variables for Target Suitability

Absence of Capable Guardianship: Life-style Routine Activities Theory postulates that the presence of a capable guardian would decrease the risk of victimisation. Crime Survey England and Wales 2013/2014 asks respondents which security methods they use to keep safe online (CSEW Questionnaire, p. 149). In the cybercrime literature guardianship measures are divided into two categories: personal and digital guardianship (Ngo and Paternoster, 2011; Van Wilsem, 2013; Holt and Bossler, 2013). This study also divided the security methods into two categories. The first category, '*Digital Guardianship*', included

computer automated security measures that are used to protect personal information. The second category, '*Personal Guardianship*', included human based security measures.

Control Variables: Socio-demographics, age, gender, having any qualification, running own business, working in a paid job and ethnicity were added as control variables to binary logistic regression model.

The Relation between Online Action and Identity Theft

Dependent Variable: Online Identity Theft (EEXPINT C), Respondents who approved that they have used the Internet in the last 12 months were asked if they have experienced “unauthorised access to/use of personal data (e.g. e-mail account/bank account)” in the last 12 months (CSEW Questionnaire, p. 143).

ABSENCE OF A CAPABLE GUARDIANSHIP			
Variable Name	Variable	Coding	Question
Digital Guardianship			
EPRODE3A	Install anti virus or other security software	NO=0 YES=1	Looking at this card, which of these things do you typically do to keep yourself safe online, including protecting your personal details on the internet?
EPRODE3B	Install a firewall on your computer	NO=0 YES=1	
EPRODE3C	Download software updates and patches whenever prompted	NO=0 YES=1	
Personal Guardianship			
EPRODE3D	Use complex passwords (contain letters, numbers and symbols)	NO=0 YES=1	Looking at this card, which of these things do you typically do to keep yourself safe online, including protecting your personal details on the internet?
EPRODE3E	Use a different password for each different online account	NO=0 YES=1	
EPRODE3F	Check for signs that a site is secure when buying online (closed padlock sign/https website address)	NO=0 YES=1	
EPRODE3G	Protect your home wireless connection (wi-fi) with a password	NO=0 YES=1	
EPRODE3H	Delete suspicious emails without opening them	NO=0 YES=1	
EPRODE3I	Log out of websites when you are finished	NO=0 YES=1	
EPRODE3J	Be cautious using public wi-fi / insecure wi-fi	NO=0 YES=1	
EPRODE3K	Only use credit cards (not debit or charge cards)	NO=0 YES=1	

Table A.4: Independent Variables for Absence of a Capable Guardianship

CONTROL VARIABLES			
Variable Name	Variable	Coding	Question
AGE	Age of the Respondents	Under 25=0 Between 25-40=1 Between 41-59=3 Over 60=4	
SEX	Gender of the Respondents	Female=0 Male=1	
EDUCINT	Having Any Qualification	No=0 Yes=1	
WORK2	Employment	No=0 Yes=1	
OWNBUS2	Running Own Business	No=0 Yes=1	
ETHGRP	Ethnicity	Non-white=0 White=1	

Table A.5: Control Variables

Dependent Variable			
Variable Name	Variable	Coding	Question
EEXPINTB	Online Identity Theft	NO=0 YES=1	In the last 12 months have you personally experienced any of the things mentioned on this card while using the Internet?

Table A.6: Dependent Variables for Online Identity Theft

Independent Variables: All variables used to explore the relationship between online activities and card-not-present fraud also used to investigate the relation between these activities and online identity theft.

Independent Variables			
Variable Name	Variable	Variable Name	Variable
EXPOSURE TO MOTIVATED OFFENDER		ABSENCE OF A CAPABLE GUARDIANSHIP	
EUSINT3A	Online banking or managing finances	EPRODE3A	Install anti virus or other security software
EUSINT3B	Buying goods or services	EPRODE3B	Install a firewall on your computer
EUSINT3C	Online government services	EPRODE3C	Download software updates and patches whenever prompted
EUSINT3D	Social networking or blogging	EPRODE3D	Use complex passwords (contain letters, numbers and symbols)
EUSINT3E	E-mail, instant messaging, chat rooms	EPRODE3E	Use a different password for each different online account
EUSINT3F	Browsing for news or information	EPRODE3F	Check for signs that a site is secure when buying online (closed padlock sign/https website address)
EUSINT3G	Playing online games/doing quizzes/competitions	EPRODE3G	Protect your home wireless connection (wi-fi) with a password
TARGET SUITABILITY/DEVICES USED TO ACCESS THE INTERNET		EPRODE3H	Delete suspicious emails without opening them
INTRUS2A	Desktop computer (at home or work or school/college)	EPRODE3I	Log out of websites when you are finished
INTRUS2B	Laptop, at home or work or school/college	EPRODE3J	Be cautious using public wi-fi / insecure wi-fi
INTRUS2C	Laptop away from home and work or school/college	EPRODE3K	Only use credit cards (not debit or charge cards)
INTRUS2D	Mobile phone or Smartphone		
INTRUS2E	Handheld computer		
INTRUS2F	Games console		
INTRUS2G	Digital TV		
INTRUS2H	Public access computer (e.g. In a library, internet cafe)		

Table A.7: Independent Variables for Online Identity Theft

Control Variables: Demographic characteristics such as age, gender, personal income, and education level, having a qualification, having a paid work and running own business were added as control variables into model.

CONTROL VARIABLES			
Variable Name	Variable	Coding	Question
AGE	Age of the Respondents	Under 25=0 Between 25-40=1 Between 41-59=3 Over 60=0	
SEX	Gender of the Respondents	Female=0 Male=1	
EDUCINT	Having a qualification	No Qualification=0 Having a qualification=1	
OWNBUS2	Running Own Business	No Running own business=0 Running own business=1	
WORK2	Employment	No paid job=0 Having a paid job=1	

Table A.8: Control Variables for Online Identity Theft

The Relation between Online Identity Theft and Card-not-present Fraud:

Dependent Variable: Card-not-present fraud victimisation (QCRDUSE) was the dependent variable to explore the relation between online identity theft and card-not-present fraud.

Independent Variables: Online Identity Theft (EEXPINTC) was the dependent variables. Socio-demographics were also included as control variables.

Independent Variable			
Variable Name	Variable	Coding	Question
EEXPINTC	Online Identity Theft	NO=0 YES=1	In the last 12 months have you personally experienced any of the things mentioned on this card while using the Internet?
RECODED_AGE	Age of the Respondents	Under 25=0 Between 25-40=1 Between 41-59=3	
SEX	Gender of the Respondents	Female=0 Male=1	
EDUCINT	Having Any Qualification	No=0 Yes=1	
WORK2	Employment	No=0 Yes=1	
ETHGRP	Ethnicity	Non-white=0 White=1	

Table A.9: Independent Variables for Online Identity Theft

Offline Correlates of Card-not-present Fraud

Dependent Variable: Card-not-present Fraud (QCRDUSE), The same dependent variable was used to determine the offline correlates of card-not-present fraud.

Independent Variables: Fraudsters use many types of scams to gain personal information of credit card users. Telemarketing fraud, advance fee schemes, ponzi schemes and pyramid schemes are the most common scams that perpetrators use to defraud people (FBI, 2015). Crime Survey England and Wales 2013/2014 contains questions about different types of fraud victimisation in Mass-marketing Fraud Module. These questions ask respondents if they have responded to a communication about a fraudulent activity or participated to a fraudulent activity in the last 12 months (CSEW Questionnaire, p. 149).

OFFLINE CORRELATES OF CARD-NOT-PRESENT FRAUD			
Variable name	Variable	Coding	Question
LOTTO2A	Responding communication about financial details	NO=0 YES=1	Have you replied to one of these requests in the last 12 months? • Send or transfer money (e.g. Western union, ukash) • Provide bank details • Provide any other financial details (e.g. Credit card, paypal account) • Provide any other personal information (e.g. Address, passport number) • To contact them/someone else
LOTTO3A	Provided bank details	NO=0 YES=1	Did you provide your bank details as requested
LOTTO5	Sent off or transferred money as requested in response to a win in a lottery or other competition	NO=0 YES=1	In the last 12 months have you sent off or transferred any money as requested in response to a win in a lottery or other competition that you haven't entered?
ANYFRAUDB	Responding to communication about investment with a guaranteed high return	NO=0 YES=1	In the last 12 months have you responded to any communication/s about any of the following: the change to make an investment with a guaranteed high return
INVEST1	Sent off or transferred money as requested in connection with a guaranteed high return investment	NO=0 YES=1	In the last 12 months have you sent off or transferred any money in connection with a guaranteed high return investment?
ANYFRAUDD	Responding to communication about help in moving large sums of money from abroad	NO=0 YES=1	In the last 12 months have you responded to any communication/s about any of the following: help in moving large sums of money from abroad
ANYFRAUDF	Responding to communication about an urgent request to help someone get out of some sort of financial trouble	NO=0 YES=1	In the last 12 months have you responded to any communication/s about any of the following: an urgent request to help someone get out of some sort of financial trouble

Table A.10: Independent Variables for Offline Correlates of CNP Fraud

The Impact of The Fear of Card-not-present Fraud and Past CNP Victimization

The Effect of Fear of Card-not-present Fraud and Past CNP Victimization on Online and Offline Behaviours:

Dependent Variables: Crime Survey England and Wales is a cross-sectional survey, which is conducted every year with different participants. However, in order to measure the effect of fear of card-not-present fraud on behaviours and guardianship measures, there should be a time ordering between victimisation and behavioural changes and guardianship measures taken. Crime Survey England and Wales 2013/2014 asked the respondents who used at least one credit card: *“nowadays, do you typically do any of the following to avoid someone obtaining your bank, building society or credit card account details?”* (CSEW Questionnaire, p. 155). Since the question that measures card-not-present fraud victimisation asked the respondents any victimisation experienced *‘within 12 months’* and this question asked the actions taken *‘nowadays’*, there is a time ordering between two questions. Hence, this questions measures actions taken after victimisation. The respondents were expected to select one or more action from seventeen choices. Whereas some of these choices represent behavioural changes in real world and cyberspace, some other represents online and offline security measures taken to prevent victimisation. In order to measure the impact of fear of card-not present fraud and past card-not-present fraud victimisation in both domains, the variables were divided into two categories, *online and offline*. Then, dependent variables were categorised according to being *‘a behavioural adaptation’* or *‘guardianship measure’*. While online behavioural change was operationalized with avoiding purchasing items on the Internet, offline behavioural change was operationalized with never using cash points.

THE EFFECT OF FEAR OF CNP FRAUD VICTIMISATION AND PAST VICTIMISATION ON BEHAVIOURS			
Variable Name	Variable	Coding	Question
Online			
QPREC2A	Avoid purchasing items on internet	NO=0 YES=1	Nowadays, do you typically do any of the following to avoid someone obtaining your bank, building society or credit card account details?
Offline			
QPREC2F	Never use cash points	NO=0 YES=1	Nowadays, do you typically do any of the following to avoid someone obtaining your bank, building society or credit card account details?

Table A.11: Dependent Variables for Fear of CNP Fraud and Previous CNP Fraud Victimization-Behaviours

Independent Variables:

Fear of Card-not-present Fraud: Scholars have operationalized the level of the fear of crime with a question that asks ‘*how worried the respondent about something*’ (Keane, 1998; Kanan and Pruitt, 2002; Jackson, 2006; Gray et al., 2008). Crime Survey England and Wales 2013/2014 asked the respondents: “How worried are you about someone using your credit cards or bank cards, or using your card details to buy things or withdraw cash without your permission?” (CSEW Questionnaire, p. 155). The survey question contained a four-point

response scale 1 (Very worried), 2 (Fairly worried), 3 (Not very worried), 4 (Not at all worried). In order to get a better assessment the variable was dichotomised by combining the first two categories and last two categories into one category. Hence whereas 1 referred to 'Worried', 0 referred to 'Not worried'.

Past CNP Fraud Victimization: The variable **QCRDUSE**, which was explained as the dependent variable above, was used as a past victimisation variable.

FEAR OF CNP FRAUD VICTIMISATION			
Variable Name	Variable	Coding	Question
QCARDW	Fear of Card-not-present Fraud	<u>Original coding:</u> Very worried=1 Fairly worried=2 Not very much worried=3 Not at all worried=4 <u>Dichotomized coding:</u> Not worried=0 Worried=1	How worried are you about someone using your credit cards or bank cards, or using your card details to buy things or withdraw cash without your permission?
QCRDUSE	Past card-not-present Fraud Victimization	NO=0 YES=1	In the last 12 months, that is since the first of (DATE), have any of your cards been used without your permission or prior knowledge to take money from your bank or building society accounts or to charge money to your credit or debit cards?

Table A.12: Independent Variables for Fear of CNP Fraud and Previous CNP Fraud Victimization-Behaviours

Control variables: Socio-demographics age and gender were added as control variables to assess the effect of fear of card-not-present fraud and past CNP fraud victimisation on behavioural adaptations and guardianship measures while holding these two variables constant. Hence it would be possible to remove the effect of two demographics from the binary logistic regression model.

CONTROL VARIABLES			
Variable Name	Variable	Coding	Question
AGE	Age of the Respondents	Under 25=0 Between 25-40=1 Between 41-59=3	
SEX	Gender of the Respondents	Female=0 Male=1	

Table A.13: Control Variables for Fear of CNP Fraud and Previous CNP Fraud Victimisation-Behaviours

The Effect of Fear of Card-not-present Fraud and Past CNP Victimization on Guardianship Measures

Dependent Variables: As explained above, the question, “*nowadays, do you typically do any of the following to avoid someone obtaining your bank, building society or credit card account details?*” (CSEW Questionnaire, p. 155), measures guardianship methods as well as behavioural changes. Guardianship methods were divided into two groups: online and offline guardianship measures. Firstly, online guardianship variables put into model to measure the effect of fear of card-not-present fraud victimisation and past card-not-present fraud victimisation on guardianship methods taken by credit card users.

Independent Variables: The independent variables and control variables used in previous analyses were used in these analyses also.

THE EFFECT OF FEAR OF CNP FRAUD VICTIMISATION AND PAST VICTIMISATION ON GUARDIANSHIP			
Variable Name	Variable	Coding	Question
ONLINE			
QPREC2B	Regularly check transactions on bank statements	NO=0 YES=1	
QPREC2H	Only use a credit card rather than a debit card online	NO=0 YES=1	
QPREC2I	Have a separate card for online purchases	NO=0 YES=1	
QPREC2J	Use computer security measures	NO=0 YES=1	Nowadays, do you typically do any of the following to avoid someone obtaining your bank, building society or credit card account details?
QPREC2K	Only purchase items from secure websites	NO=0 YES=1	
OFFLINE			
QPREC2C	Frequently change PIN number	NO=0 YES=1	
QPREC2D	Keep record of PIN number separately from cards/no record of PIN numbers kept	NO=0 YES=1	Nowadays, do you typically do any of the following to avoid someone obtaining your bank, building society or credit card account details?
QPREC2M	Shield PIN number at cash points/in shops/etc.	NO=0 YES=1	
QPREC2N	Keep card in view when paying in restaurants, etc.	NO=0 YES=1	

Table A.14: Dependent Variables for Fear of CNP Fraud and Previous CNP Fraud Victimisation-Guardianship

FEAR OF CNP FRAUD VICTIMISATION			
Variable Name	Variable	Coding	Question
QCARDW	Fear of Card-not-present Fraud	<u>Original coding:</u> Very worried=1 Fairly worried=2 Not very much worried=3 Not at all worried=4 <u>Dichotomized coding:</u> Not worried=0 Worried=1	How worried are you about someone using your credit cards or bank cards, or using your card details to buy things or withdraw cash without your permission?
QCRDUSE	Past card-not-present Fraud Victimization	NO=0 YES=1	In the last 12 months, that is since the first of (DATE), have any of your cards been used without your permission or prior knowledge to take money from your bank or building society accounts or to charge money to your credit or debit cards?

Table A.15: Independent Variables for Fear of CNP Fraud and Previous CNP Fraud Victimization-Guardianship

CONTROL VARIABLES			
Variable Name	Variable	Coding	Question
AGE	Age of the Respondents	Under 25=0 Between 25-40=1 Between 41-59=3	
SEX	Gender of the Respondents	Female=0 Male=1	

Table A.16: Independent Variables for Fear of CNP Fraud and Previous CNP Fraud Victimization-Guardianship

APPENDIX B**NATURE OF CARD-NOT-PRESENT FRAUD****Nature of Card-not-present Fraud, Demographics of Credit Card Users and Reporting Behaviour:**

Nature of Card-not-present fraud: As tables B.1 and B.2 illustrate, 5% of respondents reported card-not-present victimisation, which was the highest figure when compared to other types of self-reported victimization rates and 38% of victims received a refund for financial losses. These figures appear to contradict some scholars such as (Wall, 2008a; Wall, 2008b; Yar, 2006) who imply that the public perception of high cybercrime rates are media driven. On the other hand, the figures of financial losses support Wall (2007, p.167) who argues “De Minimism” is distinct characteristic of financial cybercrime.

SELF-REPORTED VICTIMISATION RATES	
Type of Victimisation	Percentage
Robbery	0.2*
Theft from Person	1*
Violent Crime	1.8*
Domestic Burglary	2.7*
Vehicle Related Theft	4*
Card-not-present	5.0
* Figures are taken from Statistical Bulletin of CSEW 2103/2014	
Table B.1: CNP Fraud Victimisation Rates	

How much money was lost when you experienced a loss of money in the last 12 months as a result of using the internet					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	None (i.e. all money was refunded)	72	.2	38.3	38.3
	Less than £50	21	.1	11.2	49.5
	£50 - £99	22	.1	11.7	61.2
	£100 - £249	32	.1	17.0	78.2
	£250 - £499	17	.0	9.0	87.2
	£500 - £999	6	.0	3.2	90.4
	£1,000 - £2,499	9	.0	4.8	95.2
	£2,500 - £4,999	4	.0	2.1	97.3
	£5,000 or more	3	.0	1.6	98.9
	Not yet resolved	2	.0	1.1	100.0
	Total	188	.5	100.0	
Missing	System	35183	99.5		
Total		35371	100.0		
Table B.2 Amount of Money Lost					

Demographics: Table B.3 summarizes the demographics characteristics, which will be used as control variables in analyses. In order to observe the possible difference in demographic patterns of credit card users, the figures were categorized according to victimization criteria.

Overall, the descriptive statistics related to demographics of credit card users who belong to certain age groups, have any qualification and run own business appear to be related with card-not-present fraud victimisation since the victimisation rates show bigger differences than other demographics. However, having these qualifications would not be the cause of their victimisation. There should be other factors such as online and offline life-style or guardianship methods that would be promoting victims precipitation in card-not-present fraud victimisation, which will be examined following sections.

Demographics of Credit Card Users					
		Frequency		Percent	
		Card-not-present Fraud Victimisation		Card-not-present Fraud Victimisation	
		Yes	No	Yes	No
Ethnicity	White	1019	21024	4.6	95.4
	Non-white	93	2226	4.0	96.0
Employment	No	378	10476	3.5	96.5
	Yes	734	12786	9.9	90.1
Running Own Business	No	341	9961	3.3	96.7
	Yes	10	91	9.9	90.1
Gender	Female	584	12685	4.4	95.6
	Male	528	10581	4.8	95.2
Having any qualifications	No	103	4601	2.2	97.8
	Yes	1009	18636	5.1	94.9
Highest qualification	Higher degree etc.	149	2222	6.3	93.7
	First degree etc.	222	3507	6.0	94.0
	Diplomas etc.	178	3164	5.3	94.7
	A/AS levels etc.	168	3122	5.1	94.9
	Trade Apprenticeships	44	1182	3.6	96.4
	O Level/GCSE grades A-C	171	3781	4.3	95.7
	O Level/GCSE grades D-G	39	728	5.1	94.9
Age	Under 25	84	1771	4.5	95.5
	Between 25-40	342	5673	5.7	94.3
	Between 41-59	433	7626	5.4	94.6
	Over 60	253	8196	3.0	97.0
Marital Status	Single	338	6855	4.7	95.3
	Married and living with husband/wife	562	10438	5.1	94.9
	In a same-sex civil partnership and living with partner	2	63	3.1	96.9
	Separated	48	846	5.4	94.6
	Divorced	113	2585	4.2	95.8
	Widowed	48	2417	1.9	98.1
Table B.3 Demographics of the Credit Card Users					

Reporting Behavior of CNP Victims: As table B. 4 demonstrates, card-not-present fraud victims were more likely to report the victimization to financial institutions such as banks and credit card companies. This result is consistent with Holtfreter et.al (2006) who found that 95% of fraud victims reported incidence to banks rather than police.

Reporting Behaviour of Card-not-present Fraud Victims			
Report the incident to		Frequency	Percent
Police	No	1367	94.7
	Yes	76	5.3
Action Fraud	No	1394	96.6
	Yes	49	3.4
Bank, building society, credit card company	No	704	48.8
	Yes	739	51.2
Someone else	No	1361	94.3
	Yes	82	5.7
Table B.4: Reporting Behaviour of Card-not-present Fraud Victims			

Emotional Effect of CNP Fraud Victimization and Fear of CNP Fraud Victimization: Whereas nearly %30 of respondents reported high levels of worry, about 47% of respondents reported fear of being a victim of card-not-present fraud (Tales B.5 and B.6). This result supports the findings of Henson et al. (2013), which demonstrate that people are not very fearful about being a victim of card-not-present fraud.

Emotional Effect of CNP Fraud					
		Frequency	Percent	Valid Percent	Cumulative Percent
	Very much	160	.7	11.1	11.1
	Quite a lot	265	1.1	18.4	29.5
	Just a little	581	2.4	40.3	69.8
	Not at all	436	1.8	30.2	100.0
	Total	1442	5.9	100.0	
Table B.5: Emotional Effect of CNP Fraud					

Fear of CNP Fraud Victimization					
		Frequency	Percent	Valid Percent	Cumulative Percent
	Very worried	3109	12.8	12.8	12.8
	Fairly worried	8329	34.2	34.2	46.9
	Not very worried	10002	41.0	41.1	88.0
	Not at all worried	2925	12.0	12.0	100.0
	Total	24365	99.9	100.0	
Table B.6: Fear of CNP Fraud Victimization					

REFERENCES:

- Akdeniz, Y. (2000)** *'Child Pornography'* in Akdeniz, Y., Walker, C. and Wall, D. S. (Eds.), *'The Internet, Law and Society'* Harlow: Longman
- Aneshensel, C. S. (2012)** *'Theory-Based Data Analysis for The Social Sciences'* Sage
- Andreev, P., Pliskin, N. and Rafaeli, S. (2012)** *'Drivers and Inhibitors of Mobile-Payment Adoption by Smartphone Users'* International Journal of E-Business Research (IJEER), Vol. 8(3), pp. 50-67
- Archer, N., Sproule, S., Yuan, Y., Guo, K. and Xiang, J. (2012)** *'Identity Theft and Fraud: Evaluating and Managing Risk'* Ottawa: University of Ottawa Press
- Averdijk, M. (2011)** *'Reciprocal Effects of Victimization and Routine Activities'* Journal of Quantitative Criminology, Vol. 27(2), pp. 125-149
- Averdijk, M. and Loeber, R. (2012)** *'The Role of Self-Control in The Link between Prior and Future Victimization: An Indirect Test'* International Review of Victimology, Vol. 18(3), pp. 189-206
- Bargh, J. A. and McKenna, K. Y. (2004)** *'The Internet and Social Life'* Annual Review of Psychology Vol. (55) pp.573–590
- BBC News (2011)** *'Citibank Confirms Hacking Attack'* Accessed on: 20/07/2015 Available at: <http://www.bbc.co.uk/news/technology-13711528>
- Becher, M., Freiling, F. C., Hoffmann, J., Holz, T., Uellenbeck, S. and Wolf, C. (2011)** *'Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices'* In Security and Privacy (SP), 2011 IEEE Symposium pp. 96-111
- Becker, K., Alper, O. and Lee, J. W. (2014)** *'Online Payment Security In E-Commerce: A New Approach To E-Payment Through Nfc Technology'* In 7th Annual Conference of the EuroMed Academy of Business Vol. 22 (3), pp. 218-233
- Becker, T. E. (2005)** *'Potential Problems In The Statistical Control Of Variables In Organizational Research: A Qualitative Analysis With Recommendations'* Organizational Research Methods Vol. 8(3) pp. 274-289

- Ben-Asher, N., Kirschnick, N., Sieger, H., Meyer, J., Ben-Oved, A. and Möller, S. (2011)** *'On the Need for Different Security Methods on Mobile Phones'* In Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services pp. 465-473 ACM
- Berg-Schlosser, D.B. and De Meur, G., Rihoux, B. and Ragin C.C. (2009)** *'Qualitative Comparative Analysis (QCA) as an Approach'* pp.1-19 In Rihoux, B. and Ragin, C.C. (Eds.) *'Configurational Comparative Methods: Qualitative Comparative Analysis and Related Techniques'* London: Sage Publications Ltd
- Bernard, Y. (1992)** *'North American and European Research on Fear of Crime'* Applied Psychology: An International Review, Vol. 41 pp. 65-75
- Bhatla, T. P., Prabhu, V. and Dua, A. (2003)** *'Understanding Credit Card Frauds'* Cards Business Review 2003: Tata Consultancy Services
- Bossler, A. M. and Holt, T. J. (2009)** *'On-Line Activities, Guardianship, and Malware Infection: an Examination of Routine Activities Theory'* The International Journal of Cyber Criminology, Vol.3 pp.400-20
- Bossler, A. M. and Holt, T. J. (2010)** *'The Effect of Self-Control on Victimization in the Cyberworld'* Journal of Criminal Justice, Vol. 38(3), pp. 227-236
- Bossler, A. M. and Holt, T. J. (2011)** *'Malware Victimization: A Routine Activities Framework'* In Jaishankar, K. *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior*. Boca Raton, FL: CRC, 2011, pp. 317-46
- Bossler, A. M. and Burruss, G. W. (2010)** *'The General Theory of Crime and Computer Hacking: Low Self-Control Hackers'* pp. 38-67 In Holt, T. J. and Schell, B. H. (Eds.) *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*. IGI Global
- Bouchard, M., Wang, W. and Beauregard, E. (2012)** *'Social Capital, Opportunity, And School- Based Victimization'* Violence and Victims, Vol. 27, pp. 656-673
- Brant, S. (2009)** *'Consumer Online Shopping Fears, Market Brief. First Data Corporation'* Accessed on 21.07.2015 Available at: http://www.firstdata.com/en_us/insights/consumer-online-shopping-fears-study.html

- Brenner, S. W. (2010)** *'Cybercrime: Criminal Threats from Cyberspace'* Santa Barbara, CA: Praege
- Brody, R. G., Mulig, E. and Kimball, V. (2007)** *'Phishing, Pharming And Identity Theft'* Academy of Accounting and Financial Studies Journal, Vol. 11(3) pp. 43-56
- Bryman, A. (1988)** *'Quantity and Quality in Social Research'* London: Routledge
- Bryman, A. and Cramer, D. (2001)** *'Quantitative Data Analysis with SPSS Release 10 for Windows'* New York: Routledge
- Bulakh, V. and Gupta, M. (2015)** *'Characterizing Credit Card Black Markets on the Web'* pp. 1435-1440 In Proceedings of the 24th International Conference on World Wide Web Companion International World Wide Web Conferences Steering Committee
- Bunch, J., Clay-Warner, J. and Lei, M. K. (2012)** *'Demographic Characteristics and Victimization Risk: Testing The Mediating Effects of Routine Activities'* Crime and Delinquency Vol. 20 (5) pp. 1-25
- Burgard, A. and Schlembach, C. (2013)** *'Frames of Fraud: A Qualitative Analysis of The Structure and Process of Victimization on The Internet'* International Journal of Cyber Criminology, Vol. 7(2), pp. 112-124
- Button, M., Lewis, C. and Tapley, J. (2009a)** *'Fraud Typologies and the Victims of Fraud Literature Review'* London, England: National Fraud Authority
- Button, M., Nicholls, C. M., Kerr, J. and Owen, R. (2014)** *'Online Frauds: Learning From Victims Why They Fall For These Scams'* Australian and New Zealand Journal of Criminology pp.1-18
- Casten, J. A. and Payne, B. K. (2008)** *'The Influence of Perceptions of Social Disorder and Victimization on Business Owners' Decisions to Use Guardianship Strategies'* Journal of Criminal Justice, Vol. 36(5), pp. 396-402

- Chang, M. L. and Wu, W. Y. (2012)** *'Revisiting Perceived Risk in the Context of Online Shopping: An Alternative Perspective of Decision-Making Styles'* *Psychology & Marketing*, Vol. 29(5) pp. 378-400
- Cheng, N., Wang, X., Cheng, W., Mohapatra, P. and Seneviratne, A. (2013)** *'Characterizing Privacy Leakage of Public Wifi Networks For Users on Travel'* In INFOCOM, 2013 Proceedings IEEE pp. 2769-2777
- Choi, K. (2008)** *'Computer crime victimization and integrated theory: An empirical assessment'* *International Journal of Cyber Criminology* Vol.2 pp.308-333
- Choi, K. S. (2011)** *'Cyber-Routine Activities: Empirical Examination of Online Lifestyle, Digital Guardians, and Computer-Crime Victimization'* In Jaishankar, K. *Cyber 'Criminology: Exploring Internet Crimes and Criminal Behavior'* Boca Raton, FL: CRC, 2011, pp.229-53
- Clarke, R. V. (1995)** *'Situational Crime Prevention'* *Crime and justice*, pp. 91-150
- Clarke, R. V. G. (1997)** *'Introduction to Situational Crime Prevention: Successful Case Studies'* pp. 53-70 in Clarke, R. V. (Ed.) *'Situational Crime Prevention: Successful Case Studies'* Monsey, NY: Criminal Justice Press
- Clarke, R. V. (1999)** *'Hot Products: Understanding, Anticipating, and Reducing Demand for Stolen Goods'* Police Research Series, Paper 112 London: Home Office
- Clough, J. (2010)** *'Principles of Cybercrime'* Cambridge, UK: Cambridge University Press
- Cook, T.D., Fremming, J. and Tyler, T. (1981)** *'Criminal Victimization of the Elderly: Validating the Policy Assumptions'* In *Progress in Applied Social Psychology* (G.M. Stephenson and J.M. Davis, eds.) New York; John Wiley
- Cohen, L. E. and Cantor, D. (1981)** *'Residential Burglary in the United States: Life-Style and Demographic Factors Associated with The Probability of Victimization'* *Journal of Research in Crime and Delinquency*, Vol. 18, pp. 113-127
- Cohen, L. and Felson, M. (1979)** *'Social change and crime rate trends: A Routine Activity Approach'* *American Sociological Review* Vol. (44) pp. 588-608

- Cohen, L. E., Kluegel, J. R. and Land, K. L. (1981)** *'Social Inequality and Predatory Criminal Victimization: An Exposition and Test of a Formal Theory'* American Sociological Review Vol. 46 No. 5 pp.505-24
- Copes, H., Kerley, K. R., Mason, K. A. and Van Wyk, J. (2001)** *'Reporting Behavior of Fraud Victims And Black's Theory of Law: An Empirical Assessment'* Justice Quarterly, Vol. 18, pp. 343–363
- Copes, H. and Vieraitis, L. (2009)** *'Identity Theft'* pp. 564-571 in Miller, J. M. (Ed.) (2009) *'21st Century Criminology: A Reference Handbook'* (Vol. 1). SAGE Publications
- Cornish, D. B. and Clarke, R. V. (1987)** *'Understanding Crime Displacement: An Application of Rational Choice Theory'* Criminology, Vol. 25 (4), 933- 947
- Council of Europe Convention on Cybercrime ETS.No.185 (2001)** *'Convention on Cybercrime'* Accessed on 12.07.2015 Available at: <http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>
- Croall, H. and Levi, M. (1999)** *'Corporate Victims'* Criminal Justice Matters Vol. 36(1) pp. 4-7
- Crow, I. and Semmens, N. (2007)** *'Researching Criminology'* McGraw-Hill Education (UK)
- CSEW Technical Report (2014)** *'Technical Report'* Accessed on:01.06.2015 Available at: <http://discover.ukdataservice.ac.uk/catalogue/?sn=7619>
- Curphey, M. (2015)** *'UK Credit and Debit Card Statistics'* Accessed on: 18.07.2015 Available at: <http://uk.creditcards.com/credit-card-news/uk-britain-credit-debit-card-statistics-international.php>
- Dai, B., Forsythe, S. and Kwon, W. S. (2014)** *'The Impact of Online Shopping Experience on Risk Perceptions and Online Purchase Intentions: Does Product Category Matter?'* Journal of Electronic Commerce Research, Vol. 15(1), pp. 13-24
- D'Alessandro, S., Girardi, A. and Tiangsoongnern, L. (2012)** *'Perceived Risk and Trust as Antecedents of Online Purchasing Behavior in The USA Gemstone Industry'* Asia pacific journal of marketing and logistics, Vol. 24(3), 433-460

- Davi, L., Dmitrienko, A., Liebchen, C. and Sadeghi, A. R. (2012)** *'Over-The-Air Cross-Platform Infection For Breaking mTAN-Based Online Banking Authentication'* In Black Hat Abu Dhabi Conference 2012 Accessed on:09/08/2015 Available at: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.392.6443&rep=rep1&type=pdf>
- Davis, J. P., Farnham, S. and Jensen, C. (2002)** *'Decreasing Online 'Bad' Behavior'* CHI'02 Extended Abstracts on Human Factors in Computing Systems pp. 718-719
- Drass, K. A. and Miethe, T. D. (2001)** *'Qualitative Comparative Analysis and the Study of Crime Events'* pp. 125-40 In R. F. Meirer, L. W. Kennedy, V. F. Sacco (Eds.) *'The Process and Structure of Crime: Criminal Events and Crime Analysis'* New Brunswick, NJ: Transaction
- Dugan, L. and Apel, R. (2003)** *'An Exploratory Study of The Violent Victimization of Women: Race/Ethnicity And Situational Context'* Criminology Vol. (41) pp. 959-980
- Dugan, L. (1999)** *'The Effect of Criminal Victimization on A Household's Moving Decision'* Criminology, Vol. 37, pp. 903-930
- Dyrud, M. A. (2005)** *'I Brought You A Good News': An Analysis Of Nigerian 419 Letters'* Proceedings of the 2005 Association for Business Communication Annual Convention pp. 20-25
- Eck, John E. and Ronald V. Clarke (2003)** *'Classifying Common Police Problems: A Routine Activity Approach'* Crime Prevention Studies Vol. (16) pp.7-39
- El-Din, R. S., Cairns, P. and Clark, J. (2015)** *'The Human Factor in Mobile Phishing'* pp. 53-65 In Dawson M. and Omar M. (Eds) *'New Threats and Countermeasures in Digital Crime and Cyber Terrorism'* IGI Global
- Emarketer (2014)** *'Retail Sales Worldwide Will Top \$22 Trillion This Year'* Accessed on: 15.07.2017 Available at: <http://www.emarketer.com/Article/Retail-Sales-Worldwide-Will-Top-22-Trillion-This-Year/1011765>

- Ewad, U. (2000)** *'Criminal Victimisation and Social Adaptation in Modernity: Fear of Crime in the New Germany'* pp. 166-199 In Hope, T. and Sparks, R. (Eds.) *'Crime, Risk, and Insecurity: Law and Order in Everyday Life and Political Discourse'* Abingdon, Oxon: Routledge
- FBI (2015)** *'Common Fraud Scams'* Accessed on 28/08/2015 Available at: <https://www.fbi.gov/scams-safety/fraud>
- Felson, M. and Clarke R.V. (1998)** *'Opportunity Makes the Thief'* Police Research Series Paper 98 London: Home Office
- Ferraro, K. F. (1995)** *'Fear of Crime: Interpreting Victimization Risk'* Albany: State University of New York Press, Albany
- Field, A. (2009)** *'Discovering Statistics Using SPSS'* London: Sage Publications
- Finch, E. (2007)** *'The Problem of Stolen Identity and the Internet'* pp. 29-43 in Jewkes, Y. (Ed.) (2007) *'Crime Online'* Devon: Willan Publishing
- Fisher, B. S., Daigle, L. E. and Cullen, F. T. (2010)** *'What Distinguishes Single Sexual Victims from Recurring Ones? The Role of Lifestyle-Routine Activities and First-Incident Characteristics'* Justice Quarterly, Vol. 27, pp. 102-129
- Forsythe, S., Liu, C., Shannon, D. and Gardner L. C. (2006)** *'Development of a scale to measure the perceived benefits and risks of online shopping'* Journal of Interactive Marketing, Vol. 20, pp. 55-75
- Forsythe, S. and Shi, B. (2003)** *'Consumer Patronage and Risk Perceptions in Internet Shopping'* Journal of Business Research, Vol. 56, pp. 867-875
- Gale, J. A. and Coupe, T. (2005)** *'The Behavioural, Emotional And Psychological Effects Of Street Robbery On Victims'* International Review of Victimology, Vol. 12(1), pp. 1-22
- Garg, V. and Nilizadeh, S. (2013)** *'Craigslist Scams And Community Composition: Investigating Online Fraud Victimization'* pp. 123-126 In Security and Privacy Workshops (SPW), 2013 IEEE

- Gheraouti-Hélie, S. (2013)** *'Cyber Power: Crime, Conflict and Security in Cyberspace'* (1st ed.) EFPL Press
- Gorard, S. (2002)** *'The Role Of Secondary Data in Combining Methodological Approaches'* Educational Review, Vol. 54(3), pp. 231-237
- Gottfredson, M. R. and Hirschi, T. (1990)** *'A General Theory of Crime'* Stanford, CA: Stanford University Press
- Grabosky, P. N. (2001)** *'Virtual Criminality: Old Wine in New Bottles?'* Social and Legal Studies, pp.243-9
- Grabosky, P. and Smith, R. (2001)** *'Telecommunication Fraud In The Digital Age: The Convergence of Technologies'* Crime and the Internet pp. 23-45
- Gray, E., Jackson, J. and Farrall, S. (2008)** *'Reassessing The Fear of Crime'* European Journal of Criminology Vol. 5(3) pp. 363-380
- Greckhamer, T., Misangyi, V. F. and Fiss, P. C. (2013)** *'The Two QCAs: From a Small-N To a Large-N Set Theoretic Approach'* Configurational theory and methods in organizational research Vol. (38) pp. 49-75
- Grofman, B. and Schneider, C.Q. (2009)** *'An Introduction to Crisp Set QCA, with a Comparison to Binary Logistic Regression'* Political Research Quarterly Vol.20 (2) pp.662-72
- Hakim, C. (1982)** *'Secondary Analysis and the Relationship between Official and Academic Social Research'* Sociology Vol. 16 (1) pp.12-28
- Hale, C. (1996)** *'Fear Of Crime: A Review of The Literature'* International review of Victimology Vol. 4(2) pp. 79-150
- Hassan, A. M., Kunz, M. B., Pearson, A. W. and Mohamed, F. A. (2006)** *'Conceptualization and Measurement of Perceived Risk in Online Shopping'* Marketing Management Journal, Vol. 16(1), pp. 138-147

- Helweg-Larsen, K., Schütt, N. and Larsen, H. B. (2012)** *'Predictors and Protective Factors for Adolescent Internet Victimization: Results from a 2008 Nationwide Danish Youth Survey'* *Acta paediatrica*, Vol. 101(5), pp. 533-539
- Henson, B., Reyns, B. W. and Fisher, B. S. (2013)** *'Fear of Crime Online? Examining The Effect of Risk, Previous Victimization, and Exposure on Fear of Online Interpersonal Victimization'* *Journal of Contemporary Criminal Justice*, Vol. 29(4) pp.475-497
- Higgins, G. E. and Makin, D. A. (2004)** *'Does Social Learning Theory Condition The Effects of Low Self-Control on College Students' Software Piracy'* *Journal of Economic Crime Management*, Vol. 2(2), pp.1-22
- Hille, P., Walsh, G. and Cleveland, M. (2015)** *'Consumer Fear of Online Identity Theft: Scale Development and Validation'* *Journal of Interactive Marketing*, Vol. 30 pp. 1-19
- Hindelang, M. J., Gottfredson, M. R. and Garofalo, J. (1978)** *'Victims of Personal Crime: An Empirical Foundation for a Theory of Personal Victimization'* Cambridge, MA: Ballinger
- Holt, T. J. and Bossler, A. M. (2013)** *'Examining the Relationship between Routine Activities and Malware Infection Indicators'* *Journal of Contemporary Criminal Justice*, Vol.29 pp.420–36
- Holt, T. J., Bossler, A. M. and May, D. C. (2012)** *'Low Self-Control, Deviant Peer Associations, And Juvenile Cyberdeviance'* *American Journal of Criminal Justice*, Vol. 37(3), pp. 378-395
- Holtfreter, K., Reisig, M. D. and Blomberg, T. G. (2006)** *'Consumer Fraud Victimization in Florida: An Empirical Study'* *St. Thomas Law Review*, Vol. 18, pp. 761-789
- Holtfreter, K., Reisig, M. D. and Pratt, T. C. (2008)** *'Low Self-Control, Routine Activities, and Fraud Victimization'* *Criminology*, Vol.46, pp. 189-220
- Holtfreter, K., Reisig, M. D., Pratt, T. C. and Holtfreter, R. E. (2015)** *'Risky Remote Purchasing and Identity Theft Victimization among Older Internet Users'* *Psychology, Crime and Law*, (ahead-of-print), 1-18

- Hong, J. (2012)** *'The State of Phishing Attacks'* Communications of the ACM Vol. 55(1) pp. 74-81
- Hosmer Jr, D. W., Lemeshow, S. and Sturdivant, R. X. (2013)** *'Applied Logistic Regression'* Vol. (398) John Wiley & Sons
- Howard, R. (2009)** *'Cyber Fraud: Tactics, Techniques and Procedure'* Boca Raton, FL: Auerbach Publications
- Hutchings, A. and Hayes, H. (2009)** *'Routine Activity Theory and Phishing Victimization: Who Got Caught in The 'Net'?''* Current Issues in Criminal Justice, Vol.20, pp.432-51
- IBM Cyber Security Intelligence Report (2015)** *'An Analysis of Cyber Attack and Incident Data From IBM's Worldwide Security Services Operations'* Accessed on 05/08/2015
Available at:
http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=SA&subtype=WH&htmlfid=SEW03073USEN&appname=GTS_E_GT_GT_CHDE_WH
- Indermaur, D. D. and Spiranovic, C. (2013)** *'Fear of Cyber-Identity Theft and Related Fraudulent Activity'* Psychology and Law Vol. 20 (3) pp.315-328
- Irwin, S. (2013)** *'Qualitative Secondary Data Analysis: Ethics, Epistemology and Context'* Progress in Development Studies, Vol. 13(4), pp. 295-306
- Jackson, J. (2006)** *'Introducing Fear of Crime to Risk Research'* Risk Analysis Vol. 26(1) pp. 253-264
- Jackson, J. and Gouseti, I. (2014)** *'Fear of Crime'* The Encyclopedia of Theoretical Criminology pp. 1-5
- Jagatic, T. N., Johnson, N. A., Jakobsson, M. and Menczer, F. (2007)** *'Social Phishing'* Communications of the ACM Vol. 50(10) pp. 94-100

- Jansson, K. (2007)** *'British Crime Survey: Measuring Crime over 25 Years'* London: Home Office
- Judge, P., Alperovitch, D. and Yang, W. (2005)** *'Understanding and Reversing the Profit Model of Spam (Position Paper)'* In *Fourth Workshop on the Economics of Information Security*
- Kanan, J. W., & Pruitt, M. V. (2002)** *'Modeling Fear of Crime and Perceived Victimization Risk: The (In) Significance of Neighborhood Integration'* *Sociological Inquiry* Vol. 72(4) pp. 527-548
- Keane, C. (1998)** *'Evaluating The Influence of Fear of Crime as An Environmental Mobility Restrictor on Women's Routine Activities'* *Environment and Behavior* Vol. 30(1) pp.60-74
- Kennedy, L. W. and Forde, D. R. (1990)** *'Routine Activities and Crime: An Analysis of Victimization in Canada'* *Criminology*, Vol. 28, pp. 137-152
- Kesteren, J.V., van Dijk, J., Mayhew, P. (2014)** *'The International Crime Victim Surveys: A Retrospective'* *International Review of Victimology* Vol. 20 (1), pp. 49-69
- Kosse, A. (2013)** *'Do Newspaper Articles on Card Fraud Affect Debit Card Usage?'* *Journal of Banking and Finance* Vol. 37(12) pp. 5382-5391
- Kowalski, M. (2002)** *'Cyber-Crime: Issues, Data Sources, and Feasibility of Collecting Police-Reported Statistics'* Accessed on: 18.07.2015 Available at: <http://www.statcan.gc.ca/pub/85-558-x/85-558-x2002001-eng.pdf>
- Kshetri, N. (2009)** *'Positive Externality, Increasing Returns and The Rise In Cybercrimes'* *Communications of the ACM* Vol. 52(12) pp.141- 44
- Kshetri, N. (2010)** *'The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives'* Heidelberg: Springer

- Kukar-Kinney, M. and Close, A. G. (2010)** *'The Determinants of Consumers' Online Shopping Cart Abandonment'* Journal of the Academy of Marketing Science, Vol. 38(2) pp. 240-250
- La Polla, M., Martinelli, F. and Sgandurra, D. (2013)** *'A Survey on Security for Mobile Devices'* Communications Surveys and Tutorials, IEEE, Vol. 15(1), pp. 446-471
- Lawrence, J. E. and Tar, U. A. (2010)** *'Barriers to E-commerce in Developing Countries'* Information, society and justice journal, Vol.3 (1), pp.23-35
- Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., Postel, J., Roberts, L.G., Wolff, S. (2009)** *'A Brief History of The Internet'* ACM SIGCOMM Computer Communication Review Vol. 39(5) pp. 22-31
- Liska A, Sanchirico A and Reed M (1988)** *'Fear of Crime and Constrained Behavior: Specifying and Estimating a Reciprocal Effects Model'* Social Forces Vol. 66(3) pp.827-837
- Lu, H. P. and Yu-Jen Su, P. (2009)** *'Factors Affecting Purchase Intention on Mobile Shopping Web Sites'* Internet Research, Vol. 19(4) pp. 442-458
- Malin, J. and Fowers, B. J. (2009)** *'Adolescent Self-Control And Music And Movie Piracy'* Computers in Human Behavior, Vol. 25(3), pp. 718-722
- Marcum, C.D. (2008)** *'Adolescent Online Victimization: A Test of Routine Activities Theory'* Doctoral Thesis, Indiana University of Pennsylvania.
- Marcum, C. D., Higgins, G. E. and Ricketts, M. L. (2010)** *'Potential Factors of Online Victimization of Youth: An Examination of Adolescent Online Behaviors Utilizing Routine Activity Theory'* Deviant Behavior, Vol.31 pp.381-410
- Marcum, C.D. (2011)** *'Adolescent Online Victimization and Constructs of Routine Activities Theory'* In Jaishankar K. (ed.) *'Cyber criminology: Exploring Internet Crimes and Behavior'* Boca Raton (FL): CRC Press Taylor & Francis Group
- Marlow, C. (2010)** *'Research Methods For Generalist Social Work'* Cengage Learning

- Markowitz, F. E., Bellair, P. E., Liska, A. E. and Liu, J. (2001)** *'Extending Social Disorganization Theory: Modeling The Relationships between Cohesion, Disorder, and Fear'* *Criminology*, Vol. 39, pp. 293-320
- Mason, K. A. and Benson, M. L. (1996)** *'The Effect of Social Support on Fraud Victims' Reporting Behavior: A Research Note'* *Justice Quarterly*, Vol. 13(3), pp. 511-524
- Matthews, B. and Ross, L. (2010)** *'Research Methods: A practical Guide for the Social Sciences'* Edinburgh: Pearson
- Maxfield, M. G. and Babbie, E. R. (2015)** *'Basics of Research Methods for Criminal Justice and Criminology'* (4th Ed.) Belmont, CA: Wadsworth
- Mayhew P. (1993)** *'Measuring The Effects of Crime in Victimization Surveys'* In Bilsky W., Pfeiffer C., Wetzels P. (Eds.) *'Fear Of Crime and Criminal Victimization'* Ferdinand Enke, Stuttgart
- McGuire, M. and Dowling, S. (2013a)** *'Cyber crime: A review of The evidence: Cyber-dependent Crimes'* Home Office Research Report 75 Accessed on: 27.07.2015 Available at: <http://www.justiceacademy.org/iShare/Library-UK/horr75-chap1.pdf>
- McNeeley, S. (2014)** *'Lifestyle-Routine Activities and Crime Events'* *Journal of Contemporary Criminal Justice*, pp. 1-23
- Meier, R. F. and Miethe, T. D. (1993)** *'Understanding Theories of Criminal Victimization'* *Crime and justice*, pp. 459-499
- Miethe, T. D. and McDowall, D. (1993)** *'Contextual Effects in Models of Criminal Victimization'* *Social Forces*, Vol. 71, pp. 741-759
- Miethe, T. D. and Meier, R. F. (1990)** *'Opportunity, Choice, and Criminal Victimization: A Test Of A Theoretical Model'* *Journal of Research in Crime and Delinquency* Vol. (27) pp. 243-266

- Miethe, T. D., Stafford, M. C. and Long, J. S. (1987)** *'Social Differentiation in Criminal Victimization: A Test Of Routine Activities/Lifestyle Theories'* American Sociological Review, pp. 184-194
- Miller C. (2002)** *'Weapon Carrying as a Behavioral Consequence of Fear of Crime'* International Journal of Police and Management Vol. 4(3) pp. 169–181
- Milne, G. R., Rohm, A. J. and Bahl, S. (2004)** *'Consumers' Protection of Online Privacy and Identity'* The Journal of Consumer Affairs Vol. 38(2) pp. 217-232
- Miyazaki, A. D. (2008)** *'Online Privacy and the Disclosure of Cookie Use: Effects on Consumer Trust and Anticipated Patronage'* Journal of Public Policy and Marketing, Vol. 27 (1) pp. 19-33
- Montague, D. A. (2010)** *'Essentials of Online Payment Security and Fraud Prevention'* New Jersey: John Wiley & Sons.
- Moore, D. (2015)** *'Holiday Scams to Avoid this Summer'* Accessed on: 21.07.2015 Available at: <http://www.moneywise.co.uk/scams-rip-offs/scams/holiday-scams-to-avoid-summer>
- Mowery, D. C. and Simcoe, T. (2002)** *'Is The Internet A US Invention? An Economic and Technological History of Computer Networking'* Research Policy, Vol. 31(8) pp. 1369-1387
- Mustaine, E. E. and Tewksbury, R. (1998)** *'Predicting Risks of Larceny Theft Victimization: A Routine Activity Analysis Using Refined Lifestyle Measures'* Criminology, Vol. 36(4), pp. 829-858
- Narcisse, E. (2015)** *'Scammer Is Selling Fake Games On The Windows Store'* Accessed on: 22.07.2015 Available at: <http://kotaku.com/darkest-dungeon-being-sold-on-windows-app-store-is-fake-1687484296>

- National Fraud Authority (2013)** '*Annual Fraud Indicator*' Accessed on: 12.07.2015
Available at:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/206552/nfa-annual-fraud-indicator-2013.pdf
- Newman, G. R. and Clarke, R. V. (2013)** '*Superhighway Robbery*' London: Routledge
- Ngo, F. T. and Paternoster, R. (2011)** '*Cybercrime Victimization: An Examination of Individual and Situational-Level Factors*' International Journal of Cyber Criminology, Vol. 5 pp.773-793
- Office for National Statistics Statistical Bulletin (2014)** '*E-commerce and ICT Activity-2013*' Accessed on: 15.07.2015 Available at:
http://www.ons.gov.uk/ons/dcp171778_387514.pdf
- Office for National Statistics Report (2014)** '*Monitoring E-Commerce, 2014*' Accessed on: 12/09/2015 Available at: http://www.ons.gov.uk/ons/dcp171766_373496.pdf
- Office for National Statistics (2015)** '*Crime Survey for England and Wales*' Accessed on: 01/07/2015 Available at: <http://www.crimesurvey.co.uk>
- ONS Information Paper (2015)** '*Quality and Methodology Information*' Accessed on: 17/08/2015 Available at: <http://www.ons.gov.uk/ons/guide-method/method-quality/quality/quality-information/crime-and-justice/index.html>
- ONS Bulletin (2014)** '*Crime in England and Wales, Year Ending December 2013*' Accessed on: 01.06.2015 Available at: http://www.ons.gov.uk/ons/dcp171778_360216.pdf
- Pathak, N., Pawar, A. and Patil, B. (2015)** '*A Survey on Keylogger: A malicious Attack*' International Journal of Advanced Research in Computer Engineering and Technology (IJARCET) Vol. 4 (4) pp. 1465-1469
- Pease, K. (2001)** "*Crime Future and Foresight*" In Wall D. S. (2001) (Ed.) '*Crime and the Internet*' London: Routledge

- Phifer, L. (2009)** *'The Security Risks of Free Public WiFi'* Accessed on: 10/09/2015
Available at: <http://searchsecurity.techtarget.com.au/news/2240020802/The-security-risks-of-Free-Public-WiFi>
- Policastro, C. and Payne, B. K. (2014)** *'Can You Hear Me Now? Telemarketing Fraud Victimization and Lifestyles'* American Journal of Criminal Justice, pp. 1-19
- Pratt, T. C., Holtfreter and K., Reisig, M. D. (2010)** *'Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory'* Journal of Research in Crime and Delinquency, Vol.47 pp.267-96
- Ragin, C. C. (1999)** *'Using Qualitative Comparative Analysis to Study Causal Complexity'* Health Services Research Vol.34 (5, part 2) pp.1225–39
- Reed, K. (2005)** *'When Elders Lose Their Cents: Financial Abuse of The Elderly'* Clinics in Geriatric medicine, Vol. 21(2), pp. 365-382
- Rege, A. (2009)** *'What's Love Got To Do With It? Exploring Online Dating Scams And Identity Fraud'* International Journal of Cyber Criminology Vol. 3(2) pp. 494-512
- Reisig, M. D. and Holtfreter, K. (2007)** *'Fraud Victimization and Confidence in Florida's Legal Authorities'* Journal of Financial Crime, Vol. 14(2), pp. 113-126
- Reisig, M. D., Pratt, T. C. and Holtfreter, K. (2009)** *'Perceived Risk of the Internet Theft Victimization: Examining The Effects of Social Vulnerability and Impulsivity'* Criminal Justice and Behavior, Vol. 36 pp. 369-384
- Rengifo, A. F. and Bolton, A. (2012)** *'Routine Activities and Fear of Crime: Specifying Individual-Level Mechanisms'* European Journal of Criminology Vol. 9(2) pp.99-119
- Rew, L., Koniak-Griffin, D., Lewis, M. A., Miles, M. and O'Sullivan, A. (2000)** *'Secondary Data Analysis: New Perspective for Adolescent Research'* Nursing Outlook, Vol. 48(5), pp. 223-229
- Reyns B.W., Henson B. and Fisher B.S. (2011)** *'Being Pursued Online: Applying Cyberlifestyle-Routine Activities Theory to Cyberstalking Victimization'* Criminal Justice and Behavior Vol.38 (11) pp. 1149-1169

- Reyns, B. W. (2013)** *'Online Routines and Identity Theft Victimization Further Expanding Routine Activity Theory beyond Direct-Contact Offenses'* Journal of Research in Crime and Delinquency, Vol.50 (2), pp. 216-238
- Rho, J. J. (2007)** *'Blackbeards of The Twenty-First Century: Holding Cybercriminals Liable Under The Alien Tort Statute'* Chicago Journal of International Law, Vol. 7(2), pp. 695-719
- Roberts, L. D., Indermaur, D. and Spiranovic, C. (2013)** *'Fear of Cyber-Identity Theft and Related Fraudulent Activity'* Psychiatry, Psychology and Law Vol. 20(3) pp. 315-328
- Rountree, P. W. and Land, K. C. (1996)** *'Perceived Risk Versus Fear of Crime: Empirical Evidence of Conceptually Distinct Reactions in Survey Data'* Social Forces, Vol. 74(4), pp. 1353-1376
- Routers (2011)** *'Sony Playstation Suffers Massive Data Breach'* Accessed on: 20.07.2015 Available at: <http://uk.reuters.com/article/2011/04/27/us-sony-stoldendata-idUSTRE73P6WB20110427>
- Rust, R. T., Kannan, P. K. and Peng, N. (2002)** *'The Customer Economics Of Internet Privacy'* Journal of the Academy of Marketing Science, Vol. 30(4), p. 455-464
- Saban, K. A., McGivern, E. and Saykiewicz, J. N. (2002)** *'A Critical Look at The Impact of Cybercrime on Consumer the Internet Behavior'* Journal of Marketing Theory and Practice, pp. 29-37
- Sampson, R. J. and Wooldredge, J. D. (1987)** *'Linking The Micro-And Macro-Level Dimensions of Lifestyle-Routine Activity and Opportunity Models of Predatory Victimization'* Journal of Quantitative Criminology, Vol. 3(4), pp. 371-393
- Sapsford, R. and Jupp, V. (2006)** *'Data Collection and Analysis'* London: Sage
- Schell, B. H. and Martin, C. (2004)** *'Cybercrime: A reference handbook'* Santa Barbara, California: ABC-CLIO

- Schneider, C. Q. and Wagemann, C. (2010)** *'Standards of Good Practice in Qualitative Comparative Analysis (QCA) And Fuzzy-Sets'* *Comparative Sociology*, Vol. 9(3) pp. 397-418
- Schoepfer, A. and Piquero, N. L. (2009)** *'Studying The Correlates of Fraud Victimization and Reporting'* *Journal of Criminal Justice* Vol. 37(2) pp. 209-15
- Schreck, C. J. (1999)** *'Criminal Victimization and Low Self-Control: An Extension and Test of a General Theory of Crime'* *Justice Quarterly*, Vol. 16, pp. 633-654
- Schreck, C. J. and Fisher, B. S. (2004)** *'Specifying The Influence of Family and Peers on Violent Victimization: Extending Routine Activities And Lifestyles Theories'* *Journal of Interpersonal Violence* Vol. (19) pp.1021-1041
- Shabir, G., Hamad, N. and Anosh, M. (2014)** *'A True Picture of Electronic Business on Agriculture Sector of Southern Punjab, Pakistan'* *International Journal of Innovative Research and Development*, Vol. 3(5)
- Shipley, T. G. and Bowker, A. (2013)** *'Investigating Internet Crimes: An Introduction to Solving Crimes in Cyberspace'* Elsevier, New York, NY
- Siegel, L. J. (2011)** *'Criminology'* Eleventh Edition Wadsworth: Cengage Learning
- Singh, K. (2007)** *'Quantitative Social Research Methods'* London: Sage
- Skogan, W. G. and Maxfield, M. G. (1981)** *'Coping with Crime'* Beverly Hills, CA: Sage
- Skogan, W.G. (1986a)** *'The Fear of Crime and Its Behavioral Implications'* In *'From Crime Policy to Victim Policy'* (A.E. Fattah, ed.) London: Macmillan
- Smith, E. (2008)** *'Pitfalls and Promises: The Use of Secondary Data Analysis in Educational Research'* *British Journal of Educational Studies*, Vol. (56) 3, pp. 323-339
- Smith, R. G. (2000)** *'Confronting Fraud In The Digital Age'* Unpublished Occasional Paper of the Australian Institute of Criminology

Smith, R. G. (2010) *'Identity Theft and Fraud'* pp. 273-301 In Jewkes, Y. and Yar, M. (eds.) *'Handbook of Internet Crime'* Devon: Willian Publishing

Smith, M. and Bouffard, L. A. (2014) *'Victim Precipitation'* The Encyclopedia of Criminology and Criminal Justice

Spector, P. E and Brannick, M. T. (2011) *'Methodological Urban Legends: The misuse of statistical control variables'* Organizational Research Methods Vol. 14(2) pp. 287-305

Sproule, S. and Archer, N. (2007) *'Defining Identity Theft'* Accessed on: 22.07.2105 Available at: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4285319>

Sreetheran, M. and van den Bosh, C. K. (2015) *'Fear of Crime in Urban Parks–What the Residents of Kuala Lumpur Have to Say?'* Urban Forestry and Urban Greening, Vol. 14(3), pp. 702-713

Swinyard, W. R. and Smith, S. (2003) *'Why People (Don't) Shop Online: A Lifestyle Study of the Internet Consumer'* Psychology and Marketing Vol. 20 pp. 567-97

Symantec (2014) *'Internet Security Threat Report'* Accessed on: 08/05/2015 Available at: http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Symantec_annual_internet_threat_report_ITU2014.pdf

Symantec (2015) *'Internet Security Threat Report'* Accessed on: 08/05/2015 Available at: https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf

Tajpour, A., Ibrahim, S. and Zamani, M. (2013) *'Identity Theft Methods and Fraud Types'* International Journal of Information Processing and Management Vol. 4(7) pp. 51-58

Technical Report (2014) *'Crime Survey England and Wales'* Accessed on: 01/07/2015 Available at: <http://www.ons.gov.uk/ons/guide-method/method-quality/specific/crime-statistics-methodology/2013-14-crime-survey-for-england-and-wales-technical-report--volume-1.pdf>.

The Bureau of Justice Statistics (BJS) Bulletin (2013) '*Victims of Identity Theft, 2012*'
 Accessed on 19.07.2015 Available at:
<http://www.bjs.gov/index.cfm?ty=pbdetail&iid=4821>

The Guardian (2014) '*JP Morgan Chase Reveals Massive Data Breach Affecting 76m Households*'
 Accessed on: 19.07.2015 Available at:
<http://www.theguardian.com/business/2014/oct/02/jp-morgan-76m-households-affected-data-breach>

The UK Cards Association Report (2014) '*Annual Report: Plastic Fraud Figures*'
 Accessed on: 01/08/2015 Available at:
http://www.theukcardsassociation.org.uk/plastic_fraud_figures/index.asp

Thomas, C., Thiry, J., Hsu, K., Traver, K. and Tengkiattrakul, P. (2014) '*Analysis of Online Credit Card Black Markets*' pp.1-9 Accessed on:08/08/2015 Available at:
<http://pathorn.net/article/CREDITCARD-2014.pdf>

Thomas, D. and Loader, B. (2000a) '*Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*' (Introduction), in D.Thomas and B Loader (eds), '*Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*' London: Routledge

Tillyer, M. S. and Eck, J. E. (2009) '*Routine Activities*' pp. 279-87 In J. M. Miller (Ed.), '*21st Century Criminology: A Reference Handbook*' Thousand Oaks, CA: Sage

Titus, R. M. and Gover, A. R. (2001) '*Personal Fraud: The Victims and The Scams*' Crime Prevention Studies, Vol. 12, pp. 133-152

Titus, R. M., Heinzelmann, F. and Boyle, J. M. (1995) '*Victimization of Persons By Fraud*' Crime and Delinquency, Vol. 41(1), pp. 54-72

Tive, C. (2006) '*419 Scam: Exploits of The Nigerian Con Man*' Laos, Nigeria: Chicha Favours, iUniverse

- Tropina, T. (2014)** *'Fighting Money Laundering in the Age of Online Banking, Virtual Currencies and Internet Gambling'* ERA Forum Vol. 15 (1) pp. 69-84 Springer Berlin Heidelberg
- Turban, E., David, K., Lee, J.K., Liang, T. and Turban, D. (2015)** *'Electronic Commerce: A Managerial and Social Networks Perspective'* (8th ed) London: Springer
- Valentine, L. (2013)** *'Why US Bank moved early on EMV'* American Bankers Association ABA Banking Journal, Vol. 105(4) pp. 20-23
- van Wilsem, J. (2011)** *'Bought it, but Never Got it': Assessing Risk Factors for Online Consumer Fraud Victimization'* European Sociological Review, Jcr053, pp.1-11
- van Wilsem, J. (2013)** *'Hacking and Harassment—Do They Have Something in Common? Comparing Risk Factors for Online Victimization'* Journal of Contemporary Criminal Justice, Vol. 29(4), pp. 437-453
- van Wyk, J. and Benson, M. L. (1997)** *'Fraud Victimization: Risky Business or Just Bad Luck?'* American Journal of Criminal Justice, Vol. 21(2), pp. 163-179
- van Wyk, J. and Mason, K. (2001)** *'Investigating Vulnerability and Reporting Behavior for Consumer Fraud Victimization'* Journal of Contemporary Criminal Justice, Vol. 17, pp. 328–345
- Verma, J. P. (2012)** *'Data Analysis in Management with SPSS Software'* Springer Science and Business Media
- Vis, B. (2012)** *'The Comparative Advantages of FSQCA And Regression Analysis for Moderately Large-N Analyses'* Sociological Methods and Research 41(1) pp.168-198
- Wall, D. S. (2007)** *'Cybercrime: The Transformation of Crime in the Information Age'* Cambridge, UK: Polity Press
- Wall, D.S. (2008/11)** *'Cybercrime and The Culture of Fear: Social Science Fiction(S) and The Production of Knowledge about Cybercrime'* (revised Feb. 2011) Information, Communication and Society Vol. (11) pp.861–84

- Wall, D. S. (2008b)** *'Cybercrime, Media and Insecurity: The Shaping of Public Perceptions of Cybercrime'* International Review of Law, Computers and Technology, Vol. (22) pp. 45-63.
- Wall, D. S. (2010)** *'Micro-Frauds: Virtual Robberies, Stings and Scams in the Information Age'* pp. 68-85 In Holt, T. and Schell, B. (Eds.) *'Corporate Hacking And Technology-Driven Crime: Social Dynamics and Implications'* New York: IGI Global
- Wall, D. S. (2013)** *'Policing Identity Crimes'* Policing and Society: An International Journal of Research and Policy, 23 (4): 437-460
- Warr, M. (1984)** *'Fear of Victimization: Why Are Women and the Elderly More Afraid?'* Social Science Quarterly, Vol. 65, pp.681-702
- Warr, M. (2000)** *'Fear of Crime in The United States: Avenues for Research and Policy'* In Duffee, D. (Ed.), *'Measurement and Analysis of Crime and Justice'* Vol. 4, pp. 452-489 Washington, DC: National Institute of Justice
- Whitman, M. and Mattord, H. (2011)** *'Principles of Information Security'* Cengage Learning Course Technology, Massachusetts
- Wolfgang, M. (1957)** *"Victim-precipitated Criminal Homicide"* Journal of Criminal Law, and Police Science Vol. 48 pp. 1-11
- Wolfgang, M. (1958)** *'Patterns of Criminal Homicide'* Philadelphia: University of Pennsylvania Press
- Wordpay Report (2015)** *'Alternative Payments report, 2nd Edition'* Accessed on: 13/09/2015 Available at: <http://www.worldpay.com/global/alternative-payments-2nd-edition>
- Xu, H. and Gupta, S. (2009)** *'The Effects of Privacy Concerns and Personal Innovativeness on Potential and Experienced Customers'* adoption of location-based services' Electronic Markets, Vol. 19(2-3) pp.137-149
- Yar, M. (2005)** *'The Novelty of 'Cybercrime': An Assessment In Light of Routine Activity Theory'* European Journal of Criminology, Vol. 2, pp. 407-27

Yar, M. (2006) *'Cybercrime and Society'* London: SAGE Publications

Yin P (1980) *'Fear of Crime among the Elderly: Some Issues and Suggestions'* Social Problems Vol. 27(4) pp. 492–504

Zvekic, U., Del Frate, A. A. (1996) *'The International Crime (Victim) Survey in the Developing World'* pp. 3-15 In Zvekic, U., Del Frate, A. A. (Eds.) *'Criminal Victimization in the Developing World'* DIANE Publishing

Zwick, D. and Dholakia, N. (2004) *'Whose Identity Is it Anyway? Consumer Representation in the Age of Database Marketing'* Journal of Macromarketing, Vol. 24 (1), pp. 31–43