THESIS

Course code: BE309E

Candidate number: 18

Title:

Risk management of counterfeit cards fraud: An empirical study of challenges among South Asian financial institutions

Date: 22.05.2018

Total number of pages: 62

NORD University

www.nord.no

Risk management of counterfeit cards fraud: An empirical study of challenges among South Asian financial institutions

ABSTRACT

This thesis presents and discusses how does risk management handle challenges related to counterfeit cards fraud in a South Asian context. Based on our empirical findings, we show that there are heterogenous challenges related to counterfeit cards fraud which financial institutions face and handled through effective risk management. The major part of research today focuses on challenges to any business and our research contributes to identify 'three-levels of challenges' related to counterfeit cards fraud. The findings of the research shows handling of different levels of challenges on one hand and their handling through risk management on the other. We discuss the importance of macro-level challenges which call attention to be addressed by autonomous national and international bodies.

Keywords: Risk management; challenges, counterfeit cards, fraud handling, financial institutions

Table of Contents

1 Introduction 1

1.1 Background 1

1.2 Problem statement 4

1.3 Context of study 7

1.4 Significance of the study 8

2 Literature Review 9

2.1 Risk management - definition 9

2.2 Risk management and financial institutions 10

2.3 Risk management theories 10

2.3.1 Risk management process 11

2.3.2 Types of risk in financial institutions 12

2.3.3 Enterprise Risk Management (ERM) and Basel Accord 13

2.4 Cards fraud and rapid technological advancement 16

2.4.1 Counterfeit cards fraud 16

2.4.2 Europay MasterCard and Visa (EMV) technology 17

2.5 Challenges of financial fraud 17

3 Method 20

3.1 Philosophical foundation 21

3.2 Research design 21

3.3 Data collections and participants 22

3.4 Research phases and engagement 25

3.5 Data analysis 26

3.6 Validity and reliabilty 27

4 Findings 28

5 Discussion 44

6 Conclusion 47

7 References 50

8 Appendix 58

8.1 Interview guide 58

1 INTRODUCTION

1.1 Background and actualization

The overall objective of this thesis is to advance knowledge about internal risk management processes, and alternative fraud detection techniques implemented by the financial institutions, more specifically banks, to handle counterfeit cards fraud. Credit and debit cards are issued by the banks under the license of Cards associations, i.e. Visa Inc. and MasterCard Inc. Regulators and third-party solution providers try to mitigate fraudulent activities from the cards business with the help of new technology which is considered less-effective according to the significant losses reported so far. Banks need to develop alternative fraud detection techniques at their own to deal with significant risk. The first aim of this thesis is to make an effort towards theory development within the area of risk management, secondly, the contribution may help risk managers of the other financial institutions to have an insight about effective risk management tools, and techniques developed by the banks who succeed to mitigate counterfeit fraud losses in cards business.

Managing risk is one of the primary objectives of firms operating internationally (Ghoshal, 1987). Nonetheless, investing in international markets takes on additional risk, as well as provides tremendous opportunities to the investors as compare to when they invest in local markets. Advanced technology, communication and transportation push forward the investors to explore opportunities of international business. McNeil, Frey, and Embrechts (2015) suggest that in banking, the best-known type of risk is probably market risk and risk management is a discipline of living with the opportunities which are covered with adverse effects of uncertainties.

Credit institutions including banks operate both in local and international markets. A bank is a financial institution that accepts deposits and lends money into the markets. Nonetheless, banking has dramatically changed over the last forty years and technological advancement as well as market needs have revolutionized traditional banking into electronic banking, phone banking, debit and credit cards have replaced use of cash payments, and ATMs have substituted cash withdrawals from the bank counters (Williams, 2010, p.8). Today, banks are playing vital role in capital accumulation and economic growth of a country. Schumpeter (1912) emphasized a century ago on critical importance of the banking system for a dynamic economic growth through innovation and funding productive investments. Levine and Zervos (1998) argue that banking development is strongly and positively correlated with future rates of economic growth, productivity growth, and

capital accumulation in a market. However, this technological change and excessive use of paperless money adds massive risk to the credit institutions, its returns, and ultimately effects on economic growth. Banks can convert investments into high returns, and accelerate economic growth by mitigating risk (Bencivenga & Smith, 1991).

Plastic money, debit and credit cards, is the essence and a leading character of globalization. As a form of payment, these have symbolized the transactions effortless and make instant flow of money possible around the world (Rona-Tas & Guseva, 2014). E-commerce is playing an important role today in increase of revenue and growth of the businesses in local and international markets. Whether it is a grocery store or travelling abroad, almost everyone uses a debit or credit card for payment in developed countries (Freeman, 2001; Hayashi, 2006), now the trend has also shifted towards the developing countries and cashless environment is taking away the traditional currency notes out of the scope. Recent statistic shows that a total of 19.24 billion cards are circulated globally (Statista, 2016) and global non-cash payments volume has exceeded to 726.1 billion for 2014-15 with a growth exceeding 11% (WorldPayments, 2015). Most importantly, the risk factor cannot be neglected in such a huge non-cash payments volume particularly transactions made through debit and credit cards which involve greater risk.

Banks and financial institutions that issue and accept credit, debit, gift or fleet cards, have responsibility to identify, evaluate, and to mitigate risk and fraudulent activities. All payments of debit and credit card transactions are electronically transferred among member banks through Visa Inc. and MasterCard Inc. which are the global technology corporations and payment solution providers incorporated in United States. Banks are licensed by these payment solution providers to run cards business in the industry, so banks are not only regulated by the Central Bank of a country but are also monitored by Visa Inc. and MasterCard Inc. as a cards issuer and merchant acquiring bank.

Internationalization of credit and debit cards business opens new doors for the banks. A thorough insight and knowledge of cross-border markets can give banks higher returns on investments and competitive positioning in international markets like American Express (AMEX) cards (Finel-Honigman, 2015). In this fast-growing banking network, many banks internationalize their business to achieve their organizational goals. Johanson and Vahlne (1977) define internationalization as a process which is associated with acquisition, integration and utilization of

knowledge in international markets, and Luostarinen (1979) argues that internationalization always results in a massive growth. Nevertheless, the extended opportunities are bundled with associated risks and cards business is an unsecured lending by type (Epstein, 2008 p.55).

As per MasterCard Inc., credit and debit cards fraud can be classified into two major groups, first is "Card-Present Fraud" and second is "Card Not-Present Fraud" environment. The first category mainly includes, lost and stolen cards, counterfeit cards, account takeover, and never received or fraudulent applications. However, second category is comprised of email order/telephone order (MO/TO) and e-commerce related fraud transactions (MasterCard, 2014). This thesis will focus on "Counterfeit" cards fraud from category one as it gives gigantic losses to the banks. A counterfeit card is defined as a cloned, fake or bogus card which is impersonalized by a fraudster through illegal means and without authorization of the genuine cardholder (Domil, Pavel, Imbrescu, & Pavel, 2012). Counterfeiting of cards will be explained further in chapter 2 of this thesis.

Since rapid technological advancement has changed the consumer needs and shopping behavior over a few decades (Buhalis & Law, 2008), however, banks are also facing substantial financial losses in cards business around the world markets. Report shows that global losses of cards fraud have crossed $24.71 billion till end of 2016 and is projected to increase up to $32.82 billion till 2020 (NilsonReport, 2016).

Although, there are several theories and different approaches of risk management as an effective and fundamental process to operate any business (Banks & Dunn, 2004; Hopkin, 2017), however, this might be a big challenge for the banks operating locally and internationally to evaluate risk and to mitigate fraud on such a huge volume of daily card level transactions when the card loss figures are extremely high on one hand, and regulatory threats on the other.

The next sections of this chapter will focus on risk management importance for a business including banks along with current research gaps in the literature related to technological insecurities to the cards business, and lack of any specific prevention models and techniques to manage risk of counterfeit cards fraud. In addition, the purposed contribution from this thesis towards the current literature will be discussed.

1.2 Problem statement

There are many researches so far in the field of risk management which stress that risk management is a core function to manage the organizations efficiently, particularly those which operate in different continents, in different social, political and legal conditions, so the organizations have to develop specific tools to mitigate risk for survival and growth in international markets (Kot & Dragon, 2015). Moreover, Froot and Stein (1998) argue that banks must hedge the risks involved in business to offload any potential threats.

Study of existing literature shows that various approaches and set of definitions exist related to risk management, its techniques and different models. The focus of many debates has been importance of corporate risk management in international markets. For example, Kot and Dragon (2015) present models of business risk management in international energy companies and argue that Enterprise Risk Management (ERM) is a key system used by the businesses to manage risk in international volatile financial markets. Hou (2013) outlines forms of significant risks in international markets and argues that investment in international markets takes on additional risk as well as opportunities. However, both studies emphasize only on risk management importance and present different risk models which are not applicable in banks for cards business.

Financial institutions are studied from different perspectives in current literature, however, there are only few researches that emphasize on risk management in cards business. Nevertheless, these studies are either about risk management of credit cards with respect to delinquency where borrowers do not pay back their card loans to the issuing banks or the study is regarding credit card risk management models, card fraud types or development of risk management tools. The previous studies suggest that neural network based systems and supervised learning algorithms may help banks to reduce lost or stolen credit and debit cards loss (Ghosh & Reilly, 1994; Shen, Tong, & Deng, 2007), while other researchers suggest that financial institutions can reduce such losses with implementation of modified fisher discriminant analysis (Mahmoudi & Duman, 2015). However, it is worthwhile to mention here that these studies emphasize only on lost or stolen cards risk management and ignore counterfeit cards risk management which is worthwhile and primary focus of study in this thesis.

Similarly, some researchers conclude their study suggesting the different proactive measures to reduce card fraud losses by checking the card presenter's identification at point of sale (POS) before transacting the card (Downing Jr, Howard, Goodwin, & Geller, 2016). While another study reveals a manual review of cardholder's spending behavior from previous account level transactions history at bank level to minimize lost or stolen cards losses (Kültür & Çağlayan, 2017). However, these recent studies also lack any discussion about handling of counterfeit cards fraud.

Butaru et al. (2016) had origin of their study about risk management practices of six major banks in United States. The aim of their research was to identify common drivers of risk management based on which banks try to reduce credit cards delinquency that is one of the major concern for banks after 2007-2009 financial crisis. They stress that there is an imperative need of further research in other aspects of risk management in cards business.

Lăcrămioara and Mihai (2011) emphasize on credit card fraud types in their study and argue that new counterfeiting methods will emerge in near future which require further research and global attention to safeguard financial institutions from potential losses in international markets.

Meanwhile, theories developed so far in the field of risk management and banking explain risk management fundamentals, risk models, risk types according to different nature of businesses, and risk management processes. Similarly, technological theories provide an insight only about the technological developments like Europay MasterCard and Visa (EMV) micro-chip technology and its integration with credit and debit cards (Bhargav, 2014, p.12-14; Weber, 2016), however, existing knowledge neither provides any valid reasons about how this technology is still unable to stop counterfeit cards activity nor discusses any effective measures for the banks to avoid financial losses. Thus, existing knowledge lacks both, the shortcomings of new technology and prevention techniques or possible measures for the financial institutions.

Rapid growth in technological sector has introduced serious threats to the banks involved in cards business. Potential losses from the counterfeited cards have compelled banks to find any possible solutions to mitigate high risk because cards associations, Visa Inc. and MasterCard Inc., have shifted now the liability of counterfeit fraud loss on the cards issuing banks and to the merchant member banks who have not adopted the chip technology yet (VisaInc., 2016a). However, Gray and Ladig (2015) argue that this process involves extreme cost for banks around

the world to replace old point of sale (POS) terminals with new chip-technology based terminals at their merchant establishments.

Payment solution providers, Visa Inc., and MasterCard Inc. have designed many software, and risk management tools. Also, instructed financial institutions to comply with EMV (Europay, Mastercard and Visa) to embed and equip plastic cards with small computer chips for use in local and international markets, but unfortunately the counterfeiting of cards has dramatically increased despite of secure authentication of transactions. Perhaps, this would be true that Visa Inc. and MasterCard Inc. have been unable to mitigate risk and to prevent fraud transactions on their magnetic strip technology used for credit and debit cards. It also seems unfeasible for banks operating globally to replace all credit and debit cards with new EMV micro-chip technology if card associations decide to remove magnetic strip from the cards.

On the other side, would it be correct to say that EMV chip technology is safe and a permanent solution to stop counterfeit cards losses in local and international markets? Visa Inc. claims that after EMV technology in cards business, it is impossible to compromise data of any legitimate card to make a counterfeit card (VisaInc., 2016b), however, the recent quarterly report published by Visa Inc. shows that counterfeit fraud is dropped by 58% only on merchants who have completed the chip upgrade process (VisaInc., 2017). It clearly depicts that implementation of new technology has also not been successful enough to eliminate counterfeit losses from international markets. Nevertheless, MasterCard Inc. concedes that chip technology in the cards business helps to reduce counterfeit losses globally (MasterCard, 2017).

Thus, the theoretical knowledge about new technology is limited and partial. Also, study of existing literature demonstrates that there are many researches in risk management field which suggest risk management models for private firms and banking sector in international business and markets. However, only few researchers have particularly focused on cards industry to the extent of lost or stolen cards fraud but still there is a need to study about counterfeit cards fraud risk management and prevention techniques adopted by the financial institutions. Although, it is arguable that card associations have shifted fraud loss liability to the banks and risk management tools alongside technological shift adopted by these associations have been unable to protect its member banks from the counterfeit losses.

Since financial institutions operate cards business in both local and international markets while reported fraud loss figures are significantly high to book credit losses to their accounts, so will it be easier for the financial institutions to find proactive solutions at their own? How do they prevent themselves from counterfeit fraud losses? What resources and expertise are they applying to mitigate risk in the markets? Do they lose their market reputation and customers confidence in case of counterfeit fraud losses? How do they see the compliance of new chip technology in cards issuance and chip-enabled merchant terminals? All these questions helped me to construct the following main research question of my work to fulfill the research purpose:

How does risk management handle challenges related to counterfeit cards fraud in a South Asian context?

The term Financial Institution (FI) means, more specifically a bank in our study, that accepts deposits and lends money into the markets. Today, banks also offer credit and debit cards to its customers as the means of payment. A counterfeit card is defined as a cloned, fake or bogus card which is impersonalized by a fraudster through illegal means and without authorization of the genuine cardholder (Domil et al., 2012). A risk manager is a person who identify, analyze, minimize risk or threat to prevent an organization or a business from unforeseen losses (Hopkin, 2017, p. 92).

1.3 Context of study

Statistic shows that cards fraud losses have been exceeded from $24.71 billion worldwide at the end of 2016, it is projected that this figure will cross $32.82 billion till 2020 (NilsonReport, 2016). As per recent report, the most prevalent payment card fraud exists in Mexico where 56% of the cardholders affected during 2016, followed by Brazil at 49% and USA at 47%. Report continues to Asia Pacific will lead card losses figures in India, China and UAE. United states is the only country which is on the top three list during 2014-16 (ACIWorldwide, 2016; Wallethub, 2016).

In Asia Pacific, 10% to 15% of total fraud resulted from malpractices such as card skimming and counterfeiting of credit and debit cards (MasterCard, 2014). As per statistics, Pakistan has not

been reported in the list of countries where counterfeit fraud loss has been a dominating factor in last three years, however, its neighbor cross-border countries located in Asia Pacific region i.e. India and China had significant fraud losses during the period. Pakistan is a developing country and in few past years, growth in cashless payments has been observed due to shift in consumption of plastic money. Therefore, considering Pakistan as the context of study is interesting to focus on the research question constructed in this thesis that how the financial institutions in Pakistan are handling risk of counterfeit cards fraud being a developing country, whereas the other developed countries of the world like United States and Canada are facing the substantial losses in cards business (NilsonReport, 2016).

1.4 Significance of the study

The focus of this thesis is to study internal risk management processes and fraud detection models implemented in different financial institutions, specifically banks in this thesis, to handle counterfeit cards fraud. Risk management is an integral part of an organization. As stated in above sections of this thesis, the huge financial losses and insecurity of cards business force banks to acquire different risk management tools from cards associations or third-party solution providers which might have proven less-effective to handle risk and to attain desired results. Nonetheless, financial institutions may form a customized internal risk and fraud detection model. Kim and Vasarhelyi (2012) recommend, based on their study, that a detection model using fraud indicators could be helpful to detect potential risk in efficient identification of cyber fraud. This model varies from bank to bank and depends on size of the cards portfolio and volatility of a market.

Some researchers question in their study, whether the introduction of EMV chip technology could reduce credit and debit cards fraud and recommend that future research could test its validity in the markets (Gray & Ladig, 2015).

Study of this thesis is purposed to give more clear insight on the current research gaps in the literature and development of risk management theory with an emphasis on detection models and preventive measures adopted by the financial institutions to mitigate counterfeit cards fraud. This thesis may also help risk managers of the other financial institutions to have an insight about effective risk management tools, and techniques adopted by the banks to mitigate counterfeit fraud losses in cards business.

The work is organized as follows. The next chapter of this thesis will focus on different risk management theories, risk models, types of risk, counterfeit cards fraud and Europay MasterCard and Visa (EMV) technology.

2 LITERATURE REVIEW

2.1 Risk management – definition

Different scholars have defined the term risk and risk management in different ways. Since the eighteenth century, the concept of risk is mainly linked to the concept of unfavorable events. According to Smith (1776), the chance of gain is by every man more or less over-valued, and the chance of loss is by most men under-valued. Kot and Dragon (2015) define risk as any doubts or events which may have positive or negative impacts on a company's stability, its reputation, or may effect on achieving its strategic, financial and operational objectives.

According to Toakley (1989), risk management is a procedure to control the level of risk and to mitigate its effects. Other researchers argue that in banking, the best known type of risk is probably market risk and risk management is a discipline of living with the opportunities which are covered with adverse effects of uncertainties (McNeil et al., 2015). Another researcher argues that over the years, an approach to secrets associated with risk management in business has not changed. Thus, we should stick to the fundamental practices of risk management, but in relation to new situations and opportunities (Beans, 2010).

German scholar, Berg (2010) presents the most comprehensive and precise definition of risk management as a continuous, proactive and systematic process to understand, manage and communicate risk from an organization wide perspective.

Risk management is a vast field and a fundamental consideration for every business today. Researchers have studied risk management and its importance in different aspects of the business in most of the industries. All the theories are useful in certain context because various concepts provide an insight of risk management and its practical implementation in a business which enable organizations to minimize risk and uncertainties in the markets.

2.2 Risk management and financial institutions

According to Ritter (1991), financial institutions are defined as firms like commercial banks, savings banks, bank holding companies, or representing and providing financial services to the banks itself. Another study defines financial institutions as banks, credit card companies, insurance companies, and other institutions which collect funds from the public and invest in financial assets like deposits, loans, and bonds, rather than tangible property (Bagorogoza & Waal, 2010). In this thesis, financial institutions will be discussed as banks and credit card companies specifically.

Caouette, Altman, Narayanan, and Nimmo (2008) argue that market risk has affected financial institutions ever since markets are created, and techniques for managing market risk have undergone a rapid change. Other researchers stress that it is particularly important for the financial institutions to mitigate business risk and add value through information technology (Gheorghe, Nastase, Boldeanu, & Ofelia, 2009).

Nevertheless, banks offer various types of financial services and not only credit and debit cards. It elucidates that banks need different types of systems in minimizing risk according to the nature of its operations. Risk management models and resource capacity also vary from bank to bank in view of its business portfolio and geographical markets operations. Van Gestel and Baesens (2009) describe major reasons of conducting risk management in banking sector that the banks and banking activities have evolved significantly over the time. Another researcher argues that effectiveness of risk measurement in banks depends on efficient Management Information Systems (Raghavan, 2003).

It is evident from review of different studies in the literature that risk management plays a key role for financial institutions to minimize associated risks. Risk management is an integral part of a business that allows an organization to run its operations efficiently.

2.3 Risk management theories

In this section of the thesis, major theories of risk management including risk management process, types of risks, and different risk models are discussed thoroughly with respect to existing literature.

2.3.1 Risk management process

Risk management is a process of making decisions regarding risk and their subsequent implementation, and flows from risk estimation and risk evaluation (RoyalSociety, 1992, p.3). A study shows that risk management process consists of five steps including risk identification, risk analysis, risk evaluation, risk treatment, and risk control (Norrman & Jansson, 2004).

However, different studies discuss different risk management processes. Some researchers present three steps while others presented four steps risk management process (Boehm, 1991; Stoneburner, Goguen, & Feringa, 2002; Tummala & Schoenherr, 2011). The reason behind different processes is observed as researchers studied risk management processes for distinct fields of business and for different industries.

A recent study in the field of risk management argues that risk management is a continuous process in any organization and risk planning is the first stage of risk management process (Memari, 2016, p.16). This study focuses on risk management process in developing countries. The idea seems logical as if any business needs to implement risk management practices in an organization then planning would be the first step to mitigate risk efficiently. The scope of this thesis is also to study risk management practices adopted by financial institutions in a developing country i.e. Pakistan, so we outline here the below highlighted risk management process to study further in this thesis.

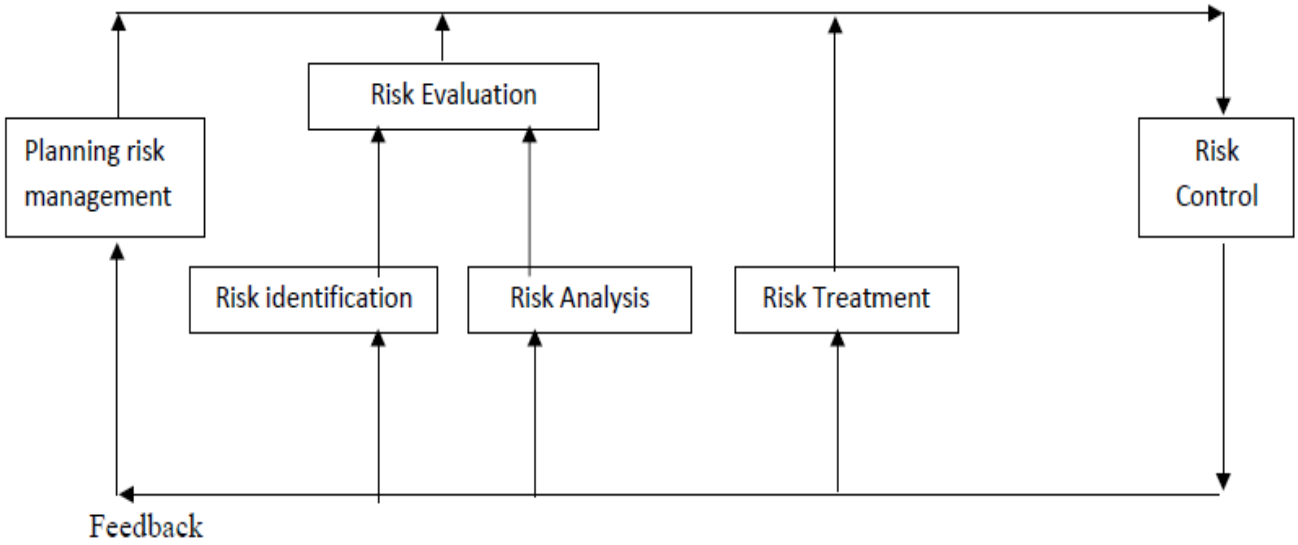


Figure 1. Risk Management Process in Developing Countries (Memari, 2016, p.16)

2.3.2 Types of risk in financial institutions

There are six main types of risk which can exist in banks or financial institutions. These can be classified as credit risk, interest rate risk, market risk, liquidity risk, operational risk, and foreign exchange risk. Other risk types may include settlement risk or performance risk. Bessis (2011) defines banking risks as the risks which may have adverse effects on profitability of several distinct sources of uncertainty. In other words, these risks may substantially influence the financial position of a bank. For better understanding of risks associated with cards business, this thesis will discuss each of these risks briefly.

Credit risk is defined as identification, monitoring and control and of risk which may arise from the possible default of consumer's repayments (Kithinji, 2010). Some other researchers suggest that credit risk is a potential loss which a bank can suffer where a borrower refuses to pay back partially or totally (Barnhill, Papapanagiotou, & Schumacher, 2002; Castro, 2013; Hawtrey & Liang, 2008).

Interest-rate risk is a risk of a decline in earnings due to the fluctuations in interest-rates. For example balance sheet items of a bank which cost or raise revenues which are interest driven (Bessis, 2011). On the other hand, MacDonald and Dowling (1993) suggest that interest rate risk is a gap between what financial institutions or banks pay to the depositors and what they charge to its borrowers.

Market risk has distinct definitions by many researchers. Most of them define market risk as loss arising due to adverse changes in market prices and rates, for example commodity price changes, or fluctuation in foreign currency exchange rates (Haneef et al., 2012; Orlitzky & Benjamin, 2001; Roulstone, 1999).

Liquidity risk is a core information about a bank of financial institution which is important to know by the customers and business partners before any deposits or investments. This shows financial soundness and positions of a bank for its inability to meet its contractual obligations (Garbade & Silber, 1979; Rahman & Banna, 2016).

Operational risk is defined as the risk of loss which may result from inefficient, failed or inadequate systems, internal processes, people or from external incidents (Chavez-Demoulin, Embrechts, & Nešlehová, 2006; Helbok & Wagner, 2006).

Foreign exchange risk refers to an exposure of a financial institution or a bank due to the potential impact of decrease in foreign exchange rates (Runo, 2013; Shachmurove, 2000).

These set of definitions gives us an insight that credit and debit cards risk may fall under operational risk or credit risk category, nonetheless, existing literature does not specify any type of risk in which counterfeit fraud loss may fall.

2.3.3 Enterprise Risk Management (ERM) and Basel Accord

Basel I or Basel Capital Accord is a regulatory framework for the banks which was initially released in 1988. It has two roles in banking industry, first role is to promote the capital stability of the banks in international markets and second is to provide fairness for competitions within the banks (Jackson et al., 1999). It also determines the bank's weighted-risk of assets and this could cover credit risk exposure of the bank. However, Basel I was criticized due to its simplicity and it lead to developments in 2004 as Basel II, which improved bank's ability to mitigate risk and control its trading activities (Lind, 2005, p.23-24). Nevertheless, financial crisis of 2007-08, stressed regulators for more tight controls on capital ratios and new criteria which could enable banks to mitigate liquidity as well as credit risks, so the final version as Basel III was released in 2009 (Feess & Hege, 2011).

Enterprise Risk Management (ERM) is a widely accepted framework which includes different methods and processes to mitigate enterprise wide risk. This framework also integrates internal control alongside risk management conceptual framework. There are a lot of studies related to ERM in existing literature. According to Liebenberg and Hoyt (2003), earlier this framework was fulfilling the needs of private firms only but now it has gained much attention of risk management professionals including banking sector. However, this framework is not able to widely support all functions of the banking industry like risk management of cards business due to complexity of process and huge number of account level transactions.

Many banks are using Enterprise Risk Management as a framework to manage risk in most of their operations. Today, banking is a versatile financial industry and different banks are providing different services to their customers besides conventional deposits and lending function.

Banking systems need constant developments in view of large product range and nature of operations. Highly designed IT based systems need to be installed by the banks according to their customized needs. At the same time, banks also require to be compliant with risk management processes and regulator's guidelines. Risk management involves more regulatory practices and stress internal control.

However, Enterprise Risk Management can analyze the potential information of a customer and may provide an instant picture of all data from other departments as and when required (Hopkin, 2017). But there are system limitations which can only manage and control risk internally. On the other hand, credit card transactions contain a large data on daily basis and only complex rules-based systems may identify risky transactions. Nonetheless, risk managers should have the in-depth knowledge of operational risk and must know the acceptable level of risk as decided by the banks.

Kot and Dragon (2015) argue that Enterprise Risk Management (ERM) cannot perform all of risk management jobs, however it functions as a bridge to provide further coordination within business and geographical structure of all activities being performed in the following model:

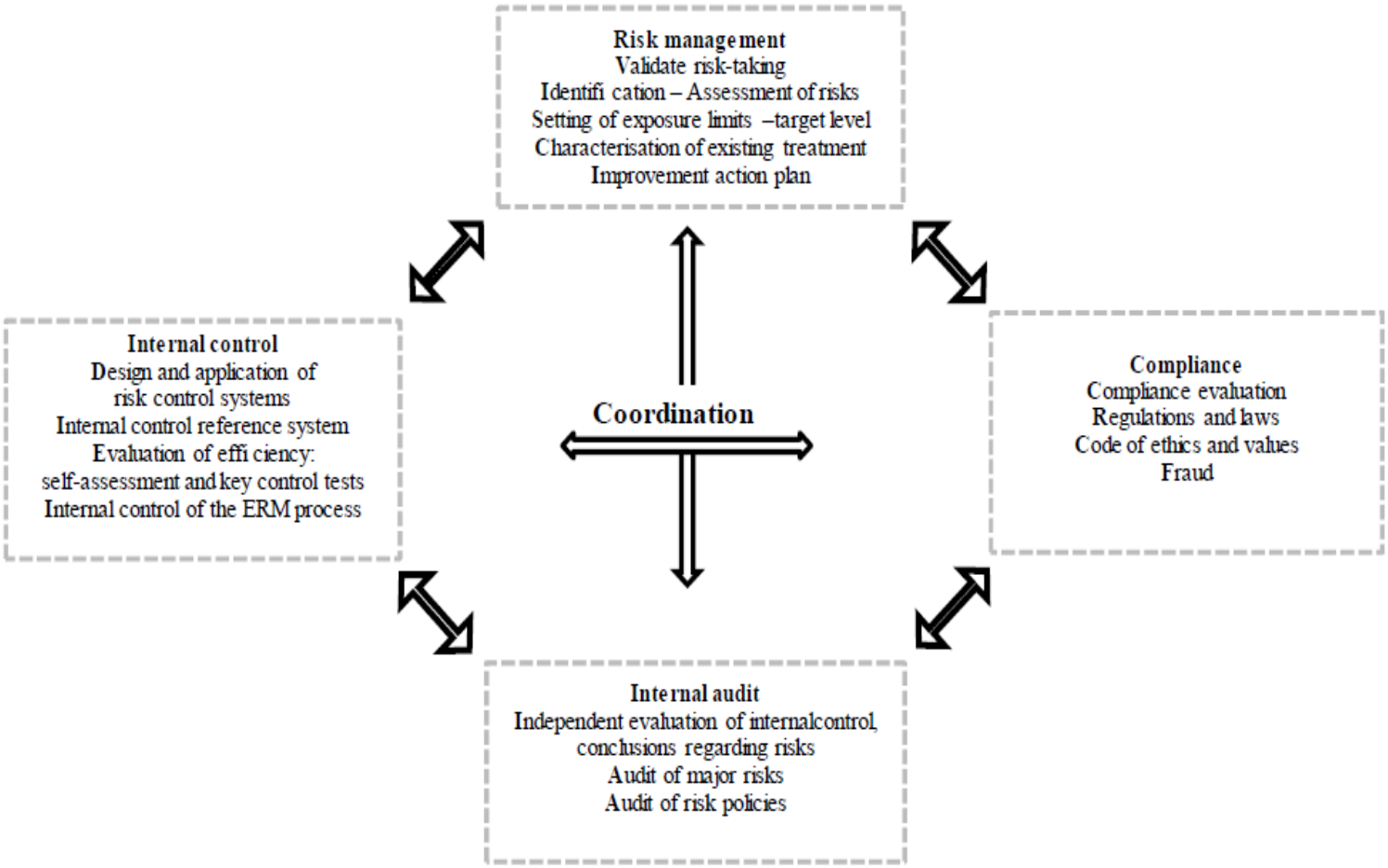


Figure 2. Enterprise Risk Management (ERM) and corporate governance (Kot & Dragon, 2015)

A study of current literature shows that researchers try to find different systems to manage risk involved in credit and debit cards fraud. Most of them suggest that neural network based systems and supervised learning algorithms may help banks to reduce lost or stolen cards loss (Ghosh & Reilly, 1994; Shen et al., 2007), while other researchers argue that financial institutions can reduce such losses with implementation of modified fisher discriminant analysis (Mahmoudi & Duman, 2015). However, it is worthwhile to mention here that these studies emphasize risk management only to the extent of lost and stolen cards and ignore counterfeit cards risk management which is primary focus of study in this thesis.

2.4 Cards fraud and rapid technological advancement

Types of credit and debit cards fraud have already been discussed in chapter 1.1 (Background description) of this thesis, as defined by cards association i.e. MasterCard Inc. In this section, we will discuss further about counterfeit cards fraud and EMV technology.

2.4.1 Counterfeit cards fraud

A credit or debit card is defined as an instrument that a bank issues to a natural or legal person according to a contract between them. The cardholder purchases goods or services from those (merchants) who accept the card without immediate payment of the goods. Payment is made from the account of the bank, who, afterwards, charges the cardholder at regular time intervals depending upon the terms of the contract and the situation (Ayub, 2007).

Counterfeiting a credit or debit card means to compromise and obtain secret information of a plastic card, and a valid pin code through illegal means in order to gain cash from ATMs, or to buy goods and services fraudulently in local and international markets. Financial institutions and payment solution providers including Visa Inc., and MasterCard Inc. are trying to control risk in cards business by proactive fraud and risk management tools, but unfortunately rapid technological advancement gives edge to the fraudsters in international markets.

As per Association of Certified Fraud Examiners (ACFE), counterfeiting is a cybercrime in which the modern technology allows the fraudsters to “skim” or copy the data of a credit or debit card from its magnetic strip through illegal means. Later, fake or cloned cards are generated by transferring the data. These fake cards can be a plain white plastic card or can also be an original look like card which fraudsters manufacture from scratch using the small embossing machines, high quality printers and smuggled holograms of card associations.

Counterfeit operations are normally observed in USA, Far East, Taiwan, China, and Hong Kong. However, California, USA is considered as the center of counterfeiting operations due to many active organized groups there. This all has been possible due to rapid technological growth, on the other hand embossers, tipping foil, computers, and magnetic strip read-write (MSRW) machines are common tools in the market. Counterfeit cards fraud is the most damaging fraud type in cards business (ACFE, 2011, p.1.1015).

2.4.2 Europay MasterCard and Visa (EMV) technology

All credit and debit cards were initially having only a magnetic strip on the back side of a card. This magnetic strip has secure information related to customer, bank and other details needed to complete a payment transaction electronically. Card associations, Visa Inc. and MasterCard Inc. are the major payment solution providers and technological firms who allow the banks around the world to run cards business. All payments are processed through these payment solution providers. However, in last few decades, there have been tremendous fraud losses in world markets due to counterfeit cards, on account of which banks and payments solution providers are compelled to find any solution to this great scam. The fraudsters compromise the data from original card's magnetic strip at targeted point of sale (POS) merchant terminals and subsequently make a fake copy of the card by transferring data into another card to transact it illegally somewhere in the world. This activity gave significant financial losses to the industry. As per recent report, this fraud loss has exceeded from $24.71 billion in last year and is projected to cross $ 32.82 billion till end of 2020 (NilsonReport, 2016).

Nevertheless, payment solution providers have now introduced Europay MasterCard and Visa (EMV) technology through which each and every transaction is processed at merchant establishment using a microchip imbedded on the card through one-time unique encrypted code. Besides this, cardholders have also to input a four-digits personal identification pin code while processing a transaction. The EMV specifications were firstly published in 1996 and since then this technology is being used for debit, credit and ATM transactions (Bhargav, 2014, p.12-14). However, the recent fraud trends show that even of the technological advancement in cards business, still the counterfeit fraud exists perhaps due to magnetic strip availability on cards.

2.5 Challenges of financial fraud

The importance of banking system in today's society is well-known and banks play a key role towards economic growth of a country. However, we cannot deny that if bank creates investment opportunities, on the other hand, it has so many challenges in handling of operations. These challenges do not only impact on operational activities of a bank but also provide substantial losses in some cases. Today, the banks are the main financial institutions accepting deposits and lending

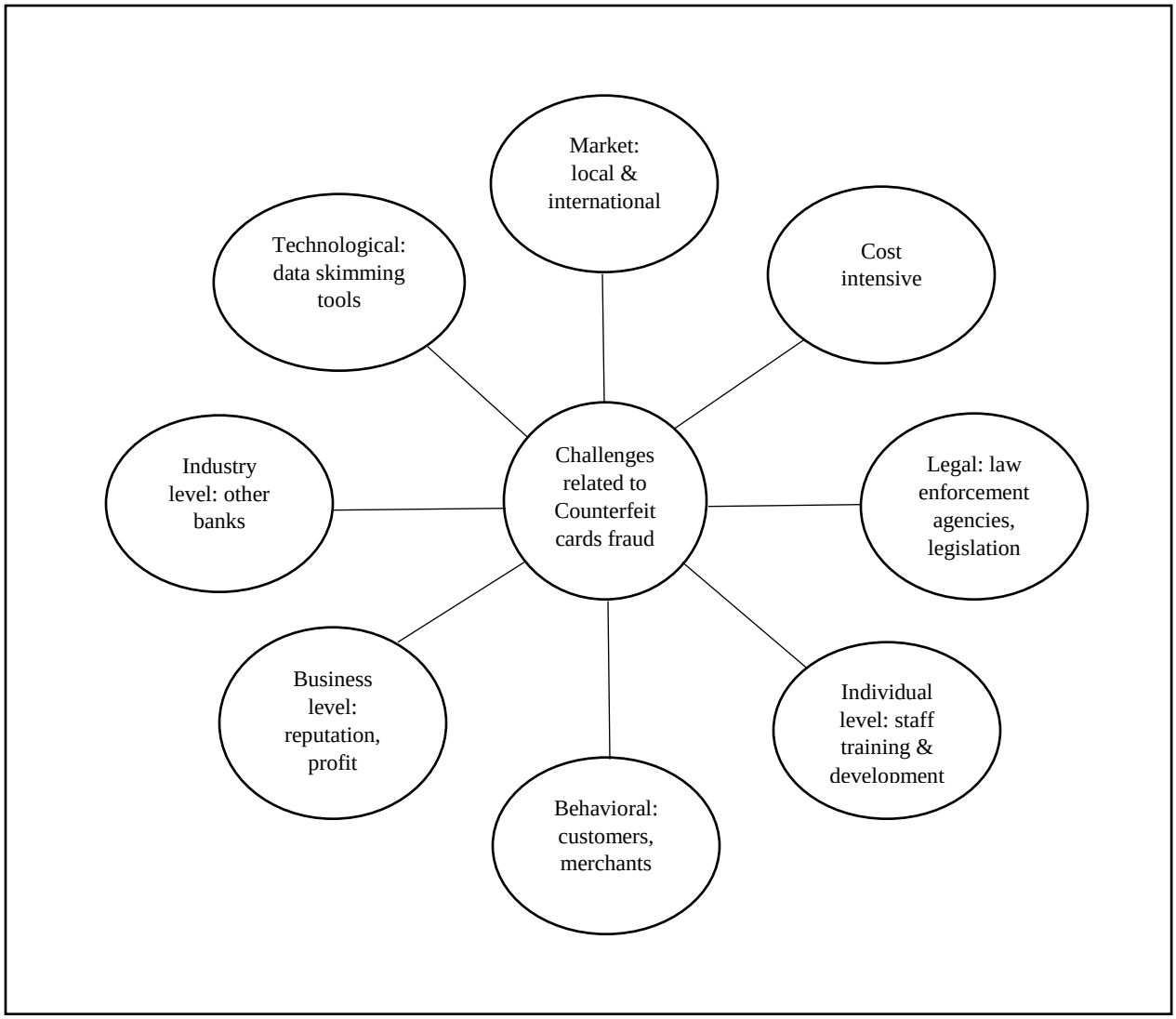
in a market. Banks have extended its services and product range to facilitate customers in different ways including consumer banking, corporate banking, and branchless banking.

Consumer banking offers direct services to the customers like credit and debit cards, and other consumer loans (Salehi & Rajabi, 2015). Nonetheless, providing credit and debit cards banks take additional risk and face many challenges within and outside the bank. As stated in chapter 1 of this thesis, banks can be classified as large-scale, medium-scale, and small-scale based on its liquidity ratio and total assets. Hence, challenges differ from bank to bank according to its size in the market. Not limited to but these challenges can be technological, legal, behavioral, market related, cost related, and business related, individual level, and industry level challenges.

Theoretical discussion has shown that many challenges exist there for a financial institution when there is any fraud on a customer's card and bank could not timely monitor and control it. It does not only impact on bank's reputation but also gives financial loss. and timely control the which impact on bank's reputation. Kent (1992) also explain different types of uncertainties to a business in his study of integrated risk management in international business, however, we argue that type of uncertainties presented by him apply to operations side of any business and do not particularly discuss any challenges with respect to cards business or counterfeit cards fraud.

We also argue that only few researchers have studies about credit cards frauds. Prior researches on cards business portray risk management either through reducing delinquency (Butaru et al., 2016), or by monitoring lost and stolen cards fraud through neural network based detection systems (Ghosh & Reilly, 1994; Kim & Vasarhelyi, 2012; Mahmoudi & Duman, 2015; Shen et al., 2007), or by checking card presenter's identification and transactions pattern (Downing Jr et al., 2016; Kültür & Çağlayan, 2017), however, no study exists related to challenges of counterfeit cards fraud and their risk handling. Thus, based on the existing information on challenges to the financial institutions and literature review, we construct below figure as challenges of financial fraud (see Figure 3) for further study.

Figure 3. Challenges of financial fraud



Van Grinsven (2010, p. 26) argues that an evident threat exists of overregulation to the financial institutions in the market. It is a big challenge for the financial institutions to handle extremely complex regulatory requirements to sustain its business.

On the credit and debit cards side, Sakharova (2012) argues that fraudsters today are organized professionals using Modern fraudsters are organized professionals using latest technology to compromise cardholders data and banks have a big threat due to development of new techniques. Another researcher argues that evolving technology and internet is filled with opportunities as well as challenges for the banks (Siau, Lim, & Shen, 2001).

Kaufman and Bliss (2008, p. 72) highlight legal system implications and argue that it is a big challenge for financial institutions because legal system does not necessarily work as needed and functions are not embedded for any individual. Madhava (2011) argues that new forms of cybercrime are challenging for the lawmakers, law enforcement agencies and the institutions. These studies clarify that new cyber-attacks are not only a challenge for a bank but also for the law enforcement agencies. Also, there can be lack of legal support from the authorities.

Sakharova (2012) argues about corrupted staff at merchant outlet that records a customer's data of a card by using an unauthorized device to manufacture the cloned card. It impacts on a bank's business relationship with the merchant also gives a loss for a fraudulent transaction.
Keep (2014) argues that staff training constitutes an influential signaling to encourage staff that they are valued to the organization and in return employer gets high level of staff commitment and motivation. However, this is a challenge now for the financial institutions to train and develop staff skillset.

According to Hull (2015, p. 568), the reputation of the financial institutions could suffer if the customer incurs any loss as result of the bank's product. Another researcher argues that payment card fraud affects consumer confidence. Similarly, in case of illegal activity on a customer's card damages reputations of the bank (Sakharova, 2012).

3 METHOD

The context of this study is risk management and fraud control techniques to handle counterfeit cards fraud, learned through the historic experience and practices developed and implemented by the risk managers of banks operating in Pakistan. This research relies on qualitative case study approach for data collection to fulfill purpose of this study as Baxter and Jack (2008) argue that "*when a case study approach is applied correctly, it becomes a valuable method for researchers to develop theory, evaluate programs, and develop interventions"*. Two types of data have been acquired for this study, primary and secondary data. Interviews and participant observations from banks operating in Pakistan are the main sources of primary data while banks' annual reports,

counterfeit cards-historic data, and documents much retrieved through online resources are part of the secondary data.***Philosophical foundation***

Easterby-Smith, Thorpe, and Jackson (2015, pp. 46-47) argue and elaborate three reasons emphasizing on importance of philosophical foundation. First, a researcher has an obligation to sense his reflexive role in research methods. Second, it provides more clarity to research design. Third, philosophical knowledge assists researchers to construct a meaningful outcome. In pursuant to philosophical assumptions given by Easterby-Smith et al. (2015, pp. 52-54), a positivist progresses research through hypothesis and statistically analyzes the large number of sampling, however, this paradigm is not that good for process, or theory generation, while social constructionist model is closely linked to the relativism, in which a researcher collects the views and experience of diverse individuals and observers to reveal the facts since a relativist argues that the truth does not exist outside of its contemporary context, however, it is created by the people. Crabtree and Miller (1999) argue that one of the key advantage of this approach is the close collaboration between researcher and the participants, enabling participants to share their experience and observations. Research question constructed in this thesis is purposed to study risk management of counterfeit cards which is based on views and experience of risk managers, therefore, research design of this thesis is framed on social constructionism paradigm to develop theory and process through experience and views of participants to fill the gap in current literature.

3.2 Research design

According to Yin (2014, p. 4), a case study approach should be considered when the focus of the study is to answer "how" and "why" questions to explain some present circumstances. He presents a twofold definition of case study research as following:

> "A case study is an empirical inquiry that (1) *investigates a contemporary phenomenon (the "case") in depth* and within its real-world context, *especially when* (2) *the boundaries between phenomenon and context may not be clearly evident*." (p. 16, emphasis added)

It is clear from the above definition that a researcher should adopt case study research design for an in-depth study with an assumption that the study is likely to involve important contextual conditions pertinent to his case. The case, in this thesis, consists of the phenomenon of decision-

making process of risk managers (handling risk), but a case could not be considered without the context, i.e. counterfeit cards fraud, and more specifically financial institutions (banks) in Pakistan. Besides this, the sampling of the research has been defined as small number of cases, therefore the chosen methodology is qualitative approach and a case study.

Banks are the cases here that issue or accept credit and debit cards and are involved in risk management of counterfeit cards fraud in Pakistan, while interview respondents are the units of analysis. Baxter and Jack (2008) argue that if a study contains more than a single case then a multiple-case study approach is required. According to Yin (2014), a multiple-case study enables a researcher to explore differences within and between cases which may provide similar or contrasting results to reach a conclusion. In this thesis, banks are the cases to identify different challenges related to counterfeit cards fraud and how the risk managers handle such challenges. We have selected 10 banks from Pakistan's banking industry based on criteria mentioned in next section of our study, therefore, multiple-case study approach is adopted in this thesis to develop theory through experience and observations of risk managers.

3.3 Data collection and participants

Marshall (1996) defines research sampling as a process of units selection from a population of interest and argues that sample for qualitative investigations tend to be a small number of cases. Purposeful sampling is the most commonly used sampling strategy in a case study approach in which selections of participants is based on a pre-defined criteria according to the research question and phenomenon of interest (Palinkas et al., 2015). Five criteria were applied when selecting participants for this study: they (a) are employed in a bank that issues or accepts credit or debit cards, (b) are working in Fraud and Risk Management unit, or Internal Control where account level transactions are monitored to minimize risk, (c) have position as risk manager or other relevant role with at least five or more years of risk management experience, (d) have insight into the processes, (e) are operating in Pakistan in order to discover patterns within a very limited targeted group due to time constraints, and to increase data comparability.

The epistemology of social constructionism suggests researchers to gather rich data from which ideas are induced (Easterby-Smith et al., 2015, p. 53), therefore, the interview approach is chosen as a suitable method of primary data collection in this thesis. DiCicco-Bloom and Crabtree (2006) suggest that in-depth interviews provide researchers a comprehensive information about the experiences of an individual. According to Kvale and Brinkmann (2009, p. 82), a qualitative research interview is an interview in which knowledge is produced socially to understand themes of the daily life from the subject's own perspectives during the interaction between interviewer and interviewee. It is clear from above definitions that data collection using interview method through experienced risk managers from the banking industry satisfies the study of this thesis.

Banks are recognized based on its market size. In this study, banks are the cases and a bank's market size can be determined from its liquidity position which means the ability of a bank to meet its financial obligations based on its total assets. However, our study is related to cards business, therefore, we have divided the selected banks from Pakistan banking industry into three groups based on total assets and total number of cards; banks with total assets of more than Rs.500 billion and with more than 300,000 cards portfolio are classified as 'Large banks', between more than Rs.150 billion and up to Rs.500 billion with more than 50,000 cards portfolio as 'Medium banks', and banks with total assets up to Rs.150 billion are considered as 'Small banks' in our study. Data about banks total assets and cards portfolio has been retrieved from online sources and the participants respectively.

The major portion of data was collected over a two-weeks period contacting and interviewing fraud and risk managers (see Table 1). Data collection was aimed to gather experience, observations, and strategies adopted by each individual bank which vary from organization to organization. Participants were contacted through email, phone, and made appointments to conduct face-to-face or telephonic interviews according to the participant's convenience.

Of the 10 informants, 5 were selected from the large banks, 2 from medium, and 3 from small banks to evaluate any heterogeneity of challenges and strategies in handling counterfeit cards fraud. In-depth interviews were carried out where informants were asked to share information

based on their experience and observations. Informants claimed that counterfeiting is itself a challenge for the banking industry today.

Table 1: List of participants

Name	Bank size	Place, Pakistan	Participant, role	Sex	Age	Years of experience
Bank 1	Large	Lahore	Country Head, Fraud & Risk Management Unit	M	42	17
Bank 2	Large	Lahore	Regional Manager, Fraud & Risk Management	M	45	20
Bank 3	Small	Lahore	Country Head, FRMU, OLA & Fraud Detections	M	44	18
Bank 4	Medium	Lahore	Manager Central, FRMU	M	35	9
Bank 5	Large	Lahore	Fraud In-charge, FRMU	M	38	15
Bank 6	Medium	Karachi	Regional Head South, Fraud & Risk Management	M	49	18
Bank 7	Large	Lahore	Manager Consumer FRMU	M	41	13
Bank 8	Large	Islamabad	Regional Manager North, FRMU	M	37	12
Bank 9	Small	Islamabad	Manager Fraud Investigations	M	36	12
Bank 10	Small	Islamabad	Manager QU, Central and North	M	41	16

*Years of experience includes participant's risk management experience only

Miles and Gilbert (2005) argue that a semi-structured interview gives a higher degree of freedom to the respondents to express their views in their own terms and allows interviewer a deeper understanding of an issue being researched. According to Easterby-Smith et al. (2015, p. 128), interviewer has an opportunity to develop secondary questions during interview to collect quality data. Therefore, semi-structured interview approach was chosen for this study with set of open questions which reduce the risk to affect participant's responses. Follow-up questions (what, how, why) and active listening techniques were applied during the interviews to collect quality data.

The interview guide consists of three set of questions (see Appendix A). The first part covers the background information of the participant to establish communication and a relaxed atmosphere to gather quality data. According to Kvale and Brinkmann (2009, p. 150), a researcher must develop an atmosphere where the participant feels comfortable to speak freely about personal experience and feelings. Thus, all interviews were conducted in a private room with only the researcher and the participant. Second part of the interview guide involves collecting core

information about the cards business and operating markets of the banks, and third part consists of set of questions related to the research topic. Half of the interviews were conducted in English and half were conducted in Urdu language according to the participants' convenience, however, were transcribed in English.

Since the interviewees have good insight of risk management, compliance, and internal control and requested not to disclose name of the bank and participant so the anonymity has been ensured at all levels of study and refer to the participant's list (see Table 1). However, permission was sought from the participants if could use their official title, background information, and role in the bank. The length of the interviews ranged from approx. 40 minutes to 1 hour and it was clearly stated that the information or data being collected will only be used for study purpose. Interviews were audio taped with permission of the participants.

3.4 Research phases and engagement

To study research question constructed in this thesis, research passed through the following phases (see Table 2). Eide and Kahn (2008) argue that a researcher should have dynamic engagement with participant during interview in order to discover and understand the phenomena in question. Therefore, active engagement of participants was ensured to gather clear insight, experience and observations to handle counterfeit cards fraud.

Table 2: Research phases and engagement

Research phase	Research engagement 2017-18
Pre-interview	Studying risk management, strategies, processes, frameworks, banks' risk management practices, laws and regulations, cards fraud, EMV technology; books, manuals, web (e.g. visa.com, mastercard.us, sbp.org.pk), 2017-18 Documents; (fraud manuals, guide to EMV chip technology, card acceptance guidelines for member banks and merchants), 2017-18 Statistics and reports of counterfeit fraud; (e.g. nilsonreport.com, statista.com, wallethub.com, worldpaymentsreport.com), 2017-18

	Articles and journals; (credit and debit cards fraud, risk management of cards, EMV chip embedded cards), 2017-18 Observations and informal conversations with country head fraud & risk (see table 1), 2017-18
Interviews 1	In-depth face-to-face interviews, 6 participants in Lahore, Pakistan, April 2018
Interviews 2	In-depth online/telephonic interviews, 4 participants in Karachi and Islamabad, Pakistan, April 2018
Post-interview	Analyzing the data, transcribing interviews, and findings with conclusion

3.5 Data analysis

We developed our pre-understanding to be able to interpret the data (Alvesson & Sköldberg, 2017, pp. 55-56) of the macro context; e.g. macro-economic factors, unemployment, law & order, cross-border challenges, the meso context; e.g. contextual intermediate factors, other banks, law enforcement agencies, and the micro context; e.g. within organization, individual level, customer level, behavioral. Finlay (2002) defines reflexivity as process by which a researcher reflects upon the data collection and interpretation process, further argues that all researchers should adopt a reflexive methodology for qualitative research.

The data was analyzed according to the meaning condensation framework (Kvale & Brinkmann, 2009, pp. 205-206) which signifies initial reading to achieve a sense of the part vs. the whole (contextualizing) and identifying meaning units relevant to the research question.

All interviews were thoroughly transcribed to begin process of data analysis. Transcribed interviews consists of 71 pages document and in first step of data analysis, each transcript was thoroughly reviewed to identify challenges and solutions from the participant's stated observations and experience. For this purpose, a total of 238 quotations were marked and were analyzed by moving back and forth between the data sources, data types, and the analytical levels. In second step, passages from highlighted transcripts were condensed into shorter statements to find 'meaning units', however, quotations are used in next chapter of this thesis for a more clear insight

of empirical findings. The data was also analyzed in a way to identify similar and contrasting patterns of the different respondents that seemed relevant to answer the research question.

3.6 Validity and reliability

This subsection includes the steps taken to increase the validity and reliability requirements demanded of a scientific research in this thesis while data collection and analyzing the data. To fulfil the purpose, various criteria are considered to ensure requirements. Inspired from Sandberg (2000) interpretative approach for understanding human competence, this thesis follows his validity and reliability criteria. The criteria, he used to justify interpretations were: communicative and pragmatic validity (Kvale, 1989, 1996) and reliability as interpretative awareness (Sandberg, 1994, 1995).

In order to achieve first criteria, i.e. communicative validity (1) purpose of the study and research question were clearly explained to the participants to establish initial understanding and to obtain their consent for the study (2) participants were asked open-ended questions to gather most comprehensive answers and follow-up questions were asked during the interview to seek further information and to interpret their answers. Pragmatic validity was achieved by: (1) observing the participants' reaction to our understanding of their answers in the interview (2) asking the participant to demonstrate practical examples about handling risk of counterfeit cards fraud, and (3) observing the participants' reaction to their answers.

Reliability as interpretative awareness was achieved by obtaining data in such a way in which participants conceive their risk management observations. More specifically (1) primarily asked what and how questions to feel participant free to focus on what handling risk of counterfeit cards fraud meant for them (2) initially treated all the statements of participants about their work as equally important to the study, and (3) asked many follow-up questions which are required the participants to interpret their statements more specifically.

Yin (2014, p. 48) argues about external validity, and emphasizes that findings can be generalized if a case study research question is to study "how" and "why" questions. The findings of this thesis

represent participants' views and experience in handling risk of counterfeit cards fraud with different risk management techniques and criteria-based systems, so the answers were different according to their own views and adopted techniques. Thus, the findings cannot be generalized fully, but can be used for a future study.

4 FINDINGS

The findings section is organized as follows: Table 3 is an overview of our findings and answers the research question; i.e. What challenges do financial institutions have related to counterfeit cards fraud and how do risk managers handle such challenges? During the interviews, we observe that financial institutions are facing challenges at three different levels i.e. within organization, within industry, and at national and international levels. Hence, we have divided challenges into three-levels of analysis i.e. micro, meso, and macro respectively.

First, macro-level challenges are presented and analyzed in view of its criticality because findings of this thesis reveal that risk managers in the industry face these macro-level challenges and have no solutions to encounter them. Autonomous local and international bodies should address the identified challenges which limit risk managers ability to handle counterfeit cards fraud. Second, meso, and micro-level challenges and their solutions are analyzed with respect to distinct strategies adopted by the risk managers in Pakistan banking industry. These two analysis answer the research question focusing on challenges and solutions to handle counterfeit cards fraud. Finally, discuss heterogenous challenges which are distinct among small-scale, medium-scale, and large-scale banks. It enables to discriminate internal and external challenges and controversies based on size of the bank.

Table 3: Findings overview

Context level	Challenges	Solutions

Macro context: macro-economic factors, unemployment, poverty, law & order, and cross-border challenges	- Online availability of data compromising tools - Migration of international fraudsters with latest fraud tools due to advance technology - Electronic travelling of compromised data internationally - Marketing of fraudulent tools - No access to mastermind fraudster in international markets - Economic decline and no foreign investments compel banks for cost-cutting - Hiding customer's name on slip by international banks hinders local banks to minimize risk - Laws are flexible and lack punitive actions - Law & order situation is not good - Weak prosecution and evidence systems - Legal system is corrupt - Fraudster involves in same crime once released - Specialized risk education lacks in country - Unemployment & poverty in country lead people to choose criminal act	**** Limitations of risk managers:*** - Challenges to be addressed by National and International autonomous bodies
Meso context: contextual intermediate factors, Industry related, other banks, law enforcement agencies, merchants	- Lack of support from law enforcement agencies - Law enforcers lack staff & technical knowledge - Coordination lacks among banks - Lack of merchants training & awareness - Counterfeiting is itself a challenge. Same industry, so all banks have similar challenges except cost & resources. - Fraudsters damage EMV-chip and transact counterfeit data from magnetic strip - Data compromising trend has shifted from international to local market - Compromising ATMs wearing mask - Existing risk management frameworks do not apply in cards business - Industry is non-compliant of EMV-chip technology - Threat of cards business license cancellation by regulators - Collusive other banks' merchants, deliberately involved in counterfeiting	- Extend coordination with law enforcers & share evidences & technical information - Extend coordination with other banks on Banking Association level - Regular trainings and fraud awareness to industry wide merchants - Observations, knowledge, and experience is shared at industry level to minimize risk - EMV compliance is mandatory at both level - Existing technology review is mandatory - Regular research at own level, and sharing information & knowledge - Surveillance with advanced tools - R&D Division should be established to develop new risk frameworks - Ensure EMV-chip compliance on issuing & acquiring both sides - Deactivate cards for international use unless customer needs it - Report incident, and termination of business relation with such merchant

Micro context: Within organization, individual level, behavioral, business level	- High cost is a barrier to EMV-chip compliance and acquisition of enhanced systems - Lack of system support - No source of knowledge about any technological advancement in international markets - Surveillance of ATMs is not up to the mark - Staff lacks analytical skills and training - Customer lacks fraud awareness - Threat of data skimming by internal staff - Lack of authority by the management - Risk of life threats due to risky nature of job - Organizational cost-cutting as a challenge - Threat of reputational loss and losing customer's relation - Opportunistic behavior of customer blaming bank and fear factor in filing a complaint - Lack of customer's interest in bank alerts - Lack of operations in remote cities	- Cost-benefit analysis are conducted and cost is absorbed to foresee betterment - Acquire latest tools & systems with change in fraud trends - Self-research on local & international market technological advancements - Surveillance with advanced tools - Internal & external staff training sessions - Customer must avail SMS alert - Internal control by IT level restrictions - Understanding of job requirements at top - Preference of duty overcomes fear - Budgeting for major requirements - Allow pre-credit and timely processing of case to avoid customer's annoyance - Provide fraud awareness to customers through marketing techniques - Immediately block suspicious cards and coordinate with branch to avoid loss

4.1 Macro-level challenges: unemployment, poverty, law & order, and cross-border challenges

Findings of this thesis show that there are various major challenges to the risk managers of the banking industry in Pakistan which belong to autonomous national and international bodies and limit the ability of risk managers to handle counterfeit cards fraud with no solutions at their end. Almost all stakeholders argue that rapid technological advancement in cards business has given an edge to the fraudsters. Now, marketing of fraudulent tools and online shopping opportunities of advanced data compromising devices at your doorstep from the international markets have made life of fraudsters very easy. Risk managers consider it as a big challenge and stated their inability to control or minimize this international market threat.

> It is very organized crime and there are big industries in international markets who are producing such tools and devices to skim data which is a worldwide phenomenon. if technology is being advanced to safeguard customers or our business portfolio on one hand, then fraudsters are also striving to break and compromise chip on the other hand. This would be a challenge for Cards Associations and the banks. (Respondent from Bank 2, large-scale, p. 15)

> Visa and MasterCard launched wave-technology in 2008 and they claimed that customers do not need to give card to anyone and just to wave their cards in front of merchant terminals so no chances of counterfeiting. However,

fraudsters have developed such (WIFI) devices which capture data while it is waved in front of merchant terminals and generate counterfeit cards. It's a big challenge […] As technology advances, so does the fraudsters advance counterfeiting tools. (Respondent from Bank 6, medium-scale, p. 44)

These quotes show that banking industry as well as card business regulators i.e. Visa Inc. and MasterCard Inc. are facing major threat of technological drawbacks. On the other hand, Visa Inc. claims that after EMV chip-technology in cards business, it is impossible to compromise data of any legitimate card to make a counterfeit card (VisaInc., 2016b) which is arguable.

According to the informants, international barriers also exist which are major challenges for them. These include mobility of international fraudsters to local market, electronic travelling of compromised data from local to international market within few hours, foreign banks' restriction on disclosing customer's name on sale receipt, and no access to mastermind fraudster located in international markets. Although, the informants argue that immediate steps should be taken by the national and international autonomous bodies since these are critical and highly affecting the industry.

Biggest challenge is cross-border data travelling from technology side. It means that compromised data travels cross-border in few hours with help of internet and counterfeit cards are generated in other countries and we cannot handle or take any action against it […] and counterfeit card generates and transact same day in any international markets including Europe, USA, […]. (Respondent from Bank 6, medium-scale, p. 44-45)

Recent, fraud wave came from Chinese fraudsters who brought latest technological skimming tools in Pakistan and were a great challenge for Pakistan's banking industry risk managers. (Respondent from Bank 10, small-scale, p. 69)

A major issue from the international markets like Europe and America is that when we retrieve receipt of charge (ROC) from international banks on a counterfeit reported case, there is no customer name on the receipt. So, we cannot authenticate whether it is a counterfeit case or not […]. (Respondent from Bank 7, large-scale, p. 53)

If any fraud gangs are burst in Pakistan; so the masterminds at their back in international markets are still active and we are unable to stop it. (Respondent from Bank 6, medium-scale, p. 45)

According to Schneier (2011), if the future is like the past, then a legal system that worked in past is likely to work in future. It means that time demands amendment in laws because purpose of an

organized crime is to make lot of money with a threat to any large-scale business. O'donnell (2004) stresses that rule of law is an essential pillar of an economy. However, risk managers find several legal challenges in handling of counterfeit cards fraud. Homogeneity has been observed in respondents' information that legal system is corrupt, and laws are flexible enough with lack of punitive actions, and weak prosecution and evidences system. For example, if a fraudster is caught during counterfeit fraud activity, he gets himself release and involves in same crime afterwards. Informants suggest legal deterrence and fear of strict legal actions must exist, however, this all is beyond their reach and with national authorities.

> Corruption is the key challenge of our country and it is not possible to stop counterfeiting as long as there is corruption. In few instances, we have observed that law enforcement agencies have escaped fraudsters against bribe. (Respondent from Bank 6, medium-scale, p. 45)

> […] recent fraud wave from Chinese fraudsters involved million dollars, however, a very short sentence and penalties were charged to them. This message in market boosts up and encourages fraudsters to continue counterfeit and skimming frauds since either they will be bailed out or will get nominal sentence if caught. (Respondent from Bank 10, small-scale, p. 69)

Unemployment rate, and inflation are major economic indicators of any country. Foreign Direct Investment (FDI) is only possible if the economic conditions of any country are sustained. Buffie (1993) determined the impact of foreign direct investment on unemployment and inflation and argued that it is an important economic factor. Informants find major macro-level challenges i.e. growing unemployment, lack of foreign direct investments, and economic decline which cause people to find new ways to earn easy-money, thus, they involve in counterfeit cards fraud.

> […] this is a white-collar crime in which educated people are involved to earn easy money. Unemployment is a big challenge, which leads the educated people to do this organized crime to make money. The people with extreme intelligence keep extreme evil minds. (Respondent from Bank 3, small-scale, p. 24)

> Unfortunately, Pakistan is going towards economic decline. Banks do not have foreign investments, that's why, banks are not in position to adopt this […] activity. (Respondent from Bank 6, medium-scale, p. 47)

These quotes show that several macro-level challenges are being faced by risk managers in the industry due to economic conditions which eventually leads to poverty and people then involve in

illegal skimming activity as it might attract them to make large money overnight. Homogeneity exists to a common challenge to all of the banks according to the informants, that there is lack of skilled risk professionals in the industry because no educational institution offers risk management education related to consumer banking.

> There is no specialized education or program at institutional level which could enhance skills and knowledge of the people about consumer banking. We have a challenge to train our staff and to upgrade them with latest fraud trends and how to minimize risk of counterfeit cards. (Respondent from Bank 1, large-scale, p. 7)

What informants argue is the need of immediate intervention of national and international autonomous bodies and to bring effective reforms to address these macro-level challenges that risk managers are encountering in their day-to-day operations in handling of counterfeit cards fraud. Data of this study shows that macro-level challenges are critical for banking industry and are beyond of risk managers ability to handle them directly.

4.2 Meso-level challenges: contextual intermediate factors, Industry related, other banks, law enforcement agencies

Informants find a market related challenge that they feel is a big challenge for the industry now-a-days. They are encountering change in data compromising fraud trend. According to the findings, earlier 'target-market' was only international markets for data compromising when local banks' cards were transacted internationally by the customers, however, today 'target-market' is Pakistan and data compromising threat is greater on ATMs than point of sale merchant outlets. Controversy exists in cross-case study analysis as one risk manager states that this trend is equally in both local and international markets, on the other hand, another informant says that this activity is greater on local markets ATMs only.

> If we see historic incidents of counterfeit cases, our cards data was earlier compromised in international markets and as an acquirer, international banks compromised cards were being transacted on our local merchant outlets and ATMs. However, now the trend has been changed and due to advance technology and ease to fraudsters, data is also

being compromised in local markets, […], the challenges are equally in both local and international markets. (Respondent from Bank 1, large-scale, p. 8)

Accordingly another risk manager states change in fraudster's modus operandi that:

Law enforcement agencies do not have any tool if a fraudster visits an ATM at 3 O'clock in the morning wearing a mask, then law enforcement agency and a risk manager will have a major challenge to identify fraudster. (Respondent from Bank 9, small-scale, p. 64)

This quote shows that the banks and the law enforcement agencies may be able to initiate their investigating inquiry in case if they could have a fraudster's identity, however, CCTV coverage is also of no use because fraudsters are wearing a mask to hide their identity.

Nonetheless, homogeneity exists towards the solutions of this ATMs data compromising challenge. Informants from different banks state strategies to handle it as:

Only solution we can do is to early detect any uneven activity and block the cards […] As a solution it need immediate action when data is being compromised at ATMs with active surveillance rather than we wait to identify later after occurrence of loss. (Respondent from Bank 6, medium-scale, p. 44-45)

[…] on the ATMs side, where fraudsters implant skimming devices and compromise customers data; we, as a solution, have installed anti-skimming devices on more than 95% ATMs to secure our business side and will hopefully complete this activity in a month or so…. (Respondent from Bank 2, large-scale, p. 13)

The results show that risk managers have several major challenges on the industry-level. First, all informants find a common major challenge of EMV-chip technology compliance which may lead banks to the cancellation of their cards business license. According to the risk managers from large-scale to small-scale banks:

The main challenge for the entire banking industry of Pakistan is 'magnetic strip'. Even If you comply EMV on your cards issuance side, it will not benefit unless all merchants in world are chip-enabled. (Respondent from Bank 3, small-scale, p. 22)

This quote describes that counterfeiting is itself a challenge and according to the information by respondents of the study, the whole industry is in non-compliance of EMV chip-technology. Only

few large-banks are partially-compliant to this, means have adopted on credit cards side but lacks on debit cards side and merchant acquiring business.

Homogeneity exists towards the solution aspects of this major challenge; all risk managers agree that EMV compliance may drop counterfeit cards fraud in local and international markets, however, controversy exists on cards associations level since Visa Inc. claims that after EMV technology in cards business, it is impossible to compromise data of any legitimate card to make a counterfeit card (VisaInc., 2016b), however, the recent quarterly report published by Visa Inc. shows that counterfeit fraud is dropped by 58% only on merchants who have completed the chip upgrade process (VisaInc., 2017) which is acknowledgement to the informants' statement and Visa Inc. claim is arguable.

> Original solution is only EMV compliance […] unless all acquirers do not disable magnetic strip on their terminals, counterfeiting could never be dropped. (Respondent from Bank 6, medium-scale, p. 44-47)

> It will work only as a solution if all banks comply on issuance and acquiring side both simultaneously. (Respondent from Bank 3, small-scale, p. 23)

In argument of EMV-chip compliance and Visa Inc. claim, informants from large and medium-scale banks discuss a major challenge that how the fraudsters break into this technology:

> Unfortunately, chip-technology is not being used solely, chip is damaged intentionally and said card has counterfeit data of any other bank in its magnetic strip. When such card is inserted into terminal, system goes on fallback transaction using counterfeit data in strip which is a challenge now for the industry. (Respondent from Bank 6, medium-scale, p. 44)

The best solution to this challenge is periodic reviews of the existing technology to overcome any shortcomings, according to the informant.

Findings reveal another major challenge for the risk managers, though the banking industry operates with extensive capital and operations, however, there is no specific framework of risk management which could help risk managers to handle counterfeit cards fraud. Kot and Dragon

(2015) also argue that Enterprise Risk Management (ERM) framework cannot perform all of risk management jobs.

> ERM is our internal framework and provide regulations only to the extent of educate the bank customers. Basel Accord is an international standard and is used by our Risk Division to assure risk standards and making policies. However, do not specifically help to minimize counterfeiting. (Respondent from Bank 7, large-scale, p. 52)

As a solution, informants state that they handle risk of counterfeit cards based on their experience and market trends only since no specific framework is in place, however, stress on development of a risk framework which could enable them to decide their line of action:

> There should be analytical R&D for the development of specific frameworks in developing countries. (Respondent from Bank 3, small-scale, p. 23)

Operating in the same industry, risk managers find lack of coordination challenge with other banks. Informants state that all banks operating in cards business offer credit and debit cards and have ATMs for cash withdrawal, however, only large-scale banks deal in merchant acquiring side too as a business partner with sale terminals at merchant outlets. Since counterfeiting is a major market challenge and data is compromised on other banks' ATMs or merchant outlets as well, so they have a challenge of support and coordination from the other banks if any counterfeit scam is reported. In such cases, they do not have access to the other bank's ATM or merchant outlet so cannot investigate or take any proactive action directly. According to informants, usually the merchants are either not trained by the banks and lack awareness or a merchant is collusive and he or his staff purposely compromise data of cardholders to involve in counterfeiting.

> Other banks' merchants involved in counterfeiting are a challenge for us as we do not have direct access to them. We have encountered other banks' merchant's collusion in accepting counterfeit cards. (Respondent from Bank 2, large-scale, p. 17)

> Merchant level challenges are industry wide and not specifically to our bank. Training and awareness to merchants is extremely important which starts from building the business relation and on-going training process. If any counterfeit card is transacted on a merchant's terminal, so it is mostly due to merchant's negligence or self-involvement in fraud. (Respondent from Bank 1, large-scale, p. 8)

To address these two industry wide challenges, informants say that merchant-level challenges are more critical because only merchant is a person who can stop counterfeiting when a fake card is presented, so it is argued that banks need to provide awareness and regular train their merchants to minimize counterfeiting. In case a merchant is collusive, banks should terminate business relationship with such a merchant and report it to other banks in the industry as well.

> We correspond with other banks and report such merchant's activity based on our investigation and request them to take necessary action against merchant closing the business relation, so that we as an industry may collectively minimize counterfeit fraud. (Respondent from Bank 2, large-scale, p. 17)

> Only awareness is the most effective tool which can prevent banks, merchants, and customers to safeguard from counterfeit fraud in market. (Respondent from Bank 8, large-scale, p. 58)

> We coordinate with other banks through emails and notify their point of compromise and also discuss matter with other banks in PBA (Pakistan Banking Association) forum. (Respondent from Bank 3, small-scale, p. 25)

Banks cannot solely handle risk of counterfeit cards fraud. Role of law enforcement agencies in any society is quite distinct to enforce law and security assurance. Banks interact with law enforcement agencies for their intervention to take up the fraud cases for further investigations. Findings show that risk managers face challenges while dealing with law enforcement agencies that work with certain limitations and according to their own regulations. Informants state that there is lack of support from law enforcement agencies side, observe extensive delays on reported cases, and cybercrime circle of law enforcement agencies lacks staff and technological knowledge about counterfeit cards fraud:

> We do not get required support and coordination and lack desired results. Now-a-days, a new fraud trend is a challenge for us that when fraudsters compromise data of our cards on ATMs, in couple of hours, they generate counterfeit cards and transfer funds of our cardholders to other banks and withdraw cash in high volume. (Respondent from Bank 2, large-scale, p. 16)

> Law enforcement agencies lack staff, technology and have work pressures. (Respondent from Bank 5, large-scale, p. 38)

As a solution to these challenges, informants say that they try to extend their coordination with law enforcement agencies and share concrete information and evidences in support of a case. Also, risk managers provide technical knowledge about counterfeit cards and data compromising tools at their own.

4.3 Micro-level challenges: within organization, individual level, behavioral, business level

The micro-level perspective refers to the challenges that a bank or a risk manager has related to the internal infrastructure, staff, cardholders, its own business network, or a small group within the organization. The data show that risk managers face many challenges at micro-level that includes cost-related, technological infrastructure and systems, staff and cardholders' individual and behavioral-level, and business level challenges while handling the counterfeit cards fraud.

Findings show that the banks, at individual level, are compromising acquisition of systems and tools required for effective handling of counterfeit cards fraud. EMV-chip technology compliance is mandatory for each bank according to the regulations of cards associations i.e. Visa and MasterCard Inc. and State Bank of Pakistan (SBP, 2016, p. 7). Informants argue that shifting cards business on chip-technology is not simple as it is being considered. In order to this, the whole industry has to replace all issued credit and debit cards, on the other hand, all sale terminals at merchant outlets are to be replaced with new terminals, also all ATMs in banking industry is required to upgrade. All these activities are extremely cost-intensive and not feasible for the banks at individual level. Gray and Ladig (2015) also advocates it that this process involves extreme cost for banks around the world.

> After economic crisis of 2008, when you try to be cost beneficial you leave so many things on stake […] if banks discontinue magnetic strip on cards, they will lose business in market because every merchant is not EMV chip-enabled in local and international markets. (Respondent from Bank 3, small-scale, p. 22)

> Cost challenge is there because the banks involved in merchant acquiring business, have to shift to EMV enabled terminals which involve high cost. Similar, is with cards issuance business as the banks should discontinue old technology and to comply with new chip-based cards. (Respondent from Bank 1, large-scale, p. 9)

Homogeneity is observed about this cost perspective while interviewing with all of 10 informants, however, controversy exists related to size of the bank. Informant from a small bank argues that small-scale banks could adopt it due to small cards portfolio size and number of ATMs, nonetheless, for the large-scale banks it is not practical with extensive business portfolio and ATMs in the market.

> There are top five banks in Pakistan with extensive branch network and they have deployed so many merchant sale terminals in the market. If they go for compliance to EMV then they definitely have to absorb a high cost exposure which is not business permissible. (Respondent from Bank 10, small-scale, p. 69)

On the solutions perspective, an informant argues that banks should absorb this cost factor to equip latest tools and systems with change in market conditions to foresee better results:

> Cost-benefit analysis are made once you are engaged in cards business or launch any product. (Respondent from Bank 2, large-scale, p. 14)

According to the findings, risk managers have staff training and development challenges since, as stated in macro-level challenges, there are no educational institutions that offer risk management education related to consumer banking and this is a limitation for a risk manager at the time of hiring new staff. On the other side, the existing staff also lacks analytical skills to identify and handle counterfeit scams and understanding of market trends:

> […] staff's analytical skills should be developed enough and trained to identify and handle counterfeit transaction incidents and to take immediate actions. (Respondent from Bank 1, large-scale, p. 5)

> We have another challenge that branch staff is unable to identify compromising scams at ATMs due to lack of training. (Respondent from Bank 6, medium-scale, p. 45)

> We also have technological communication gap like if there is any advancement in Europe, we lack any information or knowledge source in Pakistan. (Respondent from Bank 7, large-scale, p. 52)

These quotes show that lack of skilled staff is major challenge for a risk manager. Also, in absence of an effective communication source, information about any latest development or markets could not reach to a risk manager. Informants state that to encounter this challenge, they need to assess

an applicant's capabilities before hiring and later train him what they have learnt from the market experience:

> The people who come to us for job, we select them on basis of their extra-ordinary sharpness cleverness and later train them based on our experience to give them mindset, skillset, and to improve their analytical skills. (Respondent from Bank 6, medium-scale, p. 46)

The results indicate that a bank has threat of reputational loss and losing customer relationship if any counterfeit incident is reported on a card. Informants say that a customer behaves opportunistically and holds bank accountable for any disputed transaction through a fake card. Sometimes, customer also refuses to file a complaint about fraud due to fear element. In such scenario, a bank does not only lose its market reputation but also customer relationship which eventually impacts on the bank's revenue.

> If there is any counterfeit transaction on a customer's card, he always held bank responsible although TV and media is actively newscasting counterfeiting scams on air after Chinese fraudsters attack. However, customer says that this problem is only with our bank's cards and bank staff is involved in this fraud. (Respondent from Bank 6, medium-scale, p. 46)

Another risk manager argues that it is a critical challenge since chain of customers may discontinue business relation with your bank leaving a mark about your bank in the market:

> Customer's confidence shakes when there is a counterfeit transaction incident. He sometimes stops business relationship with bank due to fear of financial loss which ultimately affects our business side and revenue. Also, such customer may leave mark of our bank to other customers which causes reputational loss. (Respondent from Bank 2, large-scale, p. 17)

In order to handle such challenges, informants say that customer retention is utmost preference for a bank to sustain its market operations. In order to avoid customer's annoyance, pre-fraud and post-fraud steps are taken. At first level, surveillance of ATMs and transactions monitoring strategies are adopted to minimize risk of counterfeiting. On the other hand, customer awareness is emphasized about counterfeit fraud by sending important guidelines to be cautious.

We provide awareness to customer to keep his card and data safe, normally a good customer adheres the guidelines and we also send leaflets to customer through our marketing campaigns […], be watchful if to use card on ATM, and to report any unusual activity. (Respondent from Bank 2, large-scale, p. 18)

Immediate upon confirmation of counterfeit fraud, we give permanent credit to customer and refer matter to respective authorities. (Respondent from Bank 6, medium-scale, p. 46)

This quote shows how a risk manager, as a bank, effectively handles the customer level challenges and safeguards banks reputation. However, informer also argues about the opportunistic behavior of the customer because card was in his possession and he should be vigilant enough at the time of any transaction ensuring the safe custody of card's data and his credentials. Informer also argues on customer's casual behavior that customers do not bother to read bank's SMS about cautions to avoid from counterfeit fraud.

In other micro-level challenges, findings show that a risk manager has data compromising threat from the internal staff, lacks authority by the management, and have life threat due to risky nature of job.

Internal fraud may happen when bank staff itself leaks and compromise cardholders' data and misuse cards, so this is another challenge. (Respondent from Bank 1, large-scale, p. 6)

This quote refers to organization level threat for a risk manager that data compromising threat is not only from external sources but also from internal sources i.e. staff working within the bank who can have direct or indirect access to the customer's cards data. If anyone try to understand the vulnerability of this threat as internal vs. external, then severity of internal threat is greater than external fraudster's data compromising attempt because external sources can skim data of few cards, however, internal sources could have ability to compromise bank level customers' data. In order to avoid this challenge, respondent says that we enforce IT level restrictions and apply strong controls.

It is observed during an interview that a risk manager may have an internal challenge from its senior management and that is lack of authority to handle counterfeit fraud. According to Waligo,

Clarke, and Hawkins (2012), stakeholders involvement is complex and underestimated, so the management intervention is necessary. An informant from a large-scale bank states that:

> A fraud and risk manager should have full support and authority from your senior management and directors to take immediate action against a fraud. (Respondent from Bank 8, large-scale, p. 60)

Results show that a risk manager has also a threat to his life due to risky nature of job. There is no doubt that a risk manager always attempts to minimize risk and occurrence of fraud incidents, therefore, his life could be in danger because he acts in a way which others do not like either within or outside the bank.

> Risk manager is always at risk because he deals with internal and external frauds simultaneously. We always face challenges and have life risks and threats. (Respondent from Bank 8, large-scale, p. 59)

This quote indicates that counterfeit cards fraud handling is quite risky since it is an organized crime and motive of the people is to earn easy money regardless of the consequences. According to the informants, educated people are involved in counterfeiting activity and people with extreme intelligence keep extreme evil minds and they can cross any limits.

> We must work with honesty and should have belief that you have certain years of age (life) and nobody can take your soul before. (Respondent from Bank 8, large-scale, p. 59)

4.4 Heterogeneous challenges: Distinct among large, medium, and small-scale banks

Results show that almost all of the banks have similar challenges in the industry while handling counterfeit cards fraud. Homogeneity exists in informants' statements about similar vs. dissimilar challenges in the market and findings reveal that all banks have similar challenges on macro-level as one of the informant states that:

> In industry, all risk managers are facing same challenges because it is same industry, […] so they are facing the same challenges due to counterfeit fraud. (Respondent from Bank 8, large-scale, p. 60)

However, slight controversies exist within meso and micro-level with respect to homogeneity of challenges based on size of the banks. According to data, informants say that large-scale banks have extra challenges, first, to train their merchants due to extensive deployment of sale terminals in the market, and second, related to area coverage in smaller cities. For example, if any counterfeit activity is observed on any merchant or ATM in smaller cities then a risk manager may have no access or limited access due to lack of operations. Same challenge of area coverage goes to medium-scale banks. However, small-scale banks face costing and staffing challenges because of limited resources.

> Other banks have challenges to train their merchants. On ATMs side, other banks have similar challenges as our bank has […]. (Respondent from Bank 7, large-scale, p. 54)

> Last years, we apprehended a group […] that was training other people about techniques on how to conduct fraud. It was very surprising for us as this activity was being conducted in a small remote city. So, we have challenges related to area coverage in remote cities. (Respondent from Bank 4, medium-scale, p. 30)

> All the banks have almost similar challenges; however, small or medium scale banks may face extra challenges due to costing and staffing. Large banks have area coverage issues, like we cannot operate in every city of the country […]. (Respondent from Bank 3, small-scale, p. 25)

Informants say that, as a risk manager, they solve these extensive merchants training and area coverage challenges in remote cities by regular training and fraud awareness to industry wide merchants and for the area coverage issue, they immediately block suspicious cards to avoid any further loss and coordinate with respective branch. However, small-scale banks keep facing staffing and costing related challenges because of limited resources. Beck and Demirguc-Kunt (2006) argue that cost is a major barrier in growth of small and medium sized enterprises (SMEs).

4.5 Risk handling process of counterfeit cards

Our findings indicate homogeneity in risk handling process followed by the banks to handle counterfeit cards fraud. Informants state that the first step is transactions monitoring by their staff to identify any suspicious activity on a card. In case of any suspicion, bank contacts with the

customer to confirm authenticity of the transaction. This is an on-going process and most of the large banks analyze transactions real-time, however, medium-scale, or small-scale monitors transactions on post approval basis according to their system support. In case a customer reports a dispute on any transaction, bank immediately blocks the card to avoid further loss and keep such accounts under monitoring to assess counterfeit fraud.

> We have 24/7 online authorization department that monitors suspicious transactions. […] we contact with customers over the phone to confirm authenticity of the transaction. […] secondly, we encourage our customers to avail bank's SMS alert facility for any transaction on credit or debit cards, so that we can take a corrective remedial action on timely basis. This is how, we are handling risk of counterfeit cards. (Respondent from Bank 2, large-scale, p. 13)

After assessment of fraud, informants say that bank initiates its initial investigation process to collect evidences and to identify point of data compromising and refers case to the law enforcement agencies for legal action.

> […] once it is established that it is a counterfeit case […], then we investigate the matter that how card data is compromised and identify point of compromise […] and take appropriate action to mitigate counterfeit fraud […]. (Respondent from Bank 4, medium-scale, p. 29)

This quote shows that once the counterfeit fraud is confirmed then bank collects evidences and finds the common point of sale where data of customer's card might have been compromised by illegal means. According to the informant such cases are reported to the law enforcers for the appropriate legal action for possible recovery efforts.

5 DISCUSSION

The purpose of this thesis is to how does risk management handle challenges related to counterfeit cards fraud in a South Asian context? We attempt to develop understanding of a risk management framework based on our findings. This thesis establishes its first contribution as 'Three-levels of challenges' i.e. macro, meso, and micro-levels for a financial institution related to counterfeit cards fraud, and second contribution is risk handling process for this type of fraud. From the study of

Pakistan banking industry's risk managers, it discuss that how these two contributions impact on consumer banking industry.

Prior researches on cards business portray risk management either through reducing delinquency (Butaru et al., 2016), or by monitoring lost and stolen cards fraud through neural network based detection systems (Ghosh & Reilly, 1994; Kim & Vasarhelyi, 2012; Mahmoudi & Duman, 2015; Shen et al., 2007), or by checking card presenter's identification and transactions pattern (Downing Jr et al., 2016; Kültür & Çağlayan, 2017), however, no study exists related to counterfeit cards fraud handling and challenges that a risk manager may have.

Only, Lăcrămioara and Mihai (2011) focus on credit card fraud types and argue that soon new counterfeiting methods will emerge and would require further research with global attention. However, their study does not discuss any challenges related to the counterfeit cards fraud. Based on our findings, we argue that there are several challenges which are distinct in nature from each other and one challenge can influence the other. Therefore, we expand challenges in three-levels i.e. macro, meso, and micro and argue that these level of challenges can influence one another.

Importantly, challenges in handling of counterfeit cards fraud greatly matter which impact on sustainability of a bank's cards business. Findings of this thesis show that a risk manager has heterogenous challenges on macro, meso, and micro-level. As a risk manager, he applies internal and external controls within and outside the organization, however, he can only handle challenges to the extent of micro and meso-level because macro-level challenges are beyond to his limit and hinder a bank in handling counterfeit cards fraud. These macro-level challenges are critical and only autonomous national and international bodies can address them. Thus, this research contributes 'Three-levels of challenges' presented in chapter 4 (see Table 3). Based on our findings, we argue that financial institutions should identify first the level of a challenge before handling a counterfeit card fraud.

Second contribution is risk handling process for counterfeit cards fraud. Findings show that there is no risk management framework that exist related to counterfeit cards fraud handling and the existing frameworks in literature i.e. Enterprise Risk Management (ERM) and Basel Accord provide only general regulations to the financial institutions related to enterprise-wide risk

management and operational level activities. Kot and Dragon (2015) also support this statement that Enterprise Risk Management (ERM) cannot perform all of risk management jobs, however it functions as a bridge to provide further coordination within business and geographical structure of the activities being performed.

Memari (2016, p.16) provides six-steps risk management process for the developing countries, as presented in chapter 2 (see Figure 1). However, we argue that this process does not apply for risk handling of counterfeit cards because our findings show that risk handling of this type of fraud involves a different process adopted by the financial institutions. First two steps belong to risk discipline when the fraud is not confirmed yet including suspicious transactions monitoring and confirmation through the customer, however, next three steps are post-fraud confirmation including fraud assessment, investigation, and legal action. Thus, based on the findings of this thesis, we contribute to provide a risk handling process for counterfeit cards fraud (see Figure 4). This process is constructed based on our findings of this study that how risk management handles challenges related to counterfeit cards fraud in a South Asian context. It is worth important to mention that risk managers implement different risk management strategies to handle micro and meso-level challenges.

Nonetheless, macro-level challenges could also not be neglected because these are critical and continuously impacting on the bank, industry, as well as economy. Thus, these challenges are considered as an important part of the contribution with respect to South Asian context 'Limitations of a risk manager' and are covered in 'Outside Arena' of the presented model. We argue that macro-level challenges hamper a risk managers ability to handle counterfeit cards fraud and must be handled by the autonomous national and international bodies. According to the (Figure 4), a risk manager handles micro and meso-level challenges between the 'Inside Arena' and 'Outside Arena' domain according to the nature of the challenge. Simultaneously, a risk manager follows risk handling process for counterfeit cards fraud. With change in the challenges-level for example from micro to meso, its handling also shifts from 'Inside Arena' to 'Outside Arena'.

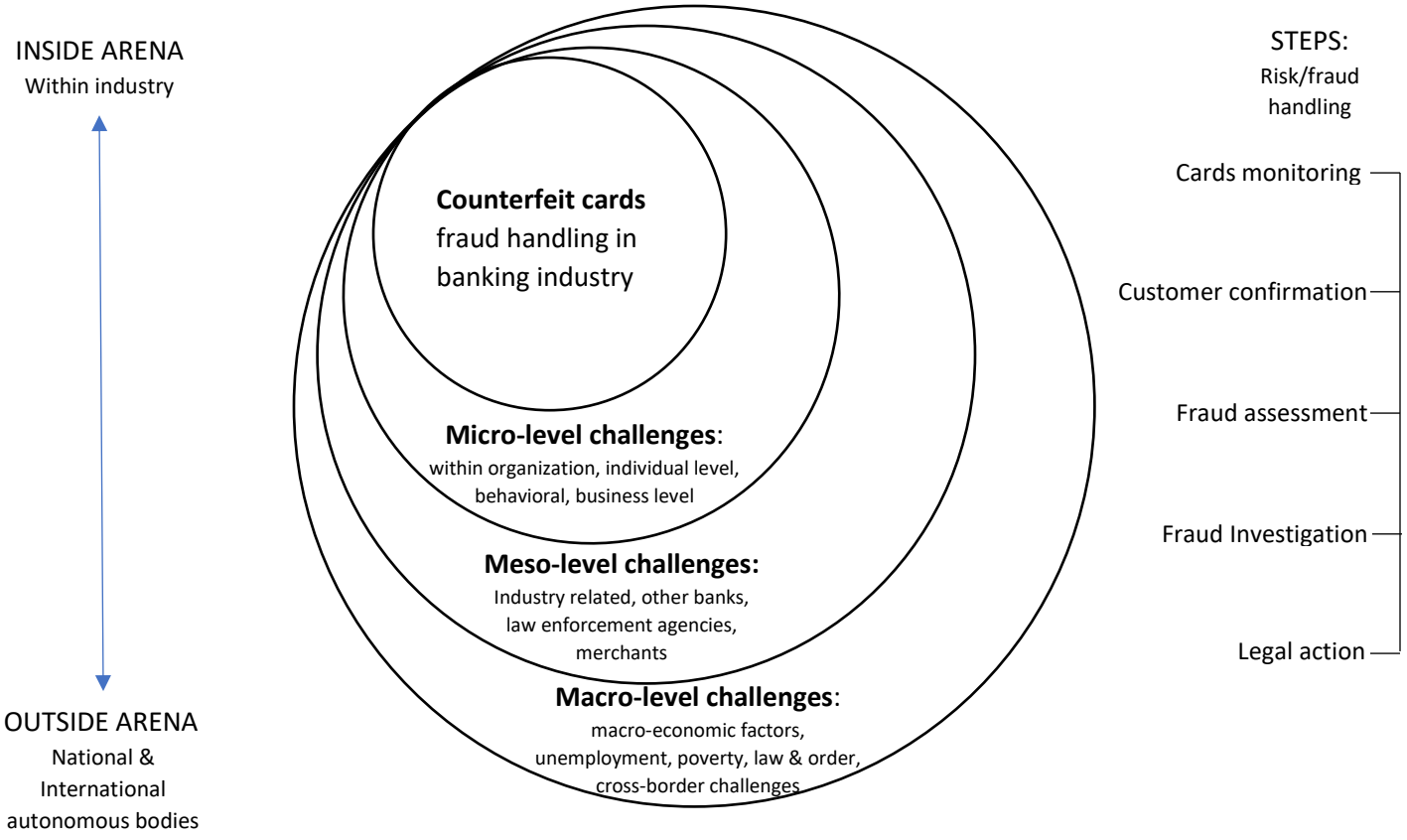


Figure 4. Three-levels of challenges & risk handling process for counterfeit cards fraud

This study offers new insights into the significance of the challenges related to counterfeit cards fraud and their handling through risk management. The third layer of macro-level challenges include shows highlighting responsibilities towards national and international bodies. What is at stake in a greater perspective, is not only the customer or a bank, but also involve macro indicators of a country.

6 CONCLUSION

The purpose of this thesis has been to develop understanding about how risk management handles challenges related to counterfeit cards fraud in a South Asian context. Thus, in a wider context we attempt to contribute heterogenous challenges in three-levels i.e. macro, meso, and micro and more

narrowly we attempt to contribute that what is at stake during risk management of these challenges. We have illustrated it through our empirical data from a South Asian context with a study of Pakistan's banking industry. Inquiry into this context has supported us to highlight challenges to financial institutions within the organization, within industry, and at national and international levels. (Figure 4) shows the three-levels of challenges and presents handling through risk management.

In our results, we identified macro-level challenges i.e. law & order, poverty, unemployment, and cross-border challenges which have the limitations for the financial institutions and cannot be handled through risk management. These are macro-economic factors and autonomous national and international bodies could develop policies to address those challenges, for more information about these challenges (see Table 3). This is why, we argue that an ignored, but a salient issue during risk management of such challenges calls attention to address. On the other hand, risk management handles the micro, and meso level challenges according to market practices, and risk management process presented in (Figure 4). However, few challenges in these two levels are also critical and require organization level as well as industry level attention. Our findings show that industry is not EMV chip-compliant on its cards business side which is considered so far as a secured tool to handle counterfeit cards fraud, so the industry is facing this challenge. Nevertheless, it is also important to understand the reason of industry's non-compliance which is high-cost factor for the banks to replace all their credit cards, merchant terminals, and upgrade of ATMs. Our results show that large-scale banks in the industry is greatly affected due to this challenge because they have extensive cards portfolio and branch network as compare to medium or small-scale banks.

The other key challenge for the industry is electronic transfer of their cards compromised by the fraudsters at a collusive merchant or compromised ATM. In our enquiries, we discovered that this is an alarming challenge for the banks because the compromised data is electronically transferred to international markets and risk management is so far unable to handle this challenge. Our findings also revealed that counterfeit cards fraud cases are referred to law enforcement agencies, however, the banks face challenge related to lack of support due to excessive number of cases already under

investigation with them. On the other hand, results show that law enforcement agencies are not technical enough to handle counterfeit fraud cases investigation.

The major issue which gives rise to counterfeit cards fraud is lack of awareness and training of merchants, customers, and branch level staff. In our empirical findings, it is discovered that financial institutions have behavioral challenges related to merchants and its customers because the provided guidelines and awareness is not taken as serious as it should be, on the other hand, security staff deputed at ATMs is not enough technical to identify if any fraudster comes to the ATM to install data compromising tools. However, risk management handling process and market practices are implemented by the banks to handle these challenges, nevertheless, we argue that these key challenges exist there and call much attention to minimize these challenges through risk management.

Our results show that risk managers have life threats due to risky nature of job while risk management of counterfeit cards fraud which is a critical challenge and require attention at individual and management level because people involved in such crime are attracted by easy money and can take any step at any level.

Our empirical findings also reveal solutions of heterogenous micro and meso-level challenges exercised by experienced risk managers to minimize challenges related to counterfeit cards, so we suggest that banking industry should identify first the level of a challenge through our presented model of ‘three-levels of challenges’ and attempt to handle challenges they face. Our emphasis here does not to suggest discontinue own practices but to adopt an effective risk management handling technique. We argue that these three levels of challenges influence on one another and our results, however, show that macro-level challenges handling is still to be addressed in a South Asian context with study of Pakistan, and there may be new challenges which banking industry may face in future at micro and meso-level, so we are giving direction to future research on it.

Acronyms

ACFE	Association of Certified Fraud Examiners
EMV	Europay, MasterCard and Visa
ERM	Enterprise Risk Management
FIs	Financial Institution(s)
PBA	Pakistan Banking Association
ROC	Receipt of Charge
SBP	State Bank of Pakistan

7 REFERENCES

ACFE. (2011, p.1.1015). FRAUD EXAMINERS MANUAL: INTERNATIONAL EDITION.

ACIWorldwide. (2016). Payment Card Security and the Arrival of EMV. *2016 Global Fraud Survey*.

Alvesson, M., & Sköldberg, K. (2017). *Reflexive Methodology: New Vistas for Qualitative Research*: SAGE Publications.

Ayub, M. (2007). *Understanding islamic finance: az keuangan syariah*: PT Gramedia Pustaka Utama.

Bagorogoza, J., & Waal, A. d. (2010). The role of knowledge management in creating and sustaining high performance organisations: The case of financial institutions in Uganda. *World Journal of Entrepreneurship, Management and Sustainable Development, 6*(4), 307-324. doi:10.1108/20425961201000023

Banks, E., & Dunn, R. (2004). *Practical risk management: an executive guide to avoiding surprises and losses*: John Wiley & Sons.

Barnhill, T. M., Papapanagiotou, P., & Schumacher, L. (2002). Measuring integrated market and credit risk in bank portfolios: An application to a set of hypothetical banks operating in South Africa. *Financial Markets, Institutions & Instruments, 11*(5), 401-443.

Baxter, P., & Jack, S. (2008). Qualitative case study methodology: Study design and implementation for novice researchers. *The qualitative report, 13*(4), 544-559.

Beans, K. M. (2010). Risk management after crisis. *The Journal of Enterprise Management*, 1-24.

Beck, T., & Demirguc-Kunt, A. (2006). Small and medium-size enterprises: Access to finance as a growth constraint. *Journal of Banking and Finance, 30*(11), 2931-2943. doi:10.1016/j.jbankfin.2006.05.009

Bencivenga, V. R., & Smith, B. D. (1991). Financial intermediation and endogenous growth. *The Review of Economic Studies, 58*(2), 195-209.

Berg, H.-P. (2010). Risk management: procedures, methods and experiences. *Risk Management, 1*(17), 79-95.

Bessis, J. (2011). *Risk management in banking*: John Wiley & Sons.

Bhargav, A. (2014, p.12-14). *PCI compliance : the definitive guide*

Boehm, B. W. (1991). Software risk management: principles and practices. *IEEE software, 8*(1), 32-41.

Buffie, E. (1993). *Direct Foreign Investment, Crowding Out, and Underemployment in the Dualistic Economy* (Vol. 45).

Buhalis, D., & Law, R. (2008). Progress in information technology and tourism management: 20 years on and 10 years after the Internet—The state of eTourism research. *Tourism management, 29*(4), 609-623.

Butaru, F., Chen, Q., Clark, B., Das, S., Lo, A. W., & Siddique, A. (2016). Risk and risk management in the credit card industry. *Journal of Banking & Finance, 72*(Supplement C), 218-239. doi:https://doi.org/10.1016/j.jbankfin.2016.07.015

Caouette, J. B., Altman, E. I., Narayanan, P., & Nimmo, R. (2008). *Managing Credit Risk : The Great Challenge for Global Financial Markets* (2nd ed. ed. Vol. v.401). Chichester: Wiley.

Castro, V. (2013). Macroeconomic determinants of the credit risk in the banking system: The case of the GIPSI. *Economic Modelling, 31*, 672-683.

Chavez-Demoulin, V., Embrechts, P., & Nešlehová, J. (2006). Quantitative models for operational risk: extremes, dependence and aggregation. *Journal of Banking & Finance, 30*(10), 2635-2658.

Crabtree, B. F., & Miller, W. L. (1999). *Doing qualitative research*: sage publications.

DiCicco-Bloom, B., & Crabtree, B. F. (2006). The qualitative research interview. *Medical education, 40*(4), 314-321.

Domil, A. E., Pavel, C. D., Imbrescu, C. M., & Pavel, C. (2012). RISK MANAGEMENT AND PREVENTION OF FRAUD IN CARD TRANSACTIONS. *Anale. Seria Ştiinţe Economice. Timişoara*(XVIII), 551-556.

Downing Jr, C., Howard, E. H., Goodwin, C., & Geller, E. S. (2016). Preventing the threat of credit-card fraud: Factors influencing cashiers' identification-checking behavior. *Journal of prevention & intervention in the community, 44*(3), 177-185.

Easterby-Smith, M., Thorpe, R., & Jackson, P. R. (2015). *Management and business research* (5th ed. ed.). Los Angeles: Sage.

Eide, P., & Kahn, D. (2008). Ethical issues in the qualitative researcher—participant relationship. *Nursing ethics, 15*(2), 199-207.

Epstein, L. (2008 p.55). *Surviving a layoff: A week-by-week guide to getting your life back together*: Simon and Schuster.

Feess, E., & Hege, U. (2011). The Basel Accord and the value of bank differentiation. *Review of Finance, 16*(4), 1043-1092.

Finel-Honigman, I. (2015). *International Banking for a New Century*. Florence: Florence, US: Taylor and Francis.

Finlay, L. (2002). "Outing" the researcher: The provenance, process, and practice of reflexivity. *Qualitative health research, 12*(4), 531-545.

Freeman, L. (2001). Paper, Plastic Or More Plastic: Debit Cards Continue To Gain Ground Among Consumers, But Some Old Payment Habits Die Hard.(Brief Article). *Credit Union Journal, 5*(19), 1.

Froot, K. A., & Stein, J. C. (1998). Risk management, capital budgeting, and capital structure policy for financial institutions: an integrated approach. *Journal of financial economics, 47*(1), 55-82.

Garbade, K. D., & Silber, W. L. (1979). Structural organization of secondary markets: Clearing frequency, dealer activity and liquidity risk. *The journal of finance, 34*(3), 577-593.

Gheorghe, M., Nastase, P., Boldeanu, D., & Ofelia, A. (2009). IT governance in Romania: A case study. *Global Economy Journal, 9*(1).

Ghosh, S., & Reilly, D. L. (1994). *Credit card fraud detection with a neural-network.* Paper presented at the System Sciences, 1994. Proceedings of the Twenty-Seventh Hawaii International Conference on.

Ghoshal, S. (1987). Global strategy: An organizing framework. *Strategic Management Journal, 8*(5), 425-440. doi:10.1002/smj.4250080503

Gray, D., & Ladig, J. (2015). The implementation of EMV chip card technology to improve cyber security accelerates in the US following target corporation's data breach. *International Journal of Business Administration, 6*(2), 60.

Haneef, S., Riaz, T., Ramzan, M., Rana, M. A., Hafiz, M. I., & Karim, Y. (2012). Impact of risk management on non-performing loans and profitability of banking sector of Pakistan. *International Journal of Business and Social Science, 3*(7).

Hawtrey, K., & Liang, H. (2008). Bank interest margins in OECD countries. *The North American Journal of Economics and Finance, 19*(3), 249-260.

Hayashi, Y. (2006). In Japan, banks and consumers turn to plastic; lenders seek new growth areas as traditional business declines; swapping cash for credit cards (Vol. 0, pp. C1).

Helbok, G., & Wagner, C. (2006). Determinants of operational risk reporting in the banking industry.

Hopkin, P. (2017). *Fundamentals of risk management: understanding, evaluating and implementing effective risk management*: Kogan Page Publishers.

Hou, X. (2013). Risk Management in International Business. *Risk Management*(27).

Hull, J. (2015). *Risk management and financial institutions* Wiley Finance,

Jackson, P., Furfine, C., Groeneveld, H., Hancock, D., Jones, D., Perraudin, W., . . . Yoneyama, M. (1999). *Capital requirements and bank behaviour: the impact of the Basle Accord*: Bank for International Settlements Basel.

Johanson, J., & Vahlne, J.-E. (1977). The internationalization process of the firm-a model of knowledge development and increasing foreign market commitments. *Journal of International Business Studies*, 23-32.

Kaufman, G., & Bliss, R. (2008). *Financial Institutions and Markets: Current Issues in Financial Markets*: Palgrave Macmillan US.

Keep, E. (2014). *Corporate training strategies: the vital component?. New Perspectives, 109-125*.

Kent, D. M. (1992). A Framework for Integrated Risk Management in International Business. *Journal of International Business Studies, 23*(2), 311. doi:10.1057/palgrave.jibs.8490270

Kim, Y., & Vasarhelyi, M. A. (2012). A model to detect potentially fraudulent/abnormal wires of an insurance company: An unsupervised rule-based approach. *Journal of Emerging Technologies in Accounting, 9*(1), 95-110.

Kithinji, A. M. (2010). Credit risk management and profitability of commercial banks in Kenya.

Kot, S., & Dragon, P. (2015). Business Risk Management in International Corporations. *Procedia Economics and Finance, 27*, 102-108. doi:10.1016/S2212-5671(15)00978-8

Kültür, Y., & Çağlayan, M. U. (2017). A novel cardholder behavior model for detecting credit card fraud. *Intelligent Automation & Soft Computing*, 1-11.

Kvale, S., & Brinkmann, S. (2009). *InterViews: Learning the Craft of Qualitative Research Interviewing*: SAGE Publications.

Lăcrămioara, B., & Mihai, P. (2011). CREDIT CARD FRAUD. *Annals of the Stefan cel Mare University of Suceava : Fascicle of the Faculty of Economics and Public Administration, 11*(1), 81-85.

Levine, R., & Zervos, S. (1998). Stock markets, banks, and economic growth. *American economic review*, 537-558.

Liebenberg, A. P., & Hoyt, R. E. (2003). The determinants of enterprise risk management: Evidence from the appointment of chief risk officers. *Risk Management and Insurance Review, 6*(1), 37-52.

Lind, G. (2005, p.23-24). Basel II–the new framework for bank capital. *Sveriges Riksbank Economic Review, 2*(2005), 22-38.

Luostarinen, R. (1979). *Internationalization of the firm: an empirical study of the internationalization of firms with small and open domestic markets with special emphasis on lateral rigidity as a behavioral characteristic in strategic decision-making* (Vol. 30): Helsinki School of Economics.

MacDonald, R. H., & Dowling, A. M. (1993). The savings and loan crisis: a system dynamics perspective. *SYSTEM, 93*, 279.

Mahmoudi, N., & Duman, E. (2015). Detecting credit card fraud by modified Fisher discriminant analysis. *Expert Systems with Applications, 42*(5), 2510-2516.

Marshall, M. N. (1996). Sampling for qualitative research. *Family practice, 13*(6), 522-526.

MasterCard. (2014). The 8 Different Types of Card Fraud [Press release]. Retrieved from https://newsroom.mastercard.com/asia-pacific/2014/10/28/8-different-types-card-fraud/

MasterCard. (2017). Help protect your customers with EMV Chip. Retrieved from https://www.mastercard.us/en-us/merchants/safety-security/emv-chip.html

McNeil, A. J., Frey, R., & Embrechts, P. (2015). *Quantitative risk management: Concepts, techniques and tools*: Princeton university press.

Memari, M. (2016, p.16). Risk management in developing countries.

Miles, J., & Gilbert, P. (2005). *A handbook of research methods for clinical and health psychology*: Oxford University Press on Demand.

NilsonReport. (2016). *Card Fraud Worldwide*. Retrieved from https://www.nilsonreport.com/upload/content.../The_Nilson_Report_10-17-2016.pdf

Norrman, A., & Jansson, U. (2004). Ericsson's proactive supply chain risk management approach after a serious sub-supplier accident. *International journal of physical distribution & logistics management, 34*(5), 434-456.

O'donnell, G. A. (2004). Why the rule of law matters. *Journal of democracy, 15*(4), 32-46.

Orlitzky, M., & Benjamin, J. D. (2001). Corporate social performance and firm risk: A meta-analytic review. *Business & Society, 40*(4), 369-396.

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and Policy in Mental Health and Mental Health Services Research, 42*(5), 533-544.

Raghavan, R. (2003). Risk management in banks. *CHARTERED ACCOUNTANT-NEW DELHI-, 51*(8), 841-851.

Rahman, M. L., & Banna, S. H. (2016). Liquidity Risk Management: A Comparative Study between Conventional and Islamic Banks in Bangladesh. *Journal of Business and Technology (Dhaka), 10*(2), 18-35.

Ritter, J. R. (1991). The long-run performance of initial public offerings. *The journal of finance, 46*(1), 3-27.

Rona-Tas, A., & Guseva, A. (2014). *Plastic money : constructing markets for credit cards in eight postcommunist countries*

Roulstone, D. T. (1999). Effect of SEC financial reporting release No. 48 on derivative and market risk disclosures. *Accounting Horizons*, *13*(4), 343-363.

RoyalSociety. (1992, p.3). *Risk: Analysis, perception and management*.

Runo, F. N. (2013). Relationship between foreign exchange risk and profitability of oil Companies listed in the Nairobi securities exchange. *Unpublished MBA Project, University of Nairobi*.

Sakharova, I. (2012). Payment card fraud: Challenges and solutions. In Intelligence and Security Informatics (ISI), 2012 IEEE International Conference on (pp. 227-234). IEEE.

Salehi, S. A. S., & Rajabi, F. K. (2015). Identification and Prioritizing Factors Influencing Bank Selection: A Case Study of Retail Banking in Tehran.

Sandberg, J. (2000). Understanding human competence at work: an interpretative approach. *Academy of management journal*, *43*(1), 9-25.

Regulations for Payment Card Security, (2016).

Schneier, B. (2011). *Secrets and lies: digital security in a networked world*: John Wiley & Sons.

Schumpeter, J. (1912). *Theorie der wirtschaftlichen Entwicklung*. Leipzig: Duncker & Humblot.

Shachmurove, Y. (2000). Portfolio analysis of major Eastern European stock markets. *International Journal of Business*, *5*(2), 1-28.

Shen, A., Tong, R., & Deng, Y. (2007). *Application of classification models on credit card fraud detection.* Paper presented at the Service Systems and Service Management, 2007 International Conference on.

Siau, K., Lim, E. P., & Shen, Z. (2001). Mobile Commerce: Promises, Challenges and Research Agenda. *Journal of Database Management (JDM)*, *12*(3), 4-13. doi:10.4018/jdm.2001070101

Smith, A. (1776). An Inquiry into the Nature and Causes of the Wealth of Nations, 2 vols. *W. Strahan and T. Cadell.[MTG]*.

Statista. (2016). Number of payment cards globally in 2016. Retrieved from https://www.statista.com/statistics/283578/payment-card-growth-trend-global/

Stoneburner, G., Goguen, A. Y., & Feringa, A. (2002). Sp 800-30. risk management guide for information technology systems.

Toakley, A. (1989). Risk, uncertainty and subjectivity in the building procurement process-acritical review. *School of Building*, 144.

Tummala, R., & Schoenherr, T. (2011). Assessing and managing risks using the supply chain risk management process (SCRMP). *Supply Chain Management: An International Journal*, *16*(6), 474-483.

Van Gestel, T., & Baesens, B. (2009). *Credit Risk Management: Basic concepts: Financial risk components, Rating analysis, models, economic and regulatory capital*: Oxford University Press.

Van Grinsven, J. r. H. M. (2010). *Risk management in financial institutions : formulating value propositions*

VisaInc. (2016a). EMV Liability Shift: Why it pays to adopt new technology [Press release]. Retrieved from https://www.visa.com/chip/merchants/grow-your-business/payment-technologies/credit-card-chip/liability-shift.jsp

VisaInc. (2016b). Questions about your chip card? Chip Cards are our best weapon in fighting counterfeit fraud. Retrieved 13 November 2017 https://usa.visa.com/visa-everywhere/security/visa-chip-card-tips.html

VisaInc. (2017). *Chip-enabled merchants up; Counterfeit fraud down*. Retrieved from https://usa.visa.com/visa-everywhere/security/visa-chip-card-stats-june-2017.html

Waligo, V. M., Clarke, J., & Hawkins, R. (2012). Implementing sustainable tourism: A multi-stakeholder involvement management framework. *Tourism management*. doi:10.1016/j.tourman.2012.10.008

Wallethub. (2016). *redit Card & Debit Card Fraud Statistics*. Retrieved from https://wallethub.com/edu/credit-debit-card-fraud-statistics/25725/

Weber, B. (2016). *EMV chip cards : background, fraud, security and small business issues* Business, Technology and Finance,

Williams, H. (2010, p.8). *Building type basics for banks and financial institutions* (Vol. 16): John Wiley & Sons.

WorldPayments. (2015). Global Non-cash Payments Volume. Retrieved from https://www.worldpaymentsreport.com/#non-cash-payments-content

Yin, R. K. (2014). *Case study research : design and methods* (5th ed. ed.). Los Angeles, Calif: SAGE.

Appendix

Appendix A

Interview guide

Research question:

How do risk management handle challenges related to counterfeit cards fraud in a South Asian context??

The aim of the study: the first aim of this study is to identify challenges that financial institutions have, more specifically banks, in handling of counterfeit cards fraud and how the risk managers handle such challenges. Secondly, this study is an effort to develop a theoretical framework of risk management which may help risk managers of the other banks to adopt effective risk handling strategies to handle with challenges related to

counterfeit cards fraud.

Before starting the interview, it will be focused to establish a conversation with participant to create relaxed atmosphere. The interview will be started seeking **verbal consent** of the participant to conduct and record the interview:

"This interview is completely anonymous and voluntary. Interview will be audio taped to collect the information accurately. If you choose to stop it at any stage of the discussion, the recording will be deleted. The data being collected, will only be used for the study purpose. Do you agree?"

Ok, so first we start with some basic information about you. Can you say your name, please?

Interviewee's background information:

Participant's name: _____

Ok, and what is your age?

Can you please tell something about your education?

What is your job title in this organization and how would you describe your role?

Could you please also tell something about your professional background and job experience?

Branch network and cards portfolio size:

Financial institution / bank name: _____

1. Could you please tell something about your bank? How many branches do you have?
2. Do you, as a bank, operate only in Pakistan or in international markets as well?
3. Does your bank deal only in cards business or is also involved in merchants acquiring business?
4. What is an approximate number of credit and debit cards issued by your bank?
5. What can be an average number of credit and debit card transactions on a daily basis in local and international markets?
6. What is your staff strength in fraud and risk management unit to minimize risk or fraud?

Now, after this introductory part, I will proceed with questions related to my research topic about challenges and solutions to handle counterfeit cards fraud.

Questions related to the research topic:

1. How do you handle risk of counterfeit cards fraud?
2. Which systems or tools do you use to minimize this fraud? Are these developed internally by the bank or acquired from other market sources?

3. In your opinion, which systems or tools are most effective in market? Do you think acquisition of enhanced systems or tools may be a challenge for the banks?

4. What would you say about rapid technological advancement in cards business? Do you see any drawbacks of technology as a challenge to minimize counterfeit cards fraud?

5. What is your view about EMV chip technology and to what extent it enables you to minimize this fraud?

6. How Enterprise Risk Management (ERM) and Basel Accord frameworks help you to control this type of fraud?

7. What challenges do you have related to counterfeit cards fraud and how do you handle these challenges?

8. What are your views about laws and regulations related to this fraud? Do you have any challenges in coordinating with law enforcement agencies to minimize this fraud?

9. What education or training a fraud or risk analyst should have to handle counterfeit cards fraud?

10. In your opinion, what challenges do other banks have in handling of this type of fraud?

11. Do you have any other remarks that you would like to express that you think you have not mentioned it before and can be valuable for this study?

Thank you so much for your participation during this interview and valued information, this would be very helpful for my study.