Hi,

Thanks for the reminder - and please accept my apologies for the delayed reply.

I have the following comments on Chapter 2.

Please proof-read carefully - there are a few typos/grammatical issues.

You need to extend your Contents page to cover Chapter 2.

Please check how to cite references when you use the author's name as part of the sentence. The date should still be placed inside parentheses/brackets.

Try to ensure that you focus on a critical discussion about the previous research - rather than a detailed discussion about the methods used.  A brief description would be ok here - a more detailed discussion could be used in your Research Methods chapter to help to justify your approach.

The chapter would benefit from being broken down into sub-sections - perhaps around the different issues that you have discussed.

Ideally, the chapter should finish with a brief summary of what you have learnt and how this has influenced your research.

I hope that this helps.

Best wishes

Steve

***Chapter 2***

***2.0 Literature Review***

The issue of online credit card is nothing new to e-commerce merchants, since the development and use of online platforms as a market place to sell goods and services fraudsters have been using illicit means in order to get goods and services without any monetary cost to themselves. Carding is one such activity, over the past 5 years have seen drastic increases in carding incidents, caused by an exponential improvement in carding techniques all this results in an ever increasing cost to e-commerce merchants and other market places. Because of the ever changing nature and improvements within the carding domain. According to the Nilson report (2016) credit card fraud will surpass $31 billion USD worldwide by the year 2020. The Lexis annual report (2016) provides more evidence to the true cost of online credit card fraud, according to this report “US merchants reported an 8% increase over last year in the cost per dollar of fraud losses, from $2.23 to $2.40, these charges are based on merchandise replacement cost and chargeback cost”. The report further provide evidence that in 2015 online merchants saw an average monthly attempt of fraud of approximately 33%, with approximately 46% of these bypassing current fraud prevention mechanism. Survey conducted by LexisNexis (2015) revealed that cases of e-commerce fraud is increasing despite the fact that merchants are investing more in security. Based on the evidence provided by these reports, it is evident that e-commerce fraud is very lucrative and carding is the main fuel behind this epidemic coupled with the remoteness of the crime and the likelihood of not getting caught. This provides enough evidence that a lot needs to be done in order to tackle the problem of e-commerce fraud, and this research aims to establish the techniques and procedures carders are using and how they do it in order to perpetuate their crime.

Carders use underground forums in order to trade, learn, teach and communicate about their carding activities, as these forums provide some amount of shadow to their identities and provide a somewhat safe haven for carders. According to research conducted by Haslebacher, Onaolapo and Stringhinin (2015) underground online forums provide a trading platform for illicit goods and services. The research focused on underground carding forums, how are they structured and operated, this provides a starting point for this current research. Underground forums will be used in order to gather first hand data needed, directly form individuals who are involved in carding. The method adopted by Haslebacher, Onaolapo and Stringhini, 2015 was to search the web for underground forums and also forums that were referenced in previous works that they reviewed. 5 forums were chosen those that were identified, were identified on the basis of size, founding date and to a lesser extent the quality of the contents of these forums. The researchers then joined these 5 online forums, and over a period of 3 months’ data was gathered and analyzed based on the aims and objectives of the research which in their case was the type of products sold, the prices, seller proficiency, seller specialization and the seller’s reputations and how does this coincides and relates with a fully functional carding forum. A similar approach will be adopted as this approach proved to be effective in the type of research conducted by Haslebacher, Onaolapo and Stringhini (2015). For the nature of this current research data needed to efficiently draw a conclusion on the aims and objectives are not readily available and to get the necessary data, the researcher will have to join similar forums but with a different view on what type of data is needed from these forums. The findings of the research conducted by Haslebacher, Onaolapo and Stringhini (2015) were presented in tables and graphs and resulted in a research that was both qualitative and quantitative in nature. The qualitative and quantitative nature of these type of research, span across the entire board as it relates to researches and other similar works of this nature.

Bulkah and Gupta (2015) presented their research on characterizing credit card black markets on the web in the same manner, being qualitative and quantitative in nature. Tables and graphs were used to present their finding, and further discussion was used to develop on their objectives. In the case of Bulkah and Gupta (2015) their research was aimed at studying online carding markets, that sell stolen debit and credit cards only, and factors that influence the type of cards sold and their prices. The methodological approach was similar to that of Haslebacher, Onaolapo and Stringhini (2015) the researchers joined 3 online carding shops and gathered data that was publicly available in these online shops. The data was collected over a period of 4-6 months, in the case of Bulkah and Gupta (2015) the carding shops that were observed were rescator.cm, dumps.pw, and 2pac.cc, but a month into gathering data, 2pac.cc came offline due to the arrest of the owner, the researchers then switched to dumps.pw as their alternative. Currently of the three carding shops observed, only rescator.cm is still currently live. This is some evidence of the ever changing and evolving nature of carding and why more research is still needed in this area of cyber crime. “As law enforcement shuts down the servers hosting online marketplaces and arrest the criminals responsible for the security breaches, thieves find new ways to thrive, often by switching hosting providers in the blink of an eye” Bulkah and Gupta, 2015. Bulkah and Gupta (2015) provided evidence in their data analysis on the volumes of cards that are being sold on a daily basis from these card shops, according to the researchers Bulkah and Gupta, 2015 between October 2014 and February 2015 rescator.cm sold 56, 976 credit and debit cards and dumps.pw sold 55,784 cards. These staggering numbers provide further evidence of the volumes of cards being traded which in theory, can be said to be directly proportional to carding attempts. Bulkah and Gupta, 2015 did in their research focus on the type of cards that are sold in these market places and the factors that influence the prices of these cards. One of the aim of this current research is to identify the type of cards that are most sought after and utilized by carders and establish if there is relationship about the different types of cards used with successful carding. Based on their findings, Credit cards are sold more than debit cards and fetch a higher price and Visa and Master cards are sold more than other card types such as American Express and Discover an also fetch higher selling price. Bulkah and Gupta (2015) did not develop a relation ship about the type of cards used and carding, this is where this research will develop on their findings to establish that carder, card relationship.

Both researches conducted by Bulkah and Gupta (2015) and Haslebacher, Onaolapo and Stringhini, 2015 can be defined as case studies, according to Oates (2006) a case study is a piece of research that focuses on one instance of a “thing” that is to be investigated, where this one instance of a thing is studied in depth using different data gathering methods, in its natural setting and being holistic in nature. In the case of Bulkah and Gupta (2015) that instance of a thing was focusing on carding shops, and for Haslebacher, Onaolapo and Stringhini (2015) that instance of a thing was focusing on carding forums. Both researches can be seen as being descriptive in nature and as such a descriptive case study. The descriptive nature is where a detailed analysis is studied of a particular phenomenon and its context. Oates (2006).

A similar approach will be utilized on this current research, a case study approach will be used but in this case the research will be an explanatory case study, as this research aims to also explain a particular phenomenon, and find linking factors of what was found in the case to theories from literatures to see if there are any relations.

A study done by cyber security company Digital Shadows SearchLight (2017) focused on an online carding course that was prepared and delivered by Russian carders, Digital Shadows focused on this tutorial in order to show the sophisticated nature and lengths to which carders are willing to go in order to accomplish their goals of successfully carding onine e-commerce websites. According to Digital Shadows (2017) consumer spending online has increased over the years and this has provided a very attractive platform for cyber criminal to exploit. “The combination of increased spending and criminal innovation contributes to a projected loss of $24 billion to credit card fraud in 2018” Digital Shadows (2017). According toe Digital Shadows online credit card fraud is an organized crime and no one single entity is usually involved, with evidence from the carding tutorial that was studied by the research group, they system that has evolved includes; the payment card data harvesters, distributors, payment card fraudsters and monetization. It is the purpose of this research to focus on the “payment card fraudsters” or carders as they are commonly called, the work conducted by Digital Shadow stated that the methods by which carders perfect their skills was by using tutorials that have been handed down and or bought on the dark web and carding forums that have been refined and updated over time in order to circumvent, security methods of that time. If this is the case, then focusing this research on online forum is the right place to start in order to gather the necessary data that is needed to satisfy the objectives of this research. The data that was used by Digital Shadows, is secondary data and this may have prevented the researchers from providing a complete and up to date analysis of carding, as whatever techniques they may have came across at the time of the study, may have been outdated by the time they were actually conducting the study, however the paper did provide a direction in which other researchers may venture as a guide to build up on the work of Digital Shadows.

Another objective of this current research is to collect existing data and observe security solutions implemented by e-commerce platforms that are mostly targeted, Payment processing company, 2014 provided some solutions e-commerce companies can use to prevent online credit card fraud and identity take over. According to the paper there a not much customers can do in order to prevent fraudulent credit card use as there is as shift from traditional physical credit card theft to more sophisticated procedures where databases are being breached and customer’s information are being stolen and sold by the thousands. In this case merchants and financial institutions will now have to put measures in place in order to fight this problem. The information provided in this paper, written in 2014 seems to provide information that is somewhat dated for todays scenario as the solutions used back then to try and fight the problem of carding and credit card fraud, may not be as efficient in todays time. This paper did no go in depth to state the exact solutions that are being deployed and if they are working or not, nor did it state how the solutions that were recommended would benefit financial institutions and e-commerce businesses. The data used was from third party sources and the data analysis from the original source may have been different from what 2checkout may have done, if given the opportunity to capture the raw data and analyzed it themselves. Gathering raw unprocessed data directly from the source would give better results in establishing if current security solutions are not efficient and if so where the problem lies and the types of solutions needed to fix this problem.

One major way of fighting this cyber crime problem is by finding trends within e-commerce fraud, and this is one of the ways this current research aims to establish the overall goal of this research. Similar work has been conducted by technology company Radial and research group ENK (2017) to find trends in e-commerce and digital fraud. One major trend highlighted is that online fraud is more prevalent during holiday seasons, “fraud attempts are the highest during Christmas eve (2.4%), Thanksgiving (2%), Black Friday (1.8%) and holiday shipment cutoff days (1.6%) ENK and Radial (2017). Sales that are via 3rd party websites are more susceptible to fraud, example; Amazon and Ebay followed by mobile sales. This trend will be very interesting to develop and expound on in this current research, as this research will seek to establish if a relationship exists between carding and holiday seasons, if this is a specific technique utilized by carders then this research will seek to uncover the reasons as such. ENK and radial (2017) went even further to categorize the top merchants that are targeted, being Airlines, money transfer services, computer and electronics, general retail and clothing in that specific order, no reason was given as to why these areas were targeted this current research will go further and will seek to develop the reason as to why these industries and areas are targeted vs other areas. As seen with the past 2 studies that were analyzed, secondary data was used in order to establish the research, there is no evidence within the scope of the research by ENK and radial that data was gathered from the source of the problem, being carders. This seems to be the current trend based on most of the works already analyzed, not much data has been gathered from sources being; carders, online forums and carding shops instead a lot of the data being used is preexisting data, and based on the solutions that are established are being targeted towards the symptom or the problem and not the source.

Cyber security company The Threat Matrix presented a white paper in 2013, to highlight some of the most current trends in cyber security, based on the threats presented by The Threat Matrix, 2013 3 particular threats can be directly associated with carding; namely “E-commerce is the new low hanging fruit for online fraud”, “Account take over and identity theft are on the rise” and “mobile is the new desktop”. Based on previous literatures reviewed, it can be established that there is a relationship between these specific trends and carding. Based on the nature of the research now being conducted these trends should become more evident during the course and a specific relationship as to why these particular trends exist developed. The approach taken by The Threat Matrix in preparing their findings, was one of a case study approach, with the data gathered to support their work being gathered from secondary sources, again this presents a gap in the information, as more information from direct players in the cybercrime world may have shed more light on these trends and why these trends exist, also the data used by The Threat Matrix maybe have been outdated by the time the white paper was ready to be published. Taking a direct approach similar to Haslebacher, Onaolapo and Stringhini, 2015 can yield more useful data and in so present a research or paper that is more informative on this topic at the time of presentation.

Getting access to stolen credit and debit card, is a major raw material that is needed for carding, and without this piece of delicate information carders would not be in a position to perpetuate their crime. Peretti, 2009 conducted a research into data breaches and how this activity fuels the underground economy of carding. According to this exploratory case study conducted by Peretti, large scale data breaches present the raw fuel for carding, stolen cards are then placed on forums and other carding stores for sale. Similar to the works of Haslebacher, Onaolapo and Stringhini (2015) and Bulkah and Gupta (2015) carding forums present the medium through which carders communicate and trade their goods, services and skills. Peretti, 2009 went further to characterize and break down the structure of these carding forums; into administrators, moderators, reviewers, vendors and the general members based on this structural break down, the focus of this current research will be on the general member, as these members are the ones buying the stolen cards, passing information, skills and tutorials about carding. Further, in order to gather the necessary first hand raw data that will be needed for this research, the researcher will have to engage as a general member within these forums. All the forums and card stores mention by Peretti at this time of this review, were no longer online, hence some of the findings may have been currently out dated, and new research is needed based on the current state of online card fraud. Peretti, 2009 classified the carding data in these forums into 2 classes, CVV (credit and debit card numbers along with matching address) and Dumps (dumps being the information that is swiped from the magnetic strips of physical cards). This current research will focus on CVVs as these are the card information being purchased online for online carding. Peretti, 2009 provides a solid starting point for future research into carding, on the surface procedures and steps that carders take are highlighted in Peretti’s research but because of advances and updates in carding many of these steps and procedures may have been obsolete and new procedures found. Peretti provides evidence of prosecution of carders within the body of work reviewed but based on the findings it can be interpreted that only major players, such as forum administrators and card shop administrators are usually arrested and prosecuted, and in many cases these administrators aren’t the culprits or carding they only facilitate the medium for carders to communicate, based on these findings this is evidence that carders more often than not get away with this cyber crime and this is another reason why more research is needed in this area, based on this alone carding is not going anywhere soon and the prospect for this cyber crime will continue to increase and continue to attract new players with more and more innovative ideas to this area of cyber crime.