Dissertation:
The Security of The ATM Machines in Relation to Students

A Dissertation submitted in partial fulfillment of the requirements for the degree of Bachelor of Science (Honors) in Business Information Systems.

Department of Computing & Information Systems
Cardiff School of Management

Student Name: Shaikha Al-Thani

Student Number: ST20110980

Date: Sunday, April 24, 2017
Declaration

I hereby declare that this dissertation entitled *The Security of ATM Machines in Relation to Students* is entirely my own work, and it has never been submitted nor is it currently being submitted for any other degree.

Candidate: <Shaikha Al-Thani>

Signature: Shaikha Al-Thani

Date: April 24, 2017

Supervisor: <Jason Williams>

Signature:

Date: April 24, 2017
Table of Contents

Abstract ................................................................................................................................. 5

Chapter 01: Introduction ...................................................................................................... 6
  1.1 The Introduction ........................................................................................................... 6
  1.2 The Background ......................................................................................................... 6
  1.3 The Problem Statement ............................................................................................. 7
  1.4 The Significance of the Research ............................................................................... 7
  1.5 The Research Aim ....................................................................................................... 7
  1.6 The Research Objectives ............................................................................................ 7
  1.7 The Research Questions ............................................................................................. 8
  1.8 The Rationale of the Research ................................................................................... 8
  1.9 The Limitations of the Study ...................................................................................... 8
  1.10 The Structure of the Dissertation ............................................................................. 9
  1.11 Conclusion ................................................................................................................ 9

Chapter 02: The Literature Review ..................................................................................... 10
  2.1 Introduction ................................................................................................................ 10
  2.2 The Basic Understanding of ATM skimming ............................................................. 10
  2.3 The Mechanism of ATM Skimming .......................................................................... 11
  2.4 The Global Rise in ATM Skimming Incidents ............................................................ 16
  2.5 Why Skimming and Other Frauds are Serious Issues ............................................. 18
  2.6 Types of Frauds that can occur at ATM Machines .................................................. 19

Chapter 3 – Methodology .................................................................................................. 20
  3.1 The Introduction ....................................................................................................... 20
  3.2 The Research Philosophy .......................................................................................... 21
  3.3 The Research Purpose ............................................................................................... 21
  3.4 The Research Strategy ............................................................................................... 21
  3.5 The Research Approach ............................................................................................. 22
  3.6 The Data Collection Method .................................................................................... 22
  3.7 The Sampling Technique ......................................................................................... 23
  3.8 The Data Analysis ..................................................................................................... 23
  3.9 The Reliability .......................................................................................................... 23
  3.10 The Validity ............................................................................................................. 24
  3.11 The Generalizability ................................................................................................. 24
  3.12 The Ethical Issues .................................................................................................... 24
  3.13 The Conclusion ....................................................................................................... 25
Chapter 4 The Results ............................................................................................................................................. 25
  4.1 The Result from the Student Surveys ............................................................................................................. 25
  4.2 Results from the Semi-Structured Interview of the Bank Security Officer .................................................. 38
  4.3 Results from the Semi-Structured Interview of the victim of the ATM Fraud ............................................... 40

Chapter 5 The Findings and their Implications .................................................................................................... 41
The Findings and their Implications .......................................................................................................................... 41

Chapter 6: Conclusions and Recommendations .................................................................................................. 43
  6.1 Conclusions ..................................................................................................................................................... 43
  6.2 The Recommendations ................................................................................................................................. 45
  6.3 Limitations of the Study ............................................................................................................................... 51
  6.4 Suggestions for Future Study ........................................................................................................................ 51

References: .............................................................................................................................................................. 53

Appendices: ............................................................................................................................................................... 55
  Appendix 1: Questionnaire for the Students ........................................................................................................ 55
  Appendix 2: Semi-Structured Interview of the Victim ....................................................................................... 57
  Appendix 3: Semi-Structured Interview of the Bank Security Officer: .............................................................. 58
Abstract

Banking services and related technologies have seen a continuous evolution or rise to better customer convenience and financial needs. In this regard, the introduction of the ATM based monetary or budgetary transaction has been a radical shift. However, the recent rise in the ATM skimming incidents, card data theft issues, online data tampering, and other forms of physical intrusions into customer safety have raised the necessity to adopt a preventive approach to combating or stopping such issues. This research is a step towards understanding the current awareness levels amongst customers on the safety precautions and guidelines. For the sake of primary study, a student population has been selected based on purposeful sampling. The research has been done or completed by adopting primary research techniques and making use of a questionnaire and semi-structured interviews to meet the research objectives. Moreover, interpretivism is a research philosophy that has been selected or chosen for this research paper. Interpretivism studies focus on meaning and it may select multiple methods in order to reflect different aspects of the issue. This philosophy has been adopted to understand participant awareness on skimming frauds, and it analyzes bank’s measures to put a stop to the fraud issues. A thematic analysis of the findings would be conducted to arrive at important conclusions. Some necessary recommendations would be made to customers and banks on how to adopt a proactive approach to manage such frauds and detect their presence in the first place. The recommendations can play an important role in increasing customer awareness and restraining the fraud issues.
Chapter 01: Introduction

1.1 The Introduction

ATMs or Automated Teller machines are something that everybody is aware of these days. ATMs are useful equipment that we all use to get cash from banks. They save us from waiting in long queues in banks for withdrawing cash from our bank accounts. However, the lack of awareness of users regarding the ATM security has been causing trouble and issues to the ATM users (Sidel, 2015). The cases of ATM frauds and skimming have been more and more common in the UK and across the globe. This is relevant even in case of the young students who are the new generation users of the ATM services. According to FICO, the number of ATM frauds and skimming incidents in 2015 in America, the UK and other European nations has increased to an unbelievable 546 percent as compared to 2014 (Krebson-Security, 2016). This shows the high necessity or need of awareness among the students and the other users regarding the ATM security and safety use measures (Krebson-Security, 2016). The research here would focus on identifying these necessities or needs and issues or loopholes that must be addressed, in terms of the awareness of students regarding the knowledge of security measures with the usage of ATMs. The primary focus of the research has been the students as they are the new generation of users of ATMs and therefore, they should be more aware than their senior fellow users.

1.2 The Background

Furthermore, several researches have been conducted on the effective use of the ATM cards and how the knowledge of the security measures of the ATM usage can aid or help in producing a safer use of ATMs. There have also been several researches in the area of ATM frauds and skimming and its impact on the ATM users. The literature review section focuses on many of such researches. However, the number of researches being conducted on the awareness of young students regarding safer use of ATMs is limited. There is also an increased necessity or need of it as young students are the new users of ATMs therefore, they need to be more effectively prepared than their fellow senior ATM users. That’s why the research here will focus mainly on the young students who are
apparently the newer users of ATMs and how awareness of the ATM security measures can benefit them.

1.3 The Problem Statement

The problem statement that will be addressed in this research paper is the necessity of awareness of the ATM security measures that the young students must be aware of. The research will understand the existing loopholes or issues in the knowledge level of these young ATM users and how these issues can be addressed.

1.4 The Significance of the Research

The research holds high importance and significance as the issue of the ATM frauds and skimming have become more and more common in the UK as well as in other parts of the world. The issues become even more challenging in case of young students, as mostly they are the new users. These facts make them more susceptible to the ATM frauds and theft issues (Sidel, 2016). Thus, the focus and assessment in the research will try to understand and picture the knowledge awareness of these young students regarding the security and the safety in ATM usage. This research would aid or help in identifying the knowledge loopholes or issues that must be addressed to ensure ATM security from theft and skimming. Moreover, the interview of the former bank employee would help in providing effective recommendations that could be useful for all the ATM users.

1.5 The Research Aim

The aim of this research is to understand the awareness levels amongst students pertaining to security issues and precautions required in the ATM usage.

1.6 The Research Objectives

The below objectives can help meet the research aim:

- To understand the current awareness levels and the knowledge of the students in relation to the ATM usage.
- To assess how banks play their role in protecting the security and privacy of their customers.
• To make recommendations to students on the best possible ways to safeguard their security and avoid skimming incidents.

1.7 The Research Questions

The below questions have been framed for this research paper:

• What is the current awareness level of students using ATMs, on the safety precautions and guidelines?
• How do banks generate awareness and knowledge about safety practices to these students?
• What steps can be taken by students to ensure protection from skimming incidents or security issues?

1.8 The Rationale of the Research

There are several reasons, which justify the rationale for this research paper. However, the primary reason for the research is the widespread lack of awareness of ATM related security in users, especially among the young students. Another major rational for the research is the increasing usage of ATMs across nations, which creates a natural requirement of awareness among users regarding the security, concerns in ATMs. The research has also focused on the young students, as they are the largest proportion of the new users of ATMs every year, which in fact makes them most vulnerable or unguarded which makes them defenseless. According to Simmons, safety and precaution is a primary requirement when it comes to banking related activities, as the stakes are too high (Simmons,, 2014).

1.9 The Limitations of the Study

The research also suffers from certain limitations. Some of the major limitations for this study or research are:

• The sample size for the survey is only 50, which is too small comparing to the population, which would create limitations on the generalizability of the findings.
The research is being conducted only through qualitative analysis this will also make the findings very subjective and open to biasness or unfairness. Thus, there will be high chances of unfairness in the findings of the research.

Interviews will also be conducted on only one bank employee and one student which is also too less to form any conclusive conclusion.

1.10 The Structure of the Dissertation

The dissertation would be followed by a well defined and a planned structure, which is explained below in detail.

- **Chapter 1:** Introduction: The introduction section explains the basic motive of the research along with the aims, the objective and the research questionnaires.
- **Chapter 2:** Literature review: The literature review takes a detailed dig or deep research on the existing literature and researches being done on the subject, which is about ATM Security.
- **Chapter 3:** Research Methodology: The methodology section assesses the research methodologies being used in the research, such as the purpose, the philosophy, the data collection and so on.
- **Chapter 4:** Results: The results section describes the results or responses obtained from the survey and the interviews.
- **Chapter 5:** Findings and their Implications: The findings section analyses the results’ and describes the patterns found in the results using a thematic analysis approach.
- **Chapter 6:** Conclusions and Recommendations: Based on the findings, conclusions are arrived at, and also important recommendations are provided at the end.

1.11 Conclusion

The introduction section in detail describes the aims and the purpose of the study and it shows the rationale behind the research. As stated in the significance of the research, the research is important as the issue of ATMs theft, skimming and frauds are popular in the UK and other parts of the world. The introduction section also explains why the research focuses on the young students and why there is a high necessity in creating awareness among them regarding the ATM frauds and security...
issues. The introduction section along with explaining the aims and the objectives of the research also explains the limitations of the study in detail.

Chapter 02: The Literature Review

2.1 Introduction

This section will help to provide the basic concepts of skimming and other related frauds at ATMs. It will also help in providing a basic understanding of the mechanism behind the skimming attacks and the mode of operation that is used by the fraudsters or the skimmers. Basically, an attempt will be made in order to describe the rising incidents of the skimming and the other fraud attacks on the ATMs at a global level and within the UK.

2.2 The Basic Understanding of ATM skimming

To begin with, the term ATM skimming describes the methods that the criminals use to capture the account information of a person on the back of the bank’s card after they used it at an ATM’s point of sale terminals. Furthermore, the criminals use devices like “skimmers” to capture the details of an ATM credit or debit card, this information is usually stored in the magnetic strip of the card (Shaikh, 2012). The information on the magnetic strips of the card can be read and deciphered by the application of a small card reader, which is kept close to the or on top of the slot of the actual card reader in order to read and record the information which is present on the magnetic track of the card. Moreover, after removing this malicious device the recorded data can be downloaded. To add to that, skimming is the process of capturing the private and the personal data of the cardholder by compromising a card-reading device for some financial or other gains. ATM skimming can be considered as an identity theft for debit and credit cards. That’s because hidden electronics are used by thieves to copy the personal data of the cardholders from the magnetic stripes of a card (Singh, 2012). A PIN capturing device or camera is also used generally with a skimming device. Criminals then store the stolen information in counterfeit or fake cards. In other words, fake credit cards carry the stolen information of the ATM skimming victims. These victims often carry their credit cards without knowing that they might have been considered as a target of a stealing crime. These fake cards appear legitimate, with issuers, logos and magnetic strips. The skimmers often use the fake
cards a few times and then abandon them before the victim realizes and reports this misuse to their issued bank (Singh, 2012). Moreover, more cards are still being issued now; the merchants have to still invest in the EMV terminals. Due to this delay there are still many cards, which have the traditional magnetic strips on them (Barker & Sheridon, 2008). The card remains vulnerable to skimming as long as the magnetic strip is present on the card with the EMV chip.

2.3 The Mechanism of ATM Skimming

It has been identified that, in an ATM skimming scenario the criminal selects an ATM, which becomes his or her target. After selecting the ATM, the criminal gathers the personal information of the cardholder using two ways. First he or she uses a portable card reader which reads the account information on the magnetic strip on the back of an ATM card (Worthington, 2009). This card reader is attached over the card reader of the ATM machine. It is designed in such a way that it looks like a part of an actual ATM. This not only gathers the information as soon as the bankcard is drawn into the ATM machine but it also stores it in the memory chip, which is present inside the reader. Next a pinhole camera is installed somewhere into the ATM machine to record the personal identification number (PIN) of the cardholder as soon as he or she enters it into the machine. Furthermore, after keeping the skimming device on the ATM machine for some time, the criminals remove them and take those devices to a separate location where they download the information that is present or stored inside the card reader. The video in the camera is used to obtain or save the PIN numbers of the different accounts. Through these steps the skimmer than transfers the different account information onto a blank card and then use the clone or fake card to obtain money from the bank accounts without the knowledge of the cardholders (Nwankkwo, 2013). The figure below illustrates the most susceptible areas for the Skimming devices.
**Figure:** Where to spot the Card Skimming or the PIN Capturing devices on an ATM Machine (Wild, 2015).

The figure below also illustrates the difference between a tampered and an un-tampered ATM Machine.

**Figure:** How to identify the difference between a tampered and un-tampered ATM Machine (elitepersonalfinance.com, 2015).
As shown or seen in the figure above, in a normal ATM, the flash card entry can be easily noticed which is not sparsely visible or completely invisible in a manipulated or tampered ATM. This means that most skimming devices tend to obscure the flash card indicator, which should serve as a vital or important clue for the users. In the tampered ATM, the attached device looks like a standard terminal, as it is manufactured to resemble the same.

Skimming devices can also be ‘piggy-backed’ into the card reader as shown in the figure below:

Here we have an example of the skimming device being piggy-backed onto the card reader.

*Figure: The Magnetic card reading device used for ATM skimming* (Siciliano, 2015).

Apart from the above-mentioned devices that read the card, fraudsters or skimmers would also try to read the pin that is entered by the customers. Various approaches are devised to make this possible. A pin-capturing device may be fitted at the top of the ATM keyboard, which takes snaps of the numbers, which the users enter.

The figure below illustrates the same:
Figure: The Pin-capturing device that is fitted right above the ATM keyboard (Feinberg, 2014).

Moreover, other approaches may also be used to capture the pin entered. The figures below illustrate how cleverly hidden cameras may be placed surrounded by brochures.

Figure: Using hidden camera to capture pin numbers entered by the ATM users (Geuss, 2016).

Apart from that, skimming also involves using duplicate keyboards carefully planted over the genuine keyboard of the ATM Machine as shown in the figure below:
As can be seen or shown in the figure above, the duplicate keyboard is hardly noticeable as it completely matches the regular ATM keyboard, and deceives the customer to input his or her pin number. Once pinned in, the keyboard stores the customer pin, along with the magnetic card readings captured using another device. Using both of the mentioned information, fraudsters or skimmers are able to clone the debit cards and steal customer money. It is during the quiet periods like early in the morning or late in the evening when the skimming devices are installed into the ATM machine. The length of the time skimming devices is nearly equal to 24 hours. Both a card skimmer or a card reader and a camera, which is a PIN-capturing device, are required for a successful skimming attempt to be undertaken. Criminals wait around to remove the devices after the customers have used the ATM machine. The downloaded information is then transmitted wirelessly to the criminal’s other devices.
2.4 The Global Rise in ATM Skimming Incidents

The ATM frauds are increasing globally. As the US ramps up its mitigation to EMV, this is likely to grow further. Even though the credit and debit card technologies have become sophisticated, the old fashioned ATM skimming is still increasing steadily. Last year alone accounted to a loss of more than $2 billion with respect to the ATM skimming all around the world. Additionally, the skimming frauds amount to 33% of all the fraudulent activities that occur globally and the losses that occurred or took place are 98% because of the skimming crime. All kinds of skimming attacks have also increased in the banks of Europe since last year. The statistics of the European ATM Security Team (EAST) show that around 18,738 incidents have been reported against the ATM crimes in Europe since 2015. This amount roundup to around 51 attacks for every 1000 ATMs attack over a certain period of time which means that there is a 19% increase since the previous year (FFA UK, 2015). Reports of EAST say that in 2015 around 327.48 million euros were lost. This was a total of 17% increase when compared to the loss incurred or that took place in 2014, which was around 279.86 million euros. These losses amount to a loss of around 884,069 euros for every ATM (FFA UK, 2015). EAST’s reports also explain the skimming activity with the help of specialization. For example, it was found that there were around 2,657 cases, which were reported where the thief tried to blow up or use other physical methods to make his or her way into the cash machine. Solid explosives or explosive gas attacks were also used to collect the data. An increase of 34% was observed from 2014, which means that 7.2 attacks were undertaken per 1000 ATMs (FFA UK, 2015). Fifteen malware incidents were also reported against the ATMs in Europe in the year 2015. These incidents were either ‘cash points’ or ‘jackpotting attacks’. EAST says that this is a decrease of 71% since 2014 (FFA UK, 2015).
The European Fraud Update report by EAST, which was published in 2016, states the different skimming incidents that had occurred in the European region. The country crime updates which was provided by representatives of 18 countries in the Single Euro Payments Area (SEPA), and 6 non-SEPA countries was used to write the report. 19 countries reported that card skimming in the ATMs, M3 – Card Reader Internal Skimming devices are used for the skimming purpose. The motorized card reader behind the shutter contains this type of device, which is placed at different locations. 7 different countries reported these types of attacks. Eight countries reported skimming attacks, which were on different terminal types and these type of attacks were reported by the unattended payment terminals (UPTs) these terminals were located at petrol stations in six different countries. Eight countries reported the logical security attacks and the ATM malware attacks, which involved the usage or attempted usage of the black box devices to allow the unauthorized dispensing of cash (FFA UK, 2015).
2.5 Why Skimming and Other Frauds are Serious Issues

Skimming and other forms of frauds associated with card usage have been witnessing a steep rise in the recent years. The data released by the Financial Fraud Action UK (FFA UK) gives a detailed analysis of the trend. The frauds in the UK payment industry are handled by the FFA UK. They lead the collective fight in this respect. Its membership includes the credit, debit and card or charge issuers, card payment acquirers and major banks. FFA UK takes the help of industries to defend the consumers and businesses from financial frauds by becoming the authoritative leader and creating a hostile environment for the fraudsters or skimmers. Data released by FFA UK in 2015, shows that a total of £567.5 million worth of losses were incurred or provoked by the UK issued cards in 2015, which was an 18% increase from the amount of £479 million in 2014. Due to the overall card fraud losses the amount that was spent on cards has increased in 2015, which has increased from 7.5p per £100, spent in 2014 to 8.3p per £100 in 2015. The following figure shows the fraud losses that took place regarding the cards that were issued in the UK from 2006 to 2015.

Figure: Total losses due to the card frauds in the UK from 2006 to 2015 (FFA UK, 2015).
As can be seen above, the last four years have witnessed a year on year increase in the number of fraud cases pertaining to card usage.

2.6 Types of Frauds that can occur at ATM Machines

Fraudsters or skimmers target the cash machines or ATMs in order to steal the cards or the card details using three different ways or approaches, which will be listed below.

**Entrapment devices**: These devices when inserted into the card slot of the card machine tend to retain the card inside the machine. Then the person is made to reenter his or her PIN, which is ultimately noted down by the criminal. After the cardholder leaves, the criminal removes the device with the card and then withdraws the cash from the account.

**Skimming devices**: This is attached to the cash machine and is used to withdraw details from the magnetic strip of the card. Using a miniature camera then captures the PIN of the user and then a fake magnetic strip card is produced. This is used with the genuine PIN to withdraw cash from the machine overseas, which have not upgraded to chip and PIN.

**Shoulder surfing**: Criminals watch the cardholder while he or she enters the PIN and then steal the cards using distraction techniques or through pick pocketing.

The seriousness of these frauds can be indicated in terms of the below figures released by the Financial Fraud Action in the UK.
As can be seen in the figure above, the year 2015 witnessed a 20% rise in the number of incidents of ATM machine frauds, primarily due to the use of sophisticated skimming devices which customers are largely unaware of (FFA UK, 2015).

**Chapter 3 – Methodology**

**3.1 The Introduction**

The research methodology is the process of establishing a complete standard process for conducting a research. According to Dawson, the research methodology determines the effectiveness of the research as well as the effectiveness of the findings to a large extent (Dawson, 2009). This research would be focusing on a wide range of primary data that would be collected from several respondents; thus, the research methodology will determine the nature of the processes that would be used in conducting the research. The research methodology section here would include the
research philosophy, the purpose, the strategy, the approach, the data collection, the sampling, analysis, the reliability, the validity, the generalizability, the ethical issues and the conclusion.

3.2 The Research Philosophy

According to Elliot, the research philosophy is about the manner in which a research builds the source, the nature and the nurturing of the knowledge expected from the research (Elliot, 2005). The research philosophy adopted here would be interpretive in the nature where the responses of the respondents will be interpreted using interpretivist research philosophy. It is about the notion in which the research process is going to be conducted or undertaken (Degu & Yigzaw, 2006). The analysis in this research would be about performance of qualitative analysis of the collected primary data. According to Ruane, the interpretivism approach would allow a mix of objective as well as subjective approaches in assessing the research subject and establishing valuable results for the research (Ruane, 2008).

3.3 The Research Purpose

A research must have a purpose to ensure that the research is being conducted and progressed in the right direction. The purpose of the research here would be to understand the existing awareness of youngsters regarding the security measures and effective usage of ATMs. The purpose of the research would be identifying issues and loopholes in the existing awareness and areas of scope of improvement. Based on the identification of the weaknesses and loopholes in the existing knowledge of the youngsters regarding safe and effective use of ATMs, suggestions would be made regarding enhancing the knowledge base about ATM security. The feedback of a bank employee and the experience of a youngster who has faced security issues while using an ATM are assessed as a part of the purpose for this research paper.

3.4 The Research Strategy

According to Silverman, the research strategy is about the manner in which you conduct your strategy. It is about choosing whether the research is to be done using primary data or secondary data or even both. It is about the choice of the manner of analysis, qualitative or quantitative or
even both (Silverman, 2007). The research strategy for the analysis of security awareness among youngsters regarding the use of ATM machines and cards would be that of primary and inductive research strategy. The research would focus only on the collection of primary data from several respondents. The research strategy would also involve the use of surveys. According to Dawson, surveys are an effective way of the collection of the data and the conducting of the social science research (Dawson, 2009). Based on the responses of the respondents in the survey, interpretation would be done using qualitative analysis. The primary research strategy is chosen to easily and effectively understand the issue at hand and also to do or to produce an analysis on the focused data collected for the purpose.

3.5 The Research Approach

The choice of the research approach can be from the available three types, which are deductive, inductive and adductive. According to Denzin & Lincoln, deductive approach can be used to prove the correctness and applicability of an existing theory in the chosen scenario. An incomplete occurrence or observation is explained and understood by qualitative analysis in an inductive research approach (Denzin & Lincoln, 2000). In this research the existing awareness of youngsters regarding the security of usage of ATMs would be studied and based on the analysis of the collected data, theories and inferences would be established. This would be done therefore; using an inductive approach would be the best choice. According to Denzin & Lincoln, inductive approach first observes and tests existing information, identifies a pattern and then establishes a theory (Denzin & Lincoln, 2000). The research will also proceed on similar direction.

3.6 The Data Collection Method

The data collection method used in the research would be that of primary data collection and qualitative data gathering. In this research three different sets of primary data collection would be done in which one of them would be a survey and the two other would be face-to-face interviews. The survey would be done on a set of 50 respondents who would be youngsters using ATM services, the sampling of which would be described later. The questionnaires would be targeted on a bank employee who is well aware of the security knowledge regarding ATMs and understands its
importance for youngsters using ATM. Another respondent would be a youngster who has faced an issue of security matters associated with the use of ATMs. The survey would be beneficial as it would be easier to conduct and more effective for the chosen research. Interviews have been done on a limited number of respondents because of the involvement of the high volume of time and efforts.

3.7 The Sampling Technique

According to Neuman, sampling is done to find the correct representation of the population. Given, the vast population of secondary sources of information for the research, sampling would be effective to find a suitable representation of the chosen population (Neuman, 2000). As per the necessity of the research, purposeful sampling technique would be used to identify the 50 respondents for the survey and the two respondents for the interview. The reason of use of purposeful sampling in this research is because while answering to the questionnaires in the survey and interviews, the respondents would also gain knowledge on the chosen subject. Other major sampling techniques such as cluster or stratified sampling may not be appropriate for the research.

3.8 The Data Analysis

The data analysis should be done effectively in order to achieve effective and applicable results. This research would be adopting thematic data analysis using qualitative analysis on the primary data collected from the surveys and the interviews. The data collected from the interviews and the surveys would also be analyzed qualitatively depending on the nature of the data, to ensure the analysis is done with a broader perspective. Using this analysis technique, themes or patterns will be discovered across the collected data, which then will be presented as the result of the research.

3.9 The Reliability

The research conducted would be highly reliable as the data would be collected directly from the primary respondents and therefore, the authenticity of the research would be ensured. The respondent’s’ identity would be kept secret but it would be ensured that only applicable respondents for the research are approached. This would ensure that the results of the research are reliable for being referred to understand the implication of awareness of security concerns in ATMs.
usage. The use of respondents only relevant to the research would ensure high reliability of findings of the research.

3.10 The Validity

The research results are expected to be highly valid for the analysis of the necessity of awareness about security measures and knowledge during using ATMs. The validity is expected to be high, as only primary data will be collected from respondents directly. Therefore, not only the data would be reliable but also valid as the data collected would be recent and applicable to a present scenario. The use of current data would ensure that their analysis would provide results that are applicable to the current level of awareness of youngsters regarding the importance and the knowledge of the security in using the ATMs.

3.11 The Generalizability

Though the research looks completely appropriate for a very large population, given the fact that almost everyone uses ATMs these days, but the generalizability of the research finding would be limited here. The generalizability of the findings of the research here therefore would be limited mainly because of the small sample size. However, the findings of the research can be used as a basis for conducting more in-depth research on the subject.

3.12 The Ethical Issues

The research ethics is the moral and ethical responsibility of the researchers and it must be taken seriously throughout the execution of the research. Research ethics is extremely crucial for the validity and reliability of the research processes and therefore the findings. The findings of the research will have no validity and reliability if research ethics is not well taken care of (Denzin & Lincoln, 2000). The research will be following an ethical process as all the respondents will be asked to provide their consent for their participation, once they are explained the purpose and aims of the research. Also the identities of the respondents will be kept secret and would not be disclosed without their prior consent. The research is being done for educational purpose and it won’t be used for any commercial gains. No data manipulation would be allowed under any circumstances.
3.13 The Conclusion

The research methodology section explains the manner in which the research would be conducted. The research methodology has been designed in a manner such that the philosophy, the approach, the sampling and the other aspects are in sync with each other and aid in achieving the desired results of the research. The philosophy of the research is of interpretive whereas the strategy would be of inductive and primary research. The research will also be using purposeful sampling and only primary data collection. The challenge in the research would be of implementing the prepared methodology effectively and therefore, special care would be taken to ensure that the methodology of the research design is implemented effectively. This would enhance the validity and the reliability of the findings of the research. The themes established in the research could be used for further in-depth analysis of the subject matter chosen with a larger sample size, so that the generalizability will be enhanced.

Chapter 4 The Results

4.1 The Result from the Student Surveys

Discussed below are the results obtained or the results that were gathered from the student surveys.

What is your Gender?

This question was aimed to understand the profile of the survey respondents. As can be seen or shown in the figure below, 60% of the respondents were females while 40% were males.
How old are you?

This question was aimed to categorize the respondents based on the demographic variable, which is the respondent’s age. As can be seen or shown in the figure below, 28% of the respondents belonged to the age group of 18-22 years old, while a large majority of the respondents, 64%, were in the age group 23-27 years old. A small number of respondents, 8% belonged to the higher age group 28-32 years old.
Where are you Studying?

This question was aimed to understand the education level of the respondents. The idea was to mainly see the distribution of ATM users across various educational levels. As can be seen or shown from the figure below, the largest group of respondents, which is 38% study in universities. 16% of the respondents are in college, and 14% of the respondents are in high school.

*Figure: The Age Group of the Respondents.*
Do you own an ATM Card?

This direct question was aimed to understand the distribution of the ATM card possession amongst the respondents. As expected, a large majority of 98% made use of an ATM card, while only 2% of the respondents denied ATM usage.
Select the banks whose accounts you hold

This question was aimed to understand the distribution of bank account holders within the selected sample for the survey. 16% of the respondents had accounts in HSBC Bank, 4% of the respondents had accounts in Lloyds Bank, and 14% of the respondents had accounts in some international banks. The majority of the respondents, which was 66%, had accounts in banks, which was not there or was not listed in the survey questionnaire list. The figure below illustrates the same:

Figure: The Respondents response based on ATM card usage.
Figure: Distribution of Respondents based on the Bank in which they owned or held an account.

What made you choose this Bank?

This question was aimed at understanding as to why students choose a specific bank. The idea was to understand if they consider the ‘security’ history of the bank as a factor while choosing or selecting it. For this reason, ‘security purposes’ was added as one of the options for the respondents to fill or choose. As can be seen or shown in the figure below, only 10% of the respondents choose their bank
based on security considerations, while a large majority chooses on the basics of services, loyalty, or other factors.

**Figure:** The Factors, which Respondents consider while choosing a Bank for them-selves.

**Do you prefer ATM Machine rather than going to actual Bank?**

This question was aimed to understand the money withdrawal behavior of the respondents. It can be seen from the responses that, 100% of them prefer to go to ATM for the money withdrawal purposes, and no one would like to go through a long queue bank processes to withdraw money.
Select the Services that are available to you through the ATM Machine

This question was aimed to understand the nature of services, which respondents are able to use through ATM machines. As can be seen in the figure below, 96% of the respondents believed that they visit ATM for cash withdrawal purposes only. Other services like, money transfer, balance enquiry, or bill payment are lesser as compared to cash withdrawal services.
This question was again aimed towards understanding the tendency level of students towards visiting ATM versus being serviced by a bank staff member. As can be seen in the figure below, 84% of the respondents like to be served by an ATM while only 14% of the respondents want to be physically served by a bank staff member.
Are you aware of the security precautions that need to be taken in case of a card being stolen?

This was a direct question aimed to understand the awareness level of the respondents on the necessary precautions, which need to be taken in the event that their card gets stolen. As can be seen or shown from the results below, 88% of the respondents believed that they understand the safety guidelines, while 12% of the respondents did not consider the same.
What makes you feel safer while using ATM?

This question was aimed to understand the perception of respondents as to what constitutes or considers as ‘Safety’ for them. As can be seen or shown from the findings, 20% of the respondents believed that safety implied closed spaces. 26% of the respondents believed that controlled access ensured better safety, while 18% of the respondents believed that presence of security guards ensured better safety. While a large majority of 32% of the respondents believed that they already felt safe.

*Figure: Respondents awareness on the safety precautions for lost ATM Card.*
Figure: Respondents perception of security within ATM premises.

Are you aware of the term ATM skimmers?

This question was aimed to understand the awareness level of the students on the prevalence of skimming incidents and frauds. As can be seen or shown in the figure below, only 48% were aware of what ATM skimming means, while the majority of them, 52% had no idea of the skimming related incidents or frauds.
**At what time do you prefer going to ATM?**

This question was aimed towards understanding the common timings in which respondents visit ATM machines. As seen from the participant responses, a large majority, 37.5% do not have any specific time for an ATM visit. Similarly, 32.5% of the respondents visit the ATM in the mornings, 10% of the respondents visit the ATM in the evenings. 12.5% of the respondents visit the ATM in the afternoon while a small percentage of 7.5% visit the ATM whenever they are free.
4.2 Results from the Semi-Structured Interview of the Former Bank Security Officer

The purpose of this interview was to gain a firsthand understanding of how banks perceive skimming in general, and the precautions, which they take from their end towards curbing or holding back these incidents.

**Background of the Respondent**

The first interview conducted was with a former security officer that used to work in one of the most popular banks. To begin with, questioning the former officer’s background helped to understand the role, which he played within the Bank. The respondent was mainly responsible for developing, implementing, and administering various security initiatives that are taken by the bank. He acted as a middleman between the customers and the bank security team and he had already spent 9 years working in the organization. He was responsible for overseeing security arrangements at bank facilities, ATM machines, and other areas of potential thefts or robberies. He was also an active participant in the scheduled audits, which the bank conducted to assess its control structures and security measures. This was convincing regarding the suitability of the respondent’s answers for meeting the research objectives.

*Figure: Preferred time for ATM visit of respondents.*

- **Preference time for ATM visit**
  - Evening: 10.0%
  - Afternoon: 12.5%
  - Mornings: 32.5%
  - No specific time: 37.5%
  - When I am free: 7.5%
Discussion on Experience and Security Issues

The respondent further elaborated or stated on his future goals as the security officer. He elaborated that before he left the bank he made plans to implement a powerful security policy within the bank, which would allow, generate awareness amongst customers, and prevent them from potential fraud incidents, this plan was undertaken based on his suggestions. He commented on various provisions, which the bank allows in case a customer loses his or her credit or debit card. He stated that the bank continuously strives to inform its customers on the possible thefts and issues which can arise in the usage of these cards. He also stated that in case the customer loses his or her credit or debit card, or detects any case of fraud, the bank allows for multiple 24x7 helpline numbers, which immediately blocks the card from further usage. The former officer commented that most of these numbers are free and can be dialed from any cell phone or landline. He also stated that the bank also takes endeavors to publish important guidelines on card usages on its official website. The bank is fully aware of ATM skimming incidents and the bank plans to take various measures to prevent such occurrences. The former officer also stated that as a first reaction to such incidents, the bank has its own policies and procedures defined. The security and risk department immediately visits the ATM that’s been tampered with and begins the necessary investigations. CCTV cameras installed in each of the ATM machines play a crucial role in tracking the criminals involved. They coordinate with the local police agencies to track fraudsters or skimmers in the district of the crime. The respondent agrees that catching fraudsters or skimmers after the incident is not a major problem as necessary security measures and camera footages facilitate the investigation process. However he does agree that preventing the crime in the first place is a major challenge that every bank faces.

Discussion on the Challenges Faced by the Respondent

The security officer believes that the greatest challenge for the bank has been to keep a check on the use of sophisticated technologies for skimming. He believed that skimming devices have been evolving to resemble the exact ATM parts and hence at times it becomes difficult for customers to track them. Similarly, he stated that almost 90% of the reported incidents of skimming involved very tiny cameras, which were really hard to detect for any customer. Under such circumstances, the
respondent believed that gaining customer trust and ensuring their safety is becoming a major challenge for the bank in current times. He also believed that incidents of skimming are a major loss for the bank as the current regulations require the bank to refund back the fund or the money stolen due to skimming, which is why elimination of the fraud is the top priority for most of the banks. Another challenging area, which the respondent believed, was to spread necessary awareness amongst students about the seriousness of the skimming issues. He believed that, most of the customers, including students were either ignorant, or not cautious enough when visiting ATMs. He stressed that, in case customers pay attention and notify the presence of skimming devices in ATMs, losses can be prevented at an early stage. To make this possible, the bank has been showing videos of tampered ATM devices, and warning signs within its corporate website. Customers are also informed through SMS on the key precautions, which they should take before drawing out money. The former security officer than stated that he felt like it was time for him to try different security departments, within different organizations and that’s why he left his former job.

4.3 Results from the Semi-Structured Interview of the victim of the ATM Fraud

The purpose of conducting this interview was to gain a firsthand understanding of how a typical skimming incident would look like, and to get insights into precautions from the perspective of a victim.

Student Background

The student interviewed was a university student whose name and nationality are not discussed here as a part of the research confidentiality which is followed within the ethical guidelines. The student belonged to the age bracket of 23-27 years old, which indicates sufficient maturity to understand skimming and the related bank frauds.

Discussion on the Incident

The student stated to have used one of the ATMs located in a remote part of his city during early morning hours. Unaware of the signs or symptoms of a tampered ATM, the student made his transactions and came back to attend his morning classes. It was only when he reached the ATM again, after a few days that he realized that he has been tricked. As a quick measure, the respondent
reported the incident to the bank as soon as he found out. Based on the information that the victim provided, the bank and the authorities were able to track and trace the tampered ATM. The respondent believed that this incident made him realize that ATM frauds can take place anywhere, and that’s why it would be advisable to always keep “your eyes open”. He also stated that, before the incident, he had absolutely no idea what skimming involved, and how serious the issue was. From the bank and the authorities, he later found out that the fraudsters or the skimmers had made use of a duplicate keyboard to capture his pin number, and a card reader has been implanted to read the magnetic strip in his debit card. Overall, his lack of knowledge on skimming made him undertake the transaction normally by ignoring the visible symptoms.

**Relationship with the Registered Bank**

The student stated that having been through this traumatic experience, he believed that the greatest fault lay with him, for ignoring bank warnings and messages on skimming issues. In his case, the bank played a major role in supporting him by making adequate refunds on time. However, the respondent believed that the larger duty lay with the customers themselves. With regard to safety precautions, the respondent believed that he was too ignorant to understand the skimming mechanism in the first place. As an ATM user, he always believed that it was only through physical means, like card stealing, or robbery that would cause harm. However, this incident made him realize, what he phrases as “the dark side of technology”.

**Chapter 5 The Findings and their Implications**

**The Findings and their Implications**

A number of crucial findings and their implications are evident through the analysis that was conducted above. The findings obtained from the student surveys help to analyze two aspects of the issue as shown in the figure below.
As can be seen in the figure, various findings emerge with regard to the demography of the respondents. It can be found that a large majority of respondents belong to a matured age group of 23-27 years old, and they are primarily university goers. Similarly, multiple findings emerge with regard to the behavior of the respondents. Firstly, it can also show and state that respondents believe in choosing banking services based on attractive loyalty points, service offerings of the bank or other considerations. Security history of the bank seems to be considered less important by most students due to the fact that most of the students are unaware of what really happens during a skimming crime. Secondly, most of the students prefer going to ATMs instead of using services directly from the bank and the primary purpose of the visits is mostly for cash withdrawal purposes only. Next, most commonly, students have no specific time to visit ATM machines, although a large number of them also prefer visiting the ATM in the early morning hours because they consider it to be more appropriate and safer. Moreover, with regard to the knowledge levels of the students, it can be seen that a large majority of them are highly unaware of the skimming and the other related fraud issues. They believe that an ATM with a security guard or closed spaces is sufficient to bring about a secured and a safe environment. A large number of them even do not feel any threat and
regard themselves as already safe due to the fact that most of them are unaware of such incidents. To add to that, the semi-structured interviews also reveal that banks do have a security policy and infrastructure to ensure customer safety. They implement security initiatives from time to time; they also conduct scheduled audits and work towards generating customer awareness. In terms of helping customers reach out in time, they make provisions for 24x7 helpline numbers, emergency response teams, CCTV camera recordings at all bank ATMs and other services. However, banks face challenges with regard to changing technological sophistication of skimming devices, the lack of sufficient cooperation from customers and the refund losses that they have to incur or be liable to from time to time. The victim interview also confirmed most of these findings, as although being a matured university goer, he was highly unaware of the skimming frauds and the precautions. He exhibited little understanding or insight of the issues, which he may fall into for the lack of being observant and careful in ATMs usage. Furthermore, all these findings have implications with regard to understanding the current awareness levels of respondents on the occurrence of frauds at ATM places, the practices and precautions which are being undertaken at the corporate level by banks and the necessary measures which can be brought in, in order to increase customer awareness.

Chapter 6: Conclusions and Recommendations

6.1 Conclusions

A number of key themes emerge on the form of conclusions from the findings and their analysis. The figure below illustrates the conclusions arrived at:
As can be seen in the figure above, an important theme to consider is the over-confidence, which is visible through student responses. It can be seen that most students do not feel threatened or do not see the seriousness of ATM security therefore they don’t find it as an issue. Closed spaces and security guards in the form of physical security barriers seem to be sufficient for them. Similar over-confidence can be seen in their bank choosing behavior, wherein they do not choose or consider security considerations to be an important parameter to finalize their bank choice. Secondly, both the knowledge and the behavior of the customers have to play a crucial role in preventing them from self-harm. The interactions reveal a clear lack of knowledge to be easily evident amongst the respondents. Students show little understanding or knowledge towards skimming frauds and are highly unaware of the services which bank provides to prevent skimming frauds in the first place.

Next with regard to the ATM visit and usage behavior of the customers, it can be concluded and stated that although most students would like to visit ATM premises for conducting transactions, they have not paid attention to security guidelines, which banks provide through their websites. A lack of service utilization is also evident in the manner in which these customers operate. They are
not truly aware of the 24x7 helpline numbers or other services, which most of the banks provide. Next, it is also evident or obvious that skimming technologies are also evolving with time, making it difficult for the banks to develop full measures to conflict decrease or stop their usage. Most banks find it challenging to keep track of sophisticated ways of stealing and hence there is a need to evolve security measures from time to time. Similarly, there is a need to capitalize on the positive efforts, which banks have been putting through. Banks are readily available to help customers approach them and obtain required information on skimming related dangers. However, not many efforts can be seen from the customer end to capitalize on these information opportunities. Overall, it is quite obvious that precautionary actions from the end of customers themselves could form to be the key towards stopping or reducing such incidents. Given the challenging environment in which banks operate and the losses, which they suffer for customer negligence and theft incidents, it would not be sustainable to adopt a reactive mode towards such incidents. The solution would be to adopt a strategy, which is more proactive towards detecting frauds in the first place, being careful and watchful in usage of the ATM, and be aware of the process to reach out to bank officials to warn about an impending fraud issue.

6.2 The Recommendations

The detailed analysis and findings of the research shows that there are indeed several aspects in the domain of the ATM safety, which must be addressed. The recommendations section will focus on three major aspects of ATMs and banks safety measures. This would ensure a better-protected use of ATM and it would increase the avoidance of unwanted incidents that harms them. The figure below shows the general aspects that would be covered in detail in this recommendation section.
As stated above, each of these sections will be described in detail and the corresponding recommendations or best practices to be followed will also be explained. The context of the ATM security is very critical and therefore, it would need a collaborated approach between the banks and the users.

**General Awareness**

The general awareness section here will be explaining the basic choices or decisions that young students take as an ATM or banking services’ users. These recommendations are more specific to the whole banking sector along with the usage of the ATMs. These recommendations are completely based on the findings of the research. Some of the major recommendations on the field of general awareness in ATM usages are shown and stated below in the figure.
**Figure:** *Recommendations in General Awareness for Banking/ATMs*

- **Choosing Banks:** The research clearly showed that only a very small percentage of banking services users choose their banks on the basis of their security standards. In fact, several users don’t even have any idea about the safety and the security measures that are taken by their banks. Therefore, young students who open their accounts in the banks must be made aware about the security standards of the banks and they must understand its high importance.

- **Use of ATMs:** In the survey, it was found that the majority of the ATM users think that their ATMs are only for money withdrawal. It shows that they have limited awareness in understanding the several usages of ATMs. Thus, users and especially young students must be made aware of the several uses of the ATMs such as the money transfer, the bill payments, the balance enquiry, and the mini-statements. This would showcase the high utility of the ATMs, which might inspire the respondents to be more careful for the ATM security.

- **Over-Confidence:** The survey also showed the high degree of over-confidence among the young ATM users regarding the necessary ATM security awareness. This is dangerous, as even with adequate knowledge, ATM users must be updated with the latest security information, as the dangers with the ATM securities keep evolving. The factor of over-confidence also makes the young ATM users more prone to theft and skimming. Thus, the young ATM users must be convinced that they need to continuously update themselves regarding banking and the ATM security measures, to ensure their safety.
• **Awareness (Skimming):** The interview and the survey showed that the ATM users are not very much aware of the different kinds of theft and security dangers regarding the ATM usages. This shows that there is a necessity of compulsory education to the ATM users regarding the ATM safety and the banking precautions. This would ensure the required awareness among the ATM users and safeguard them against unwanted incidents or situations.

**ATM Usage & Security**

The analysis in the research clearly showed that there is a concern in the knowledge levels of the young students regarding the ATM usage and security issues. Education is a powerful tool and only by ensuring awareness among students, the ATM thefts and security problems can be avoided or reduced. These recommendations would aid the users in following the best practices that would safeguard them against the ATM security problems. Some of the major best practices that ATM users including young students can follow are:

- ATM users should not keep their ATM pins written anywhere, especially in obvious places like their ATM cards, back of their ATM cardholders or in a paper kept in the purse or bag. The user should only memorize the security pin of an ATM card, and no one else should know it. The user could keep it in a hidden place where others can’t find it.

- ATM pins should also not be written in diaries and in the backside of a deposit slip, which can get lost easily. Once found by anybody else, this puts the ATM users in a vulnerable position. Thus, at first ATM pins should never be written anywhere and even if the users write them, they should never be in places where it can get lost easily or could be found by other users.

- Keep a track of the details of the transactions in your accounts, which can be easily done through ATM cards. Users should quickly and proactively connect with the bank if there is any unexpected account associated with their accounts. As smart users, the details of ATM card transactions debit as well as credit should also be checked and monitored regularly. Users should and must get in touch with the bank officials in case of any discrepancies.

- Keep changing your ATM pins regularly and the same holds true for the online banking account password and other transaction passwords. The ATM pins should be set with codes that are not
obvious to others who know you. ATM pins should never be the important dates in your life. For instance, it should not be your own or father’s/mother’s or Spouse’s birth date and year.

- Finally keep your mobile phone associated with your ATM limited to yourself. Avoid friends and others looking into the contents of your mobile as it also contains several details of your ATM, bank account. Also avoid connecting your mobile to unsafe sites as it makes the content of your mobile including your ATM and banking details vulnerable.

**Safeguard against Skimming**

As it has been discussed in detail in the research, skimming is one of the most common and prevalent ways of ATM frauds and thefts. The research clearly defines several manners in which skimming is being done by thieves and frauds. This puts the whole ATM security aspects in jeopardy and thus lack of awareness regarding skimming in ATM machines is a real matter of concern for both banks as well as ATM users. The ATM users and banks can take several steps to stay protected against skimming activities. Some of the major recommendations in this direction are shown below in the figure.

*Figure: Best Practices and Steps to Safeguard against Skimming, inputs* (Hartman, 2015).
• **Be Vigil or Observant:** As an ATM user if you find the ATM reader a little loose or some kind of tape is attached to the ATM reader portion, the best thing to do in this scenario is to report it to the bank without using such ATMs. Thieves often attach another small reader between the actual ATM readers, which makes it completely theft prone. Users can even pick around with their fingernails to check that any other device is not attached in the ATM reader or the keypad.

• **Check for the Camera:** Whenever there is a skimming device attached with the ATM readers, thieves also attach a camera underneath the top of the ATM. This camera is used to record the ATM pins entered by the users. Checking whether there is a pin-sized hole underneath the top of the ATM can easily identify this type of camera. If this camera hole is present in this position of the ATM machine, do not use your ATM cards in this certain machine and inform the banking institutions. Also prevent others from using such machine as they may end up losing all their funds that are in their accounts.

• **Focus on Accounts:** Though the federal laws in the UK and most of the other countries cover banking frauds such as skimming but they are still not sufficient to protect the users. Banking or ATM users must report any unexpected debit or credit in their accounts as soon as they notice them. The more time the user takes in notifying the banks regarding skimming or any banking frauds, the lesser is their chances of being recovered.

• **Use Credit Cards:** Though not the best solution, but usage of credit cards provide some sense of security to the ATM users. Credit card money is the bank’s money and in case of any frauds or theft, it is the bank’s money that is stolen. As a card user, all you need to do is prove that it was not you who used the card.

• **Vigilance or keep an open eye in New Places:** Be more vigil or observant while using ATM cards in newer places such as tourist destinations and market places. It would be at best if you use the ATM machines that are present within the bank. That’s because they are less vulnerable to skimming and frauds.

• **Have Faith in your Guts:** As an ATM user you may at times find a situation as fishy or as susceptible which may be the positioning of the ATM, the wiring around the ATM or the
rejection of your cards. In case of such doubts or suspicions, do not use your ATM cards in this
certain ATM machine and inform the bank as soon as possible.

- **Better Safe than Sorry:** As an ATM user you need to always keep the security of your banking
account and card as the highest priority. You can always make a purchase few days later
therefore, whenever you are in doubt, avoid using your ATM cards.

### 6.3 Limitations of the Study

The study being conducted is a thematic analysis that has been done using the inputs from the
surveys and the interviews. However, there are certain limitations of the study, which must be
highlighted. One of the major limitations of the study is its small sample size, which makes it really
hard to derive a generalized theory or suggestions using the findings of the research. Therefore, the
results of this research may not be directly applied but it rather should be used as a baseline for
future future research. Another major limitation of the study is the nature of the analysis being
done. The research has used qualitative analysis only, which causes a concern regarding the
biasness or unfairness and subjective nature of the findings. Lack of any quantitative
analysis makes the result completely subjective. Another important limitation of the research has been its focus on
only two interviews, which is again a very small sample size for any kind of generalizability of the
findings. Thus, this research serves more on the aspect of providing a baseline for future research
rather than being used directly for making changes in banking services.

### 6.4 Suggestions for Future Study

Banking services are very critical and important services for the population and therefore, the
banking and ATM safety are equally very important. There is a scope of research on the manners in
which ATM security can be better taught to the ATM users. Users are usually not very proactive in
learning ATM and banking security and thus, by finding effective ways of teaching them, better ATM
security can be ensured. Another major aspect of the subject has also not been assessed in the
research, which can be used for future studies. This would be regarding the risks and high profile of
hacking of ATM cards through online channels. Phishing attacks and hacking of ATM details from
spam websites is also another concern for ATM and banking security. More study can also be done in
manners of educating old and senior citizens and other ATM users as their level of awareness regarding ATM and banking security is expected to be even lower than the young students.
References:


Appendices:

Appendix 1: Questionnaire for the Students

1) Gender
   - Male
   - Female

2) How old are you?
   - 18-22
   - 23-27
   - 28-32

3) Where are you studying?
   - High School
   - College
   - University

4) Do you own an ATM Card?
   - Yes
   - No

5) Select the banks whose account you hold:
   - HSBC
   - Lloyds Bank
   - Royal Bank
   - Barclays
   - Net West
   - International Banks
   - Other

6) What made you choose this bank?
   - Loyalty
   - Services
   - Security Purposes
   - More withdrawal options
   - All of the above
   - Other
7) Do you prefer using the ATM Machine rather than going to the actual bank?
   o Yes
   o No

8) Please select the following services that your bank provides through the ATM Machine:
   o Bills Payment
   o Balance Enquiry
   o Pin Change Option
   o Money Transfer
   o Cash Withdrawals

9) Select your Preference:
   o To be served by a banker
   o To be served by an ATM

10) Are you aware of the security precautions that you should take in terms of your card being stolen?
    o Yes
    o No

11) What would make you feel safer when using an ATM?
    o Closed Space
    o Security Guards
    o Controlled Access
    o I Already feel safe
    o Other

12) Are you aware of ATM Skimmers?
    o Yes
    o No

13) What time do you prefer using the ATM?
### Appendix 2: Semi-Structured Interview of the Victim

<table>
<thead>
<tr>
<th>Order of semi structured Interview with the one of the students who claimed to be a victim of an ATM fraud</th>
<th>Discussed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Ask respondent approval to use recording systems</td>
<td></td>
</tr>
<tr>
<td>Ask respondent to sign and acknowledge consent form</td>
<td></td>
</tr>
<tr>
<td>2) Ask Background questions</td>
<td></td>
</tr>
<tr>
<td>Confirm information about;</td>
<td></td>
</tr>
<tr>
<td>• Name</td>
<td></td>
</tr>
<tr>
<td>• Date of birth</td>
<td></td>
</tr>
<tr>
<td>• Nationality</td>
<td></td>
</tr>
<tr>
<td>• Level of study</td>
<td></td>
</tr>
<tr>
<td>3) <strong>Discuss about how did the incident take place</strong></td>
<td></td>
</tr>
<tr>
<td>• How did you find out that you were a victim of an ATM fraud?</td>
<td></td>
</tr>
<tr>
<td>• How did this experience make you feel?</td>
<td></td>
</tr>
<tr>
<td>• Are you aware of the term ATM Skimmers?</td>
<td></td>
</tr>
<tr>
<td>4) <strong>Discuss his or her relationship with their registered bank</strong></td>
<td></td>
</tr>
<tr>
<td>• Do you think it was your bank’s fault?</td>
<td></td>
</tr>
<tr>
<td>• Did the bank pay you back?</td>
<td></td>
</tr>
<tr>
<td>• Are you aware of the security precautions that you should take in order to protect your privacy?</td>
<td></td>
</tr>
</tbody>
</table>
### Appendix 3: Semi-Structured Interview of the Bank Security Officer:

<table>
<thead>
<tr>
<th>Order of semi structured Interview with the bank security officer</th>
<th>Discussed</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Ask respondent approval to use recording systems</td>
<td></td>
</tr>
<tr>
<td>Ask respondent to sign and acknowledge consent form</td>
<td></td>
</tr>
<tr>
<td>2) Ask Background questions</td>
<td></td>
</tr>
<tr>
<td>Confirm information about;</td>
<td></td>
</tr>
<tr>
<td>• name of the organisation</td>
<td></td>
</tr>
<tr>
<td>• respondents position</td>
<td></td>
</tr>
<tr>
<td>• years working for the organisation</td>
<td></td>
</tr>
<tr>
<td>• Level of study</td>
<td></td>
</tr>
<tr>
<td>3) Discuss about Experience and career goals:</td>
<td></td>
</tr>
<tr>
<td>• What are your career goals as a Bank security officer?</td>
<td></td>
</tr>
<tr>
<td>• What do you do if a customer lost his debit or credit card?</td>
<td></td>
</tr>
<tr>
<td>• Are you aware of the term ATM Skimmers?</td>
<td></td>
</tr>
<tr>
<td>• What do banks do when they realize one or more of their ATMs have been skimmed?</td>
<td></td>
</tr>
<tr>
<td>4) Discuss about the toughest challenges faced:</td>
<td></td>
</tr>
<tr>
<td>• What is the toughest problem you’ve had to face?</td>
<td></td>
</tr>
<tr>
<td>• How did you overcome it?</td>
<td></td>
</tr>
</tbody>
</table>