A Conceptual Framework for Evaluating the Security of Household Bank Customers in the Kingdom of Saudi Arabia



Deena Alghamdi

Linacre College

Computer Science Department

Oxford University

This thesis is submitted for the degree of Doctor of Philosophy

Trinity 2017

In The Name Of Allah Most Gracious

Most Merciful

DECLARATION

This dissertation is the result of my own work and includes nothing which is the outcome of work done in collaboration except where specifically indicated in the text. It has not been previously submitted, in part or whole, to any university of institution for any degree, diploma, or other qualification.

Signed:_____

Date:_____

ABSTRACT

This work evaluates the security of household banking in the Kingdom of Saudi Arabia by investigating the fit between the Saudi banking system and the practices of its household customers. A framework is developed to evaluate both technical and human factors, to help build a secure and effective banking system. Three building blocks contribute to the framework: the household context of use of bank systems in Saudi Arabia, banking technologies and processes, and Saudi banking policies and infrastructure. A qualitative study of the household context of use employs grounded theory to identify the banking practices of household customers and the factors influencing them. Data were collected in two phases: from 47 household customers, using telephone interviews, focus groups and the diary/interview method, then from 23 Saudi bankers interviewed by telephone. Each method was adjusted to accommodate the unique settings of the research context, such as being a Saudi female researcher collecting data from participants of both genders, the sensitivity of the topic and the intimate nature of the household context. This research contributes as a practical guide by describing each method used in detail, serving to inform and guide future work in a similar context. The second block in the framework is the security analysis of the banking technologies and processes used by participating household customers: online banking, telephone banking and bank cards. The two analytical approaches are STRIDE, which aims to identify objectives and vulnerabilities in bank technologies regarding specific security threats, and DREAD, which is used to quantify the risk from such threats. The third block is the Saudi banking policies and infrastructure that guide the use of the technologies issued by the Saudi Arabian Monetary Agency (SAMA) the leading authority to the Saudi banking sector, involving a deep analysis of the official policies and regulations related to the household context of use of bank technologies.

The framework is applied to evaluate the security of household banking in two case studies: the use of new technologies such as mobile banking and the use of fingerprints as a new security mechanism in the authentication process of bank cards.

ACKNOWLEDGEMENTS

Praise be to Allah, the Lord of the worlds. And the blessings and the peace be upon the last messenger of Allah, Mohammed (Peace Be Upon Him and All Other Prophets and Messengers).

First and foremost, thanks and praise to Allah, the most gracious and most merciful, for his directions and guidance throughout my entire life.

The author is very grateful to both Prof. Marina Jirotka and Prof. Ivan Flechais for their enthusiastic supervision, enlightening inspiration, continuing encouragement and invaluable technical suggestions throughout the course of this investigation. The author also appreciates the guidance given to improve her research skills. Deep thanks also go to all lecturers, professors, academic and administrative staff and students at Oxford University for their assistance and support during my studies.

Special thanks are due to all the participating bank customers and bankers who made this research possible. The author is grateful to Umm Al-Qura University for providing the necessary financial support for this research to continue.

My deepest thanks and special gratitude go to my dear parents: my mother Rahmah for her ceaseless prayers and support, and my father Eiddah for his continuing encouragement and for building a strong belief in my abilities since I was a child. My deepest thanks to my lovely children Abdulmohsen and Omar for supporting me throughout my academic research. Finally, my thanks to my brothers and sisters and all my relatives for their support and encouragement during my different research stages. I am also deeply grateful to all friends whose support and unforgettable companionship I really value.

PUBLICATIONS

2012:

Alghamdi, D."Gender Differences, Women and the Internet" Saudi Scientific International Conference (SIC), London 2012.

2013:

Flechais, I., M. Jirotka and D. Alghamdi (2013). In the balance in Saudi Arabia: security, privacy and trust. CHI '13 Extended Abstracts on Human Factors in Computing Systems (CHI EA '13). Paris, France, ACM, New York, NY, USA, 823-828.

2015:

Alghamdi, D., I. Flechais and M. Jirotka (2015). Security Practices for Households Bank Customers in the Kingdom of Saudi Arabia. Symposium On Usable Privacy and Security. Ottawa, Canada.

CONTENTS

1 INTRODUCTION **1**

1.1 RESEARCH SCOPE AND CONTRIBUTION 6

1.2 RESEARCH APPROACH 8

1.3 THESIS STRUCTURE 9

2 BACKGROUND **12**

2.1 INTRODUCTION 12

2.2 BANK SYSTEMS 12

2.2.1 Security analysis *16*

2.2.1.1 STRIDE 17

2.2.1.2 DREAD 17

2.3 THE KINGDOM OF SAUDI ARABIA 19

2.3.1 Religion and cultural norms *19*

2.3.2 Gender roles in the KSA *21*

2.3.3 Saudi bank system *26*

2.3.3.1 Saudi banking history 27

2.3.3.2 Saudi banking today 28

2.3.3.3 Saudi banking policies 38

2.4 FAMILIES AND HOUSEHOLDS 38

2.5 HUMAN-COMPUTER INTERACTION 41

2.5.1 Usability and security *43*

2.5.2 Human values and security *44*

2.5.3 Social elements and security *48*

2.6 CHAPTER SUMMARY 52

3 METHODOLOGY **53**

3.1 INTRODUCTION 53

3.2 HUMAN-COMPUTER INTERACTION 54

3.3 GROUNDED THEORY 55

3.3.1 Validity of grounded theory *59*

3.4 RESEARCH CONTEXT 61

3.5 RESEARCH METHODS 65

3.5.1 Semi-structured interviews *65*

3.5.2 Focus groups *66*

3.5.3 Diary/interview *67*

3.6 RESEARCH IN ACTION 68

3.6.1 Eliciting data from customers *70*

3.6.1.1 Pilot study 70

3.6.1.2 Second round 72

3.6.1.3 Third round 74

3.6.2 Eliciting data from bankers *76*

3.6.3 Challenges of using interviews in the research context *77*

3.6.4 Challenges of using focus groups in the research context *80*

3.6.5 Challenges of using diaries in the research context *83*

3.7 CHAPTER SUMMARY 85

4 MODEL OF HOUSEHOLD CUSTOMERS' PERSPECTIVE 86

4.1 INTRODUCTION 86

4.2 HOUSEHOLD CONTEXT OF USE 87

4.3 MODEL BUILDING 88

4.4 GROUNDED THEORY SEMANTICS 89

4.5 MODEL OF HOUSEHOLD CUSTOMERS' PERSPECTIVE 89

4.5.1 The extent of sharing practices *91*

4.5.1.1 Summary 95

4.5.2 Motivations *96*

4.5.2.1 Trust and distrust 97

4.5.2.2 Assurance 101

4.5.2.3 IT skills 101

4.5.2.4 Having little money and making life comfortable 102

4.5.2.5 Accessing cash and illiteracy 102

4.5.2.6 Backup 103

4.5.2.7 Family finances 104

4.5.2.8 Summary 104

4.5.3 Conforming Practices *106*

4.5.3.1 Summary 109

4.5.4 Challenging practices ... *110*
4.5.4.1 Appeal to a higher authority ... 111
4.5.4.2 Financial co-dependence and financial independence ... 112
4.5.4.3 Summary ... 113
4.6 CHAPTER SUMMARY ... 113
5 MODEL OF BANKING PERSPECTIVE ... 117
5.1 INTRODUCTION ... 117
5.2 MODEL BUILDING ... 118
5.3 MODEL OF THE BANKING PERSPECTIVE ... 118
5.3.1 Responsibility confusion ... *119*
5.3.1.1 Boundaries of bankers' responsibilities ... 120
5.3.1.2 Confidentiality of credentials ... 124
5.3.1.3 Summary ... 126
5.3.2 Customer authentication concerns ... *126*
5.3.2.1 Summary ... 128
5.3.3 Banking services and infrastructure ... *128*
5.3.3.1 Summary ... 131
5.3.4 Risks to banking security ... *131*
5.3.4.1 Risk of impersonation ... 132
5.3.4.2 Lack of auditability ... 133
5.3.4.3 Summary ... 134
5.4 CHAPTER SUMMARY ... 134
6 MODEL OF THE GENDER PERSPECTIVE ... 137
6.1 INTRODUCTION ... 137
6.2 MODEL BUILDING ... 138
6.3 MODEL OF THE GENDER PERSPECTIVE ... 139
6.3.1 Control ... *140*
6.3.1.1 Men are guardians of women ... 140
6.3.1.2 Accessing cash ... 141
6.3.1.3 Insider threats ... 144
6.3.1.4 Summary ... 147

6.3.2 Infrastructure *147*

6.3.2.1 Proof of identity 147

6.3.2.2 Segregated branches 150

6.3.2.3 Summary 152

6.3.3 Identity *152*

6.3.3.1 Role in the household 153

6.3.3.2 Authorisation 157

6.3.3.3 Summary 158

6.3.4 Workaround *159*

6.3.4.1 Appeal and arbitration 159

6.3.4.2 Secret bank account 162

6.3.4.3 Summary 164

6.4 CHAPTER SUMMARY 164

7 A CONCEPTUAL FRAMEWORK FOR EVALUATING THE SECURITY OF HOUSEHOLD BANK CUSTOMERS IN THE KSA 167

7.1 INTRODUCTION 167

7.2 HOUSEHOLD CONTEXT OF USE 169

7.3 BANKING POLICIES AND INFRASTRUCTURE 172

7.3.1 Proving the identity of household customers *172*

7.3.2 Educating customers *173*

7.3.3 Bank credentials *173*

7.3.4 Bank cards *174*

7.3.5 SMS notification service *174*

7.3.6 Section summary *175*

7.4 BANKING TECHNOLOGIES AND PROCESSES 176

7.4.1 Spoofing *177*

7.4.1.1 Online banking 177

7.4.1.2 Telephone banking 179

7.4.1.3 Bank cards 181

7.4.2 Tampering *182*

7.4.2.1 Online banking 182

7.4.2.2 Telephone banking 184
7.4.2.3 Bank cards 185
7.4.3 Repudiation 185
7.4.3.1 Online banking 185
7.4.3.2 Telephone banking 187
7.4.3.3 Bank cards 187
7.4.4 Information disclosure 189
7.4.4.1 Online banking 189
7.4.4.2 Telephone banking 190
7.4.4.3 Bank cards 191
7.4.5 Denial of service 192
7.4.5.1 Online banking 192
7.4.5.2 Telephone banking 193
7.4.5.3 Bank cards 194
7.4.6 Elevation of privilege 195
7.4.6.1 Online banking 195
7.4.6.2 Telephone banking 196
7.4.6.3 Bank cards 197
7.4.7 Section summary 198
7.5 USING THE FRAMEWORK TO EVALUATE THE SECURITY OF BANKING PRACTICES OF HOUSEHOLD CUSTOMERS IN THE KSA 198
7.5.1 Using biometrics in authentication 199
7.5.1.1 Household context of use 200
7.5.1.2 Banking policies and infrastructure 203
7.5.1.3 Banking technologies and processes 204
7.5.1.4 Evaluation and recommendations 206
7.5.2 Using mobile banking 207
7.5.2.1 Household context of use 207
7.5.2.2 Banking policies and infrastructure 209
7.5.2.3 Banking technologies and processes 210
7.5.2.4 Evaluation and recommendations 211
7.6 CHAPTER SUMMARY 212

8 CONCLUSION **214**

8.1 OVERVIEW 214

8.2 CONTRIBUTIONS 216

8.2.1 Substantive contributions *216*

8.2.1.1 Identifying practices 216

8.2.1.2 Household context of use. 217

8.2.1.3 A conceptual framework for evaluating banking security 217

8.2.2 A practical guide to the methodology *217*

8.2.2.1 Reflections on building rapport with participants 218

8.2.2.2 Reflections on the sensitivity of the research topic 218

8.2.2.3 Reflections on the methods of collecting data 219

8.3 CRITICAL REVIEW 221

8.3.1 Research scope *221*

8.3.2 Thesis complexity *222*

8.3.3 Framework validation and evaluation *222*

8.4 FUTURE WORK 223

8.4.1 Testing the model's theory *223*

8.4.2 Testing the model's predictions *223*

8.4.3 Comparative studies *224*

8.4.4 Non-banking familial practices *225*

9 APPENDICES **226**

10 REFERENCES **264**

LIST OF TABLES

TABLE 1: DREAD CLASSIFICATION (MEIER, MACKMAN ET AL. 2003B). 18

TABLE 2: DEMOGRAPHIC INFORMATION ON HOUSEHOLD CUSTOMERS 68

TABLE 3: DEMOGRAPHIC INFORMATION ON PARTICIPATING BANKERS 76

TABLE 4: DREAD ANALYSIS FOR SPOOFING OF ONLINE BANKING 178

TABLE 5: DREAD ANALYSIS FOR SPOOFING OF TELEPHONE BANKING 180

TABLE 6: DREAD ANALYSIS FOR SPOOFING OF BANK CARDS 182

TABLE 7: DREAD ANALYSIS FOR TAMPERING WITH ONLINE BANKING 183

TABLE 8: DREAD ANALYSIS FOR TAMPERING WITH ONLINE BANKING 184

TABLE 9: DREAD ANALYSIS FOR TAMPERING WITH BANK CARDS 185

TABLE 10: DREAD ANALYSIS FOR REPUDIATION OF ONLINE BANKING 186

TABLE 11: DREAD ANALYSIS FOR REPUDIATION OF TELEPHONE BANKING 187

TABLE 12: DREAD ANALYSIS FOR REPUDIATION OF BANK CARDS 189

TABLE 13: DREAD ANALYSIS FOR DISCLOSURE OF ONLINE BANKING INFORMATION 190

TABLE 14: DREAD ANALYSIS FOR DISCLOSURE OF TELEPHONE BANKING INFORMATION 191

TABLE 15: DREAD ANALYSIS FOR DISCLOSURE OF BANK CARD INFORMATION 192

TABLE 16: DREAD ANALYSIS FOR DENIAL OF SERVICE IN ONLINE BANKING 193

TABLE 17: DREAD ANALYSIS FOR DENIAL OF SERVICE IN TELEPHONE BANKING 194

TABLE 18: DREAD ANALYSIS FOR DENIAL OF SERVICE FOR BANK CARDS 195

TABLE 19: DREAD ANALYSIS FOR ELEVATION OF PRIVILEGE FOR ONLINE BANKING 196

TABLE 20: DREAD ANALYSIS FOR ELEVATION OF PRIVILEGE FOR TELEPHONE BANKING 196

TABLE 21: DREAD ANALYSIS FOR ELEVATION OF PRIVILEGE FOR BANK CARDS 197

TABLE 22: SUMMARY OF DREAD ANALYSES 198

LIST OF FIGURES

FIGURE 1: FRAMEWORK FOR EVALUATING THE SECURITY OF HOUSEHOLD BANKING. 5

FIGURE 2: BANKING INFRASTRUCTURE AND SERVICES IN THE KSA 30

FIGURE 3: ONLINE BANKING REGISTRATION PROCESS 35

FIGURE 6: HOUSEHOLD CONTEXT OF USE 87

FIGURE 7: EXAMPLE OF A GROUNDED THEORY NETWORK DIAGRAM. 89

FIGURE 8: MODEL OF HOUSEHOLD CUSTOMERS' PERSPECTIVE. 91

FIGURE 9: THE EXTENT OF SHARING PRACTICES. 92

FIGURE 10: MOTIVATIONS. 97

FIGURE 11: CONFORMING PRACTICES 106

FIGURE 12: CHALLENGING PRACTICES. 110

FIGURE 13: MODEL OF THE BANKING PERSPECTIVE. 119

FIGURE 14: RESPONSIBILITY CONFUSION. 120

FIGURE 15: CUSTOMER AUTHENTICATION CONCERNS. 127

FIGURE 16: BANKING SERVICES AND INFRASTRUCTURE. 129

FIGURE 17: RISKS TO BANKING SECURITY. 132

FIGURE 18: MODEL OF THE GENDER PERSPECTIVE. 140

FIGURE 19: HOUSEHOLD CONTEXT OF USE 167

FIGURE 20: FRAMEWORK FOR EVALUATING THE SECURITY OF HOUSEHOLD BANKING. 168

FIGURE 21: APPLYING THE FRAMEWORK TO A COUNTERMEASURE. 199

LIST OF APPENDICES

APPENDIX 1: PILOT STUDY QUESTIONS 227

APPENDIX 2: FOCUS GROUP QUESTIONS 229

APPENDIX 3: SAMPLE DIARY 231

APPENDIX 4: INTERVIEW QUESTIONS WITH CUSTOMERS IN THE 3RD ROUND OF DATA COLLECTION 232

APPENDIX 5: INTERVIEW QUESTIONS FOR BANKERS 234

APPENDIX 6: INVITATION LETTER 236

APPENDIX 7: CONSENT FORM 239

APPENDIX 8: SAMPLE OF DATA CODING 242

APPENDIX 9: MODEL OF HOUSEHOLD CUSTOMERS' PERSPECTIVE 243

APPENDIX 10: MODEL OF BANKING PERSPECTIVE 244

APPENDIX 11: HOUSEHOLD CONTEXT OF USE OF BANK SYSTEM 245

APPENDIX 12: CODES AND MEMOS 247

APPENDIX 13: INSIDER ATTACK CASES 258

1 INTRODUCTION

The aim of this work is to evaluate the security of household banking in the Kingdom of Saudi Arabia (KSA) by investigating the fit between the Saudi bank system and the banking practices of household customers. On the assumption that the Saudi system, in common with others worldwide, is based on a design conceived originally for a very different Western culture, questions arise as to whether its imperfect fit with its customers' practices may affect the security of the system itself and of these customers. Past research into computer security, including human-computer interaction security (HCISec), has tended to focus on tackling technical issues or improving user interfaces to security tools (Dourish and Redmiles 2002, Friedman and Felten 2002, Ka-Ping 2002). Whilst this is an important aspect of improving the overall usability and effectiveness of secure systems, it does not go far enough; for example, the HCISec community has come to realise relatively recently that many reported security breaches have been enabled and facilitated by inappropriate user behaviour. Thus, researchers have presented arguments such as the following:

> *The goal of security is not to build systems that are theoretically securable, but to build ones that are actually secure... It requires close examination not only of the technology, but also of the human beings that will use it* (Tognazzini 2005, p. 31).

Tognazzini thus considers a major requirement to ensure the security of a system to be the close examination of its users. By studying users' security practices, experts have found that these constitute "a vital variable" impacting the effectiveness of a system's security, according to Weirich and Sasse (2001). They found, for example, that colleagues in a workplace will commonly disclose passwords to each other as a sign of trust between them, to the extent that not participating in this social practice can easily be seen as hiding something, although doing so offers a clear opportunity for hackers and industrial spies to use social engineering techniques. Certainly, such disclosure is against the security requirements of the password-based authentication mechanism whereby passwords should be kept secure and not disclosed to anyone.

This mismatch between the actual practice of users and the security requirements of a system may occur because of the complexity of the security mechanisms (Zurko and Simon 1997). Other researchers (Adams and Sasse 1999, Sasse, Brostoff et al. 2001, Weirich and Sasse 2001) found that most users inadvertently break these security rules as a consequence of bad design, difficult requirements or an inadequate security culture. Alternatively, Sasse and Flechais (2005) argue that this mismatch arises from the conflict between security policies and the social relationships of the users.

This argument would apply to various systems including bank systems. Banks play an essential role in many aspects of daily life, helping customers with investment, finance and asset management. In addition, they provide services like secure payments, current

and savings accounts, which facilitate customers' essential everyday tasks such as paying bills without the inconvenience of using cash. The importance of banks and their daily use by millions of customers motivates the urgency of ensuring the security of their systems by the close examination of customers and their practices, with the aim of avoiding any conflict or mismatch between the security requirements of bank systems and customers' practices. A key issue is that the banking system and its policies were designed to be universal but are, in reality, designed primarily for Western cultures; 'universal' design principles may turn out to be anything but, conflicting with local aesthetics, metaphors and assumptions (Marcus and Gould 2000). In the context of money and banking, it is important to consider cultural norms, because money is managed and owned in different ways in different cultures (Singh 1997).

For example, Singh et al. (2007b) conducted a study of bank security requirements and cultural norms among Australian households. As a security measure, bank systems in Australia require their customers not to share the access codes to their accounts with anyone, not even family members; the danger is that sharing leads to the customer being legally unprotected. In a qualitative study of the practices of 79 people with issues of security and privacy in personal banking, Singh et al. (2007b) found that the banks' dependence on authentication via user name and password was in conflict with the social practice of sharing information about money within couples. The study shows that when one person in a couple controls the money, paying the bills and monitoring internet banking, it is usual for that person to control all accounts, joint and individual, including the accounts of the person's partner. Singh et al. (2007b) conclude that "the everyday violation of these security requirements results from the lack of fit between security design and social and cultural practice".

While banks serve both organisations and households, this thesis focuses on household bank customers, as users' practices in the household context are relatively underexplored. Gaw et al. (2006) found that users were in the habit of reusing passwords. This weakens household security, as exemplified by the repeated security breaches affecting Sony, which found that more than 93,000 of its household users used the same usernames and passwords as log-in credentials for different accounts (Zetter 2011). Such duplication allows intruders to collect the credentials from one source and use them to gain access to other accounts. Sony estimated that consequent breaches in spring 2011 would cost the company more than $170 million (Zetter 2011). Moreover, it was found that even after users' Sony accounts were breached, 59% of people were still using the exact same password on Yahoo Voices (Goldberg 2011, Hunt 2012). Such cases underline the need for a better understanding of household users' practices to enhance the security of both customers and service providers.

The household context is interesting when compared to the organisational one for a number of reasons: first, users spend longer hours and conduct a broader variety of activities at home than they usually do in the workplace. Second, the organisational context typically contains only employees, while the household context may include wider groups of employed and unemployed users such as housewives, househusbands, students, children, pensioners and others. Third, households interact with a variety of different services, each offering different forms of security components, configuration options and advice, yet in most households, responsibility for security does not rest with an experienced security practitioner. While organisations face similar challenges, they can devote greater resources to staffing, formulating security policies and educating their employees in matters of security.

All of the above considerations motivated the present research, whose aim is to build a framework to evaluate the security of Saudi banks' systems by investigating the fit between them and the banking practices of their household customers. Three building blocks are essential in this framework, as seen in Figure 1: the household context of use of bank systems in the KSA, which involves identifying the banking practices of household customers and the factors influencing these practices; the banking technologies and processes used by household customers; and the banking policies and infrastructure that guide the use of these technologies.

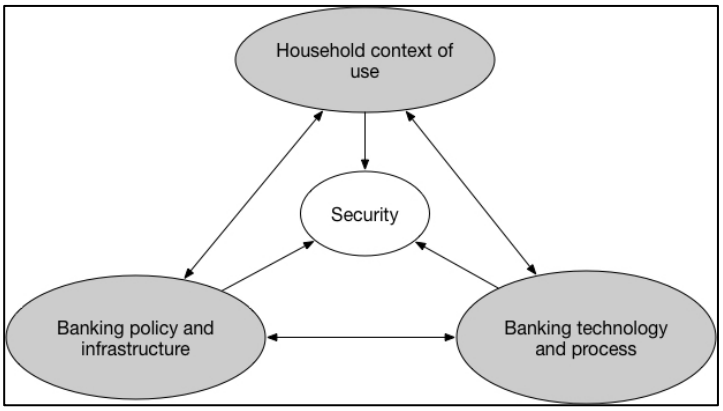


Figure 1: Framework for evaluating the security of household banking.

Each block affects the others and the security of household banking. This framework provides a means of addressing both technical and human factors and evaluating them, as a contribution towards a secure and effective banking system. Without a framework describing customers' practices and the related requirements, it would be difficult to evaluate the current system or to propose an improvement that is effective and secure while at the same time matching the actual banking practices of household customers. There is, therefore, a need to identify the banking practices of household customers and to assess the significance of their effects on the security of the banking system, in order to inform future research efforts into making that system more secure. This framework has important public policy implications for the efforts to achieve a more competitive

and efficient financial system. This study may also help to protect and possibly improve individuals' banking security and could assist the regulatory authorities in determining future courses of action to be pursued to further strengthen the Saudi Arabian banking sector, particularly the domestically incorporated banks.

Therefore, the overall research question addressed by this work is: How can the security of Saudi bank systems be evaluated by considering household customers' banking practices?

This can be further broken down into the following questions:

RQ1: What are the banking practices of household customers of Saudi banks that affect the security of the banks' systems?

RQ2: How can technical security mechanisms be augmented in Saudi banks' systems to improve the fit between the banking practices of their household customers and the banks' technical systems?

These questions are answered respectively by examining the banking practices of household customers and by identifying the bank's regulations and banking perspective related to these practices. By empirically investigating this problem, a framework is created for use in evaluating the banking practices of household customers and the security of the current system.

1.1 Research Scope and Contribution

This research is concerned with the use of banks by customers; importantly, the banking system in question is that of the KSA, which may be broadly similar to those in other parts of the world, but with some differences. This thesis does not seek to identify or to

take account of the similarities and differences between banking systems in different countries.

This study focuses on the part of the banking system related to interactions between customers and the system, whereas those aspects of the system related to finance and business issues lie outside the scope of the study. Banks serve a wide range of customers, but this study is concerned only with household customers and the banks' rules and regulations as related to such customers.

The aim of this research is to investigate the banking practices of household customers of Saudi banks as well as to explore how the findings can be best integrated into a conceptual framework associated with the Saudi banking system. Its main contribution is the development of a conceptual framework that can be utilised to evaluate the banking security practices of household customers in the KSA. The framework is designed to help the designers and developers of Saudi banks' systems to orient their work by assessing how a particular technical security mechanism fits with the banking practices of their household customers. Without such a conceptual framework, it would be unclear which elements of the existing Saudi banking system are responsible for positive outcomes and which can be improved on; we are unaware of any conceptual framework which integrates details of the systems of Saudi banks with the banking practices of their household customers. Constructing the framework required a deep qualitative investigation and analysis of the banking practices of household customers of Saudi banks. Qualitative research is primarily exploratory, seeking an understanding of underlying causes, attitudes and motivations, while quantitative research serves to quantify a problem by generating numerical data or data that can be presented in statistical form (Glesne and Peshkin 1992, Morgan 1996). The present research is a qualitative investigation whose framework offers a detailed account and description of

the banking practices of household customers, of the factors influencing the adoption of their practices and of customers' and bankers' perspectives. The findings of that investigation had then to be integrated with knowledge of the systems operated by these banks. This thesis does not seek to provide improvements to the current banking system, although it is anticipated that the proposed framework might be used in future for this purpose.

Moreover, given the shortage of existing guidance for applying different qualitative methods in Islamic and Arab countries in general and the KSA specifically, this thesis contributes as a practical guide by providing a detailed description of the application of such methods used in the research context of the KSA. This description may guide future researchers in choosing suitable methods for this context and prepare them for the conditions they may find, indicating how to adjust their methods to address and avoid the difficulties and the cultural constraints associated with the context.

1.2 Research Approach

A key contribution of this research is to produce a conceptual framework evaluating the banking security of household bank customers in the KSA. There are no pre-existing studies related to this area and the methodological approach has been shaped accordingly. After considering the advantages and drawbacks of other approaches, grounded theory (Glaser and Strauss 1967, Glaser 1992, Glaser 1998, Charmaz 2006) was chosen as the appropriate analytical methodology to draw out the key factors influencing the banking security of household customers and their practices and to understand the reasons and motivations for these practices. Grounded theory has been described as "a research method that involves creating conceptual frameworks or theories by analysing the data collected" (Charmaz 2006), p. 187). This approach was

found to be suitable for this kind of research, as it is "an inductive theory discovery methodology that allows the researcher to develop a theoretical account of the general features of a topic while simultaneously grounding the account in empirical observations or data" (Martin and Turner 1986). Grounded theory validates its results by continually informing them with the empirical data that have been collected. Data collection in the context of KSA banking practices proved to be particularly challenging, as will be detailed later in the thesis; thus the methods and techniques adopted were appropriate to the intimate nature of the household context and to the cultural and religious constraints of the KSA (Section 3.4: Research context). Telephone interviews, focus groups and diaries were the means chosen to collect data from household customers, while telephone interviews were used to gather material from bankers.

1.3 Thesis Structure

Following this introductory chapter, the remainder of the thesis consists of seven chapters, as follows:

Chapter 2 lays out the contextual background to the study in four parts. The first describes banking systems in general. As these were designed for Western cultures and this thesis focuses on a non-Western one, the second part describes the KSA, sketches the main characteristics of Saudi culture and outlines the Saudi banking sector. The unit of analysis is the household and the third part reviews the interdisciplinary literature on the concepts of family and household. The final part of the chapter discusses the research domain of the security of human-computer interaction and reviews the relevant literature.

Chapter 3 describes the research methods selected for data collection and analysis and provides a justification for these methodological approaches based on the research context. There follows a review of each method used to collect data and the challenges encountered when adopting them in the KSA research context.

Chapters 4, 5 and 6 present in turn the three models built during the study, beginning in Chapter 4 with a model of the household customers' perspective. The chapter first describes the process of model building based on the data collected from household bank customers, then it presents and discusses the model in detail.

Chapter 5 presents the model of the banking perspective; it first describes the building of the model from the data collected from bankers, then details the model and discusses its elements.

Because of the strong influence of gender on banking security in the KSA, Chapter 6 presents a third model, of the gendered perspective, built on the findings from both household customers and bankers regarding the impact of gender in the banking context.

Chapter 7 presents a framework for evaluating the security of household bank customers in the KSA and is in four parts. The first focuses on the final model, which integrates the above three partial models and encapsulates the household context of use of bank systems by household customers in the KSA. Together with an analysis of Saudi banking policies and infrastructure and of banking technologies and processes, it forms the conceptual framework. These two elements therefore comprise the second and third parts of the chapter. The framework is then used to evaluate the security of household banking in the KSA in two cases: the use of a new banking technology and the use of new security mechanisms for an existing technology.

Chapter 8 draws conclusions from the research by detailing what the findings mean for the security of household banking and for future developments. It also discusses the limitations of the current research, enumerates its contributions and reflects on the use of each method in the research context, concluding with suggestions for future work in this area of research.

2 BACKGROUND

2.1 Introduction

The previous chapter has set out the problem that motivated this research, whose purpose is to study the practices of household bank customers in the KSA and to build a framework for evaluating the security of household bank customers. This background chapter begins in Section 2.2 with an introduction to bank systems in general and a discussion of the approaches to analysing the security of bank technologies, followed in Section 2.3 by a detailed description of the Kingdom of Saudi Arabia. This section focuses on three aspects of Saudi culture related directly to the findings of this research: religion and cultural norms in Section 2.3.1, gender roles in Section 2.3.2 and banks in Saudi Arabia in Section 2.3.3. Section 2.4 discusses the concept of 'household' as the unit of analysis in this research. Finally, Section 2.5 reviews the literature on the security of human-computer interactions into which this research fits.

2.2 Bank Systems

This section presents background information on bank systems and services adapted and used worldwide, offering an outline of the threat modelling that will be used later to analyse the security of bank services in the framework presented in Chapter 7.

A bank system can be considered a socio-technical system which operates on a technical basis and is used by millions of people every day (Whitworth and Ahmad 2013). The term 'socio-technical system' was first coined after the Second World War by the Tavistock Institute in London (Long 2013). It refers to the interaction between the social and technical factors which affect different aspects of the system, such as its efficiency and security, so that optimizing any of these factors will tend to improve the overall system. Detailed examination reveals that the term 'socio-technical' covers every aspect of a system, including hardware (PCs, hubs, routers), software (applications, programs, codes), users and their practices, system services and regulations, data flow and structure.

According to Cherns (1987), one of the principles of designing or operating such a system is the importance of addressing and optimising both technical and social factors. Social engineering attacks on socio-technical systems will specifically target those users who have access to the secure system, thus evading software and hardware countermeasures. These attacks may succeed where there exists a mismatch between the user practices required by software and hardware countermeasures on one hand and users' actual practices on the other. For example, if an attacker mimics a technical support operative, users may be persuaded to help with a supposed upgrade by sharing passwords with the attacker, despite the fundamental prohibition of divulging passwords in a password-based authentication mechanism. Such gaps between users' obligations and their actual performance raises significant difficulties for computer security. The disparity between expected and actual user practice can arise in two ways. If security designers fail to address human factors in a socio-technical system, design decisions may be taken without considering the requirements of both social and technical aspects of the system. Alternatively, security designers may address both sets of factors but

developers may fail to apply them. Possible causes are prioritising functional needs over security design, or difficulties in using the security techniques that have been designed.

Services offered by banks include opening and managing bank accounts, cash management (deposits, withdrawals, transfers), cheques, loans, debit and credit cards, and the Electronic Funds Transfer at Point of Sale (EFTPOS) system, which allows the customer to use a bank card to pay for purchases at a retail outlet by transferring money immediately from his or her bank account to the retailer's account. In a study of patterns of purchase loyalty and retail payment methods in New Zealand, Wright (2002) conducted face-to-face surveys of bank customers over 15 years and found that EFTPOS was widely used (by 72% of the sample, compared with 10% for cheques and 12% for credit cards), its primary competition coming from cash payment (67%).

Many banks offer more cost-effective channels as alternatives to bank branches to deliver their services, such as automated teller machines (ATMs) and telephone, online and mobile banking. For example, consider the cost per transaction of checking a customer's account balance, which is $10.00 if the customer visits a branch, $3.00 when contacting a live representative by telephone, $0.40 using an automated telephone system and just a few pennies by internet (Barrett 1997); offering these channels to customers and encouraging them to use them can save money, time and effort for banks and their customers. Mobile banking may be distinguished from online banking by the use of a smartphone application, rather than a personal computer and web browser (Brown, Cajee et al. 2003). Mobile banking services allow customers to use a mobile device for transactions such as statement and balance enquiries, ordering cheque books and completing funds transfers. The advantages of mobile banking are its convenience, offering access to banking, no matter what the location or time; and its efficiency

(Jarvenpaa, Lang et al. 2003, Laukkanen 2007, Tiwari, Buse et al. 2007, Kanniainen 2010).

Besides having existed for almost three decades, telephone banking is still considered an essential requirement for the future of automated banking systems and is also seen as one of the strong competitors in the banking environment (Wan, Luk et al. 2005). A study by (Lassar, Manolis et al. 2005) lists telephone banking as one of the four major banking channels, with branch banking, ATMs and online banking. Additionally, telephone banking is more cost-effective and more easily accessible to customers than ATMs or online banking (Sundarraj and Wu 2005).

Different customer segments have widely varying channel preferences, because they often prefer a particular channel for a particular transaction (Peak 1997), depending on many factors that research has uncovered. Banking customers from 18 to 26 years old were found to use ATMs, telephone and internet banking interchangeably, but users of internet banking were unconfident about the security of the websites of banks, despite considering the channel efficient and easy to use (Calisir and Gumussoy 2008).

Using SMSs as a communication channel between the business and the individual customer has the potential to improve the management of customer relationships, because the bank can use SMSs to market its products and services, to confirm internet or telephone transactions, to confirm the use of another channel to contact the bank, to confirm appointments or issue reminders and to acknowledge that a complaint has been lodged (Fornell and Wernerfelt 1987, Johnston and Mehra 2002, Peevers, Douglas et al. 2011).

The security analysis of bank services is an essential element in the conceptual framework presented in this thesis and will follow the threat modelling approach presented next.

2.2.1 Security analysis

A wide variety of tools and methods can be used to analyse the security of bank systems, but Leeuwen et al. (2016) point out that researchers must expend considerable effort to match the conceptual goals of their research with the methods and techniques used to achieve these goals. For example, Dorst (2015) developed five problem-focused design practices (coevolution, developing problem situations, creating frames, exploring themes, and fostering a discourse) to provide a new angle for approaching open and complex problems. Meanwhile, Dunne and Martin (2006) refer to the use of abduction to generate an idea or a number of ideas, followed by deduction to take these ideas to their logical consequences and predict their outcomes, then the testing of the ideas in practice and induction to generalize from the results. However, as one of the essential focuses of this thesis is the security of bank systems, bank technologies and services are analysed by means of threat modelling, which is a structured approach that enables the identification of security risks relating to a system—in this case, a bank system. The two specific tools used are STRIDE and DREAD, which are processes developed by the Microsoft Application Consulting and Engineering Team to represent various methods or scenarios through which an attacker may attack a system (Prasath 2010). STRIDE helps in identifying objectives and vulnerabilities in technologies regarding specific security threats, while DREAD it used to quantify the risk from particular threats to technologies.

2.2.1.1 STRIDE

There is a wide variety of security threats; however, these can be categorised according to the attacker's goals and objectives, using STRIDE. This is a threat classification model developed by Microsoft for thinking about computer security threats, where STRIDE stands for (Meier, Mackman et al. 2003a):

- ***Spoofing identity:*** An illigitimate user masquerades as a legitimate user.
- ***Tampering with data:*** Users can potentially change data delivered to them.
- ***Repudiation:*** Insufficient auditing or recordkeeping may lead users to dispute transactions. There are many forms of electronic evidence, often stored securely in an audit trail free of the risks affecting the actual events and safe from manipulation by parties to disputes. Banks should create such evidence routinely, so that if a dispute arises which the parties cannot resolve, an arbitrator has the evidence to do so (Boyd 2009).
- ***Information disclosure:*** submitting secure sensitive information to attackers.
- ***Denial of service:*** making a service unavailable to users.
- ***Elevation of privilege:*** A user elevates his/her role to a higher privilege one.

2.2.1.2 DREAD

After using STRIDE, threats can be rated according to the risks they pose, to allow those associated with the highest risk to be resolved first, before the other threats are addressed. A simple system of rating threats can be used; however, it has been found that team members will usually not agree on ratings. To help solve this, DREAD adds new dimensions that help to determine what the impact of a security threat really means. Meier, Mackman et al. (2003b) define DREAD as a classification scheme for quantifying and prioritizing the amount of risk presented by each threat evaluated; according to them, risks can be quantified as follows:

- ***Damage potential:*** If a threat exploit occurs, how much damage will be caused?
- ***Reproducibility***: How easy is it to reproduce the threat exploit?
- ***Exploitability:*** What is needed to exploit this threat?
- ***Affected users:*** How many users will be affected?
- ***Discoverability:*** How easy is it to discover this threat?

Each aspect of DREAD is rated according to the criteria set out in Table 1.

Table 1: DREAD classification (Meier, Mackman et al. 2003b).

Rating		3	2	1
D	Damage potential	The attacker can subvert the security system; get full trust authorisation; run as administrator; upload content.	Leaking sensitive information	Leaking trivial information
R	Reproducibility	The attack can be reproduced every time and does not require a timing window.	The attack can be reproduced, but only with a timing window and a particular race situation.	The attack is very difficult to reproduce, even with knowledge of the security hole.
E	Exploitability	A novice programmer could make the attack in a short time.	A skilled programmer could make the attack then repeat the steps.	The attack requires an extremely skilled person and in-depth knowledge every time to exploit.
A	Affected users	All users, default configuration, key customers.	Some users, non-default configuration.	Very small percentage of users, obscure feature; affects anonymous users
D	Discoverability	Published information explains the attack. The vulnerability is found in the most commonly used feature and is very noticeable.	The vulnerability is in a seldom-used part of the product, and only a few users should come across it. It would take some thinking to see malicious use.	The bug is obscure, and it is unlikely that users will work out damage potential.

The DREAD algorithm, shown below, is used to compute a risk value:

Risk_DREAD= DAMAGE + REPRODUCIBILITY + EXPLOITABILITY + AFFECTED USERS + DISCOVERABILITY

The calculation always produces a number between 5 and 15; threats with overall ratings of 12 to 15 can be considered high risk, 8-11 as medium risk and 5-7 as low risk.

The security analysis of bank services using STRIDE and DREAD is an essential element in the conceptual framework and will therefore be presented in Chapter 7. Since the focus of this thesis is on the bank systems in a non-Western culture, specifically in the KSA, the next section introduces the KSA and certain aspects of Saudi culture related to this research.

2.3 The Kingdom of Saudi Arabia

The KSA was founded in September 1932 by King Abdul-Aziz Al-Saud. It is one of the largest countries in the Middle East, with an area of over 2,000,000 square kilometres (772,204 square miles). In 2011, its population reached 28.4 million (Pew Research Center 2009). Arabian culture, including Saudi culture, has inspired many anthropologists to investigate the settings and circumstances of human life, describing the interaction between people and their social and physical environment, and relations between household members (Smith 1903, Lipsky 1959, Lapidus 1973, Cole 1975, Cole and Altorki 1989, Al-Rasheed 2007, Cole 2010, Hilden 2011). The following sections focus on three important factors related to the topic of this thesis and its findings which must be discussed in advance: religion and cultural norms, gender roles in the KSA and the Saudi banking system.

2.3.1 Religion and cultural norms

Two very important interrelated features of Saudi culture are religion and cultural norms. Saudi culture is rooted in a mixture of values originating from traditions and Islamic principles. It is difficult to separate cultural phenomena from religious ones and this study seeks to understand how participants invoke these large categories to account for practices using the principle of the qualitative methodology membership categorisation device analysis (MCDA). The aim of MCDA is to understand how

members of society invoke and use different categories to shape and describe the social world (Kelly 2008).

The KSA and its constitution have been described as "a sovereign Arab Islamic state with Islam as its religion; God's Book and the Sunnah [ways and practices] of His Prophet, peace be upon him, are its constitution, Arabic is its language" (International Constitutional Law 2005). Most of its population (97%) are Muslims (Pew Research Center 2009) and their religion plays an important role in Saudi life and politics, as Islam is considered a defining element of Saudi identity (Moaddel 2006). Because of the existence of the two holy mosques (in Makkah and Al Medina), people sometimes refer to the Kingdom as the Land of the Two Holy Mosques; and Saudi Arabia is considered responsible for preserving the Islamic religion. Consistent with this status, Saudi law is derived from the holy Qur'an and the Hadith[1] of Prophet Muhammad (peace be upon him) (Baki 2004, AlLily 2011, Ministry of Higher Education 2012).

Saudi culture is sometimes described as a political culture that acts as a protective screen to ensure that the evolution of technology and human society happen within suitable limits of form and extent (Gallagher and Searle 1985). In such a culture, changes or unforeseen trends in behaviour or belief are considered unacceptable and strongly resisted (AlLily 2011). For example, when in September 1963 the government declared its intention to educate women, there were protests against this policy which the government had to suppress by force (Huyette 1985, Hamdan 2005). Nevertheless,

[1] The Hadith is the written record of the Prophet's sayings and his daily practices.

girls' education gradually became accepted by the Saudi populace and by 2015, close to half of the seven and a half million school students were female (General Authority of Statistics 2015). Another example of changes not being easily accepted is the current slow progress in amending aspects of gender roles, such as women driving and male guardianship, as detailed in the next section. This background is important in understanding the strong impact of religion and cultural norms on the banking practices of household customers, as discussed in Chapters 4, 5, and 6. In addition, gender has a powerful influence on customers' banking practices; therefore, the following section discusses gender roles in the KSA.

2.3.2 Gender roles in the KSA

The second aspect of Saudi culture that is important for the present study is gender. The predominant binary view of gender as simply comprising 'male and female' may be partially inspired by a statement in the Qur'an that God "created everything in pairs" (51:49). This may form the basis of the Islamic doctrine that every person is either male or female and partially explains the illegality of homosexuality in the Kingdom. Since September 1932, any homosexual act may be punished by death; therefore, lesbian, gay, bisexual and transgender (LGBT) people in Saudi Arabia tend to prefer to keep their sexual orientation secret (Moftah 2015, Bearak and Cameron 2016, Equaldex 2016). However, a particular problem identified in the KSA is that of misinterpreting the sex of newborns, which can occur because of defects in an infant's external organs. There is growing demand for treatment of such children as they grow up (Whitaker 2016). In such cases only, the Saudi health ministry announced in 2014 that all gender-correction operations in the kingdom, whether in private or public hospitals, would require the ministry's prior approval (Arab News 2014) and this would undoubtedly ensure that

they complied with religious criteria. Accordingly, the term ‘gender’ is used in this thesis to refer to the male/female dichotomy.

As Islamic principles are stated in the Qur’an and the Prophet’s Hadith, it is worth mentioning that neither the Qur’an nor the Hadith forbids women from joining in public life. However, the Qur’an does warn that the mixing of the sexes could lead to “seduction and the ‘evil consequences’ that might follow” (Almunajjed 1997). Jurists in the KSA have responded by restricting tightly all interaction among unrelated men and women (Del Castillo 2003). Therefore, gender segregation is fundamental to Saudi society (Deave 1980) and is even applied to foreigners when on Saudi soil (Mirza 2008). Culturally, segregation by gender extends to almost all aspects of private and public life in the KSA, including schools, universities, mosques, government facilities and even bank branches, as described in Section 2.3.3.2 (Al-Turki 1987) (Baki 2004). According to Deif (2008), Saudi Islamic scholars maintain this norm with the social-religious justification that “*loose interaction across gender lines is one of the major causes of fornication, which disintegrates society and destroys its moral values and all sense of propriety*” (p. 13).

Deave (1980) notes another consequence of gender segregation in the KSA: Saudi culture assumes that the household is likely to be headed by a man, that male relatives must be responsible for solving any difficulties that may arise and that they are also responsible for family members’ behaviour. It is therefore crucial to monitor the behaviour of family members to maintain family honour, whose significance is clear from the idea that a family which loses its honour loses everything (Del Castillo 2003). This notion of family honour is strongly associated with the chastity of female members (Del Castillo 2003) (Lipsky 1959). That is, any improper behaviour by a woman may “raise suspicion or provoke an attack on her morality, the consequences of which the

entire family would suffer" (Arebi 1994), p. 40). This, in turn, has resulted in the need to prevent the disclosure of female identities, voices and photos (Arebi 1994) (Jamjoom 2009), the main purpose being to make it difficult for women to lose their sexual virtue (Mackey 2002). In addition, by law and custom, men are responsible for women (Deave 1980) and Islamic law states that it is a man's responsibility to provide financially for the household and specifically for his wife, whose participation in funding household expenditure is optional (Alosaimi 2009).

A Saudi female must obtain her male guardian's consent to perform many daily activities, including joining a university, having a job and travelling outside the country (Deif 2008). Because of the strong belief in the need to preserve female chastity, women in the KSA are not permitted to drive and those who defy this ban risk jail; therefore, women must use vehicles driven by a chauffeur or a close male relative (Yamami 1996). Saudi cities rarely have reliable public transport networks and where there are buses, women must use a separate entrance at the back and occupy designated seating (Jerichow 1998).

The gender segregation that pervades Saudi culture also affects government documents such as the national identity (ID) card. This is credit-card sized and contains a 2.86 megabyte optical strip and a contact chip to store data, as well as fingerprints and a facial image. Any Saudi citizen—male or female—with a national ID card will typically use it to prove their identity. However, some women do not have one, so to prove their identity they must use a family ID card containing information on the male head of the

household and his facial image; it also contains information on his wife (or wives)[2] and the names of unmarried daughters and of sons under 15 years old, but their images are not recorded. A male Saudi citizen will typically be issued a national ID card when he reaches 15 years old, but this has less often been true for a woman, for two reasons: 1) because a man needs a national ID card to apply for a driving licence, whereas it is illegal for women to drive, and 2) because of the social pressure arising from the stigma of revealing a woman's image to a man who is not her *mahram* (a male relative whom she would be ineligible to marry). This can result in a male guardian not giving his written consent, which is a requirement for a national ID card to be issued to a female, obliging her to rely instead on the family ID card where her image is not recorded. One implication of the extension of gender segregation to national ID cards concerns the use of banking facilities by a female customer who does not have such a card, as discussed in details in Section 2.3.3.2. However, as recently as 23 November 2016, a new law declared that all females aged 15 years and over must be issued with national ID cards (Thakefni 2016).

These issues of male guardianship over women, the ban on women driving and the need for the guardian's consent rank the KSA high on the list of countries lacking equality between the genders (McKinsey Global Institute 2015). In January 2013, in a move to reduce gender inequality and towards empowering Saudi women, King Abdullah

---

[2]According to Islamic and Saudi law, if a man has the physical and financial ability, then he can be married to up to four women at the same time.

unexpectedly announced changes to the Majlis Ash-Shura (the Consultative Assembly of Saudi Arabia), ensuring that 20% of its seats were reserved for females. The Majlis Ash-Shura is similar to the parliaments of other countries, but its members are appointed by the King. It has 150 members, all of whom were male before this announcement (Majlis Ash-Shura 2015) (SPA 2015). The restructuring of the Majlis is ongoing and it is hoped that the proportion of female members will increase further. In addition, Saudi Vision 2030, a major national transformation programme announced in 2016, includes an important reference to providing equal opportunities for men and women and increasing women's participation in the workforce from 22% to 30% (Saudi Vision 2016). Conversely, the Saudi Vision programme does not point to any changes in male guardianship over women, to the driving ban or to the need for the guardian's consent, yet these issues of gender equality appear to be in transition, as evidenced by the volume of contributions in 2016 to social media, especially Twitter. The KSA has a particularly high number of Twitter users, at approximately 1.9 million, amounting to 50% of the total number of Arab users, despite Saudi Arabia being only the sixth-largest Arab country in terms of population (KSA Transition to Knowledge Society 2014). In mid-2016, repeated hashtags trended for several days demanding an end to male guardianship and the granting of greater freedom of action for women, including full economic freedom. Some tweets called for the state to differentiate between protective guardianship and controlling guardianship, claiming that the former is founded on Islamic rules, while the latter merely reflects Saudi norms. The debate was intensified when on 8 September 2016 Sheikh Abdullah Almanee supported this distinction in Okaz, a major Saudi newspaper, claiming that Islam maintained full freedom for women and that the notion of guardianship applied only in marriage (Al Dabis 2016). Although Dr Almanee is a prominent member of the Saudi Council of Senior Scholars,

which advises the King on religious matters and is considered the highest religious body in the KSA, many Saudis appear not to accept the validity of his conclusions. Another campaign, in favour of allowing women to drive in Saudi Arabia, called upon women to defy the driving ban on 26 October 2013, but it failed to gain widespread support after firm warnings from the Saudi Ministry of Interior. After this protest, which was the third of its kind since 1990, a number of women were arrested or lost their jobs.

The next section gives an account of the history and the present situation of banking in Saudi Arabia.

2.3.3 Saudi bank system

The third important element of the background to this banking-related study is the Saudi bank system itself. This section will provide the reader with important information needed to understand the banking practices of household customers discussed in Chapter 4, especially information about Saudi banking and the facilities and services it provides to household customers.

Banks in the KSA are Islamic banks, which are supposed to adhere strongly to the principles of Islamic law, derived from the Holy Qur'an, the Hadith of the Prophet Muhammad (Peace be upon him) and the juristic reasoning (*ijtihad*) of Islamic scholars (Kamali 1999). Haron (1997) explains that

> *…while making profit from business is allowable in Islam, the accumulation of profit without utilization for the betterment of the community is forbidden… Islamic banks are expected to be more sensitive to the needs of society, promote more social programs and activities, and make contributions towards the needy and poor families*.

However, the activities of Saudi banks concerning profit and interest are matters of finance and business which, as explained in Chapter 1, Section 1.1, are beyond the scope of this thesis. This study focuses on those aspects of the Saudi banking system related to interactions between household customers and the banks' systems.

The following subsections take in turn a historical and a contemporary view of banking in the KSA.

2.3.3.1 Saudi banking history

The history of banks and bank systems in the KSA started in the early 20th century with a few foreign-based trading houses (including a trading arm of the Algemene Bank Nederland) and money changers, which provided most of the finance-related services (Saudi Arabian Monetary Agency 1999). Their main function was to serve the major sources of finance in the Saudi economy: the trading community and pilgrims (Saudi Hollandi Bank). After that, foreign banks started entering the market, for various reasons, including the discovery of oil in 1939 and the subsequent inflow of royalty revenue into government coffers. Following the Second World War, there was a surge in oil demand and thus in production, causing government revenues and expenditure to rise rapidly. The French Banque de l'Indochine and the Arab Bank opened branches in Jeddah in 1948, followed in 1950 by the British Bank of the Middle East, the National Bank of Pakistan and Bank Misr of Egypt, which together with the local money changers provided banking services such as deposit taking and lending (Saudi Arabian Monetary Agency 1999).

The main aims of the Saudi government in creating the Saudi Arabian Monetary Agency (SAMA) in October 1952 were to establish a stable monetary mechanism and to stabilise the currency. A type of paper money, the 'pilgrim receipt', was gradually

introduced in the 1950s, its value supported by foreign currencies and precious metals. The decade ended with low inflation, a fixed rate of 3.75 Saudi riyals (SAR) to the US dollar, higher foreign currency reserves and a normal paper currency (Saudi Arabian Monetary Agency 1999). The Banking Control Law, issued in 1966, gave SAMA broad powers of supervision (Al-Suhaimi 2001) and the authority to issue rules and regulations, pursue violations and recommend institutions for new licences. The 1970s ended with banking depending on expatriates, because insufficient suitably qualified Saudi nationals were available to fill vacancies. SAMA addressed this shortage during the 1980s by encouraging the banks to train Saudis and to develop their information and communications technology (ICT) capability. Meanwhile, the national authorities introduced various mechanisms for strengthening the financial markets and the technological underpinnings of Saudi banking. The system was comprehensively modernised, which involved connecting Saudi banks to the SWIFT payment network, introducing a national network of ATMs from which customers could access their accounts and establishing a system of debit, credit and charge cards. All Saudi banks were obliged to respond by investing in ICT and improving both their back-office and front-office operations. In 1997, the EFTPOS system was set up, along with an advanced electronic share trading and settlement system, which enabled same-day settlement (Saudi Arabian Monetary Agency 1999).

2.3.3.2 Saudi banking today

The Saudi banking sector now consists of 12 local banks supervised by SAMA. Under the religious and cultural constraints mentioned in Section 2.3, these all have separate men's and women's branches; access to the latter is limited to female employees and female customers.

Since the beginning, women have had access to bank branches to open accounts and to manage their money as they please (Entendahod 2015), in line with their several economic rights, such as the right to work, as stated in the Labour Code, Chapter 9 (Saudi Arabia Ministry of Labor 2015), the right to inherit, and the right to manage their own businesses. In addition, widows and orphans receive a monthly allowance from the government. Before the introduction of separate branches for men and women, bank branches served customers of both genders, but the fact that that all of the employees were males was inconvenient and violated female customers' privacy, because each woman would normally have to be accompanied by a mahram, to whom all of her banking activities would be exposed. The opening of women's branches, offering speed, efficiency and flexibility of financial services, was an important step in the provision of services for women in the KSA. This development was introduced gradually, with Al Rajhi Bank opening its first ladies' branch in 1979 (Al Rajhi Bank 2014), while the Bank of Holland did not do so until 1999 (Saudi Hollandi Bank). Despite this improvement, women's physical access to banks and financial services is still difficult (Cotula 2002), due to the limitations on movement mentioned in Section 2.3.2. The participation of females in the Saudi banking sector has continued to grow: women now account for 18% of the banking workforce and females have recently been appointed to important positions in several banks. In August 2013 the National Commercial Bank (NCB) appointed Lama Ghazzaoui as chief financial officer and senior vice-president; Maha Mohammad Al-Sudairi recently took over as board secretary and chief governance officer of Saudi Hollandi Bank; and in March 2014 Sarah Alsuhaimi became chief executive and a board member of NBC (Timewell 2014).

As summarised in Figure 2, the current KSA banking infrastructure includes gender-segregated bank branches, ATMs, EFTPOS, cheques, ATM cards (a special type of

debit cards that can also be used for EFTPOS, but not for online shopping) and credit cards. Banks offer different kinds of account (running account, joint account, loans, or savings account), online banking, telephone banking and mobile banking. The security mechanisms differ among these channels and from bank to bank.

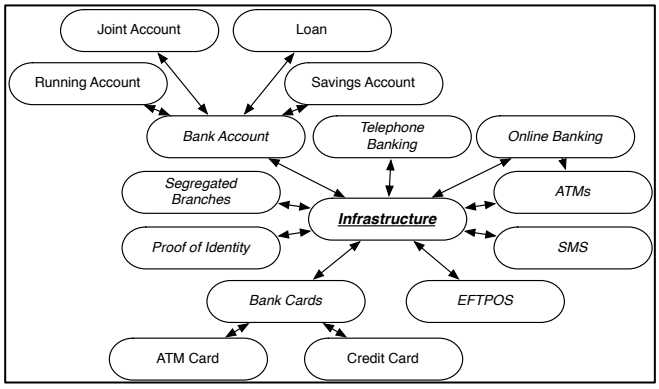


Figure 2: Banking infrastructure and services in the KSA

In order to make use of banking services in a branch, the customer must first prove his/her identity by presenting a national ID card, proof of identity being a requirement of SAMA rules (SAMA 2012). However, as mentioned in Section 2.3.2, some female customers do not have a national ID card, so to prove her identity such a customer must use a family ID card, which does not include her facial image, and engage a relative or a female friend (as women are not allowed to be accompanied by unrelated males) with a national ID card to support her claim. This may allow women without national ID cards to prove their identity, but it is open to the threat of impersonation, as emerged from the data and is discussed in Chapter 6, Section 6.3.2.1. However, a law passed in November 2016 now requires that national ID cards be issued to all females aged 15 years and over (Thakefni 2016).

The rest of this section describes the current situation of the Saudi banking sector and reviews published studies of the use of banking services in the KSA as essential background to the banking practices of the participants in this study.

One of the services offered by Saudi banks and widely used by their customers is SMS notification, where the bank system sends an SMS to the account holder acknowledging each transaction carried out on the account, e.g. money transfer, deposit, withdrawal and online access.

Evidence that Saudi bank customers prefer the use of electronic channels to visiting bank branches is reported by Al-Somali et al. (2009), who found that only 9% of respondents visited a branch to conduct their banking transactions; a report by SAMA indicates that 90% of total bills in 2011 were paid through electronic channels as compared to 43% in 2007 (Monthly Statistical Bulletin 2012, cited by (Sohail and Al-Jabri 2014).

- Cheques

Another service offered by Saudi banks is the use of cheque books, which can be issued to household customers. However, confidence in this facility is marred by the volume of uncovered ('bounced' or 'rubber') cheques, of which about 158,300, valued at about 14.8 billion SAR, were written up to the end of November 2009, according to the statistics issued by the Saudi Credit Information Company (Alhossaini 2011). This phenomenon, arising for various reasons such as insufficient credit, is reflected in the low usage of cheques in the KSA and may explain why none of the participants in this study reported using cheques, as mentioned in Section 4.5.

- Bank cards

The ATM cards issued by Saudi banks are more popular than credit cards, being used in around 1.56 million daily transactions, of which over two thirds are ATM withdrawals (International Monetary Fund 2013). One of the reasons for the popularity of ATM cards over credit cards is that the former are debit cards, whose use is unaffected by the

long-running debate as to whether the prohibition of interest under Islam extends to credit cards. Many view Saudi society as a model of Islamic organisation, within which the two most holy places are located. The country's basic law is derived from the Quran, which prohibits interest being paid or demanded, but views differ on applying this to the use of credit cards. Some argue that settling the full balance each month, thus paying no interest, meets the religious stipulation, but others say that because a person signing up for a credit card accepts the possibility that interest will be paid, which is in itself counter to Islam, then the actual payment of interest is not sufficient to negate the prohibition. Such arguments made many Saudis reluctant to take up credit cards when they were first introduced. However, this attitude seems to be changing gradually, so that around the turn of the millennium, the national credit card market was reported to be growing at about 160% per year. In 2004, the annual volume of credit card transactions in the KSA was around 2.4 billion SAR ($640 million). At the end of 2009, there were 12.16 million eligible and active cards issued by the commercial banks (one active card per 2.2 head of population) functioning as both ATM and EFTPOS cards (BIS 2012). This would explain why only three participants in this study held credit cards, as shown in Section 4.5.

A further subject related to the use of bank cards is online shopping. Abdulmuhmin and Alabdali (2004) found that online shopping was not popular in the KSA; only 26.6% of respondents indicated that they had bought products over the internet at any time between December 1998, when public access to the internet was first allowed by the Saudi authorities, and 2004. Alsharif et al. (2013) note the relatively low use and adoption of online shopping despite the large number of internet users and increasing experience of computers and the internet among Saudis; in 2013 there were 16.5 million internet users in the KSA and internet penetration was 55.1% of the population (Madar

Research Group 2014). Alsharif et al. (2013) found that 49% of their respondents had never bought online, 17% rarely did so and only 12% regularly shopped online. Similarly, a more recent study found that most Saudi customers were not habitual online shoppers, because their affection for the social aspects of shopping and contact with colleagues and friends were more significant than the technical advantages of shopping online (Alam, Malik et al. 2016). This would explain why only four participants in this study had ever shopped online, as shown in Section 4.5.

- ATMs and EFTPOS

Recently, some 10,885 ATMs were in daily operation in Saudi Arabia (BIS 2012, International Monetary Fund 2013). During 2010, more than a billion ATM transactions took place to a total value of 468.4 billion SAR. On average, each card was used at an ATM 8.4 times per month for cash withdrawal, account information or supplementary services (bill payment, share-dealing, statement requests, etc.). Some 80,505 point-of-sale terminals are also in operation across the KSA. In 2010, there were 151.18 million EFTPOS transactions in the country, to a total value of 71.86 billion SAR. A survey of bank customers in the KSA found that ATM usage prevailed as the main means for 48% of respondents to carry out banking transactions (Al-Somali, Ghlami et al. 2009). It is to be expected that ATM withdrawals will far outstrip payments through other channels, given the large number of transactions for which payment must be in cash and cannot currently be made through another channel e.g. paying taxi fares, buying newspapers, using local shops, or providing children's school money. In a study of demographic differences in usage and attitudes toward the Saudi Arabian EFTPOS system, Abdulmuhmin (1998) found that high-income-earning Saudi males were more likely to be users of EFTPOS than any other demographic group of bank customers. He found that 58% of consumers reported owning at least one credit card; nine years later, this

had increased to 63%, according to (Abdulmuhmin and Umar 2007), who found that credit card ownership in the KSA was higher among females and positively related to income, education, age and attitude towards the religious aspects of credit card debt. Interestingly, their study found that the three major uses of credit cards among respondents were for internal travel, for emergencies and to obtain additional liquidity. In another study, Abdulmuhmin and Alzamel (2001) found that Saudi retailers believed that the presence of EFTPOS in a retail store encourages customers to spend more and reduces the incidence of cash theft, but that it also increases the time spent by customers at the checkout counter and leads to congestion at the checkout. Despite this inconvenience, the above advantages would explain why the use of ATM/EFTPOS cards was found to be the most common banking practice among participants in this study, as reported in Section 4.5.

- Online and mobile banking

Online banking is offered by all banks in the KSA, providing access to accounts and to most of their services. There are two ways to register for online banking via a bank's website (Figure 3). Most banks use the first of these methods, which involves choosing a username/password, providing information including the customer's mobile number, account number, card number and card PIN, after which a one-time authentication code is sent to the customer's mobile. Having registered, the customer can access the account online by providing three pieces of information each time: the username, password and a different one-time authentication code which is sent to the mobile number for each access.

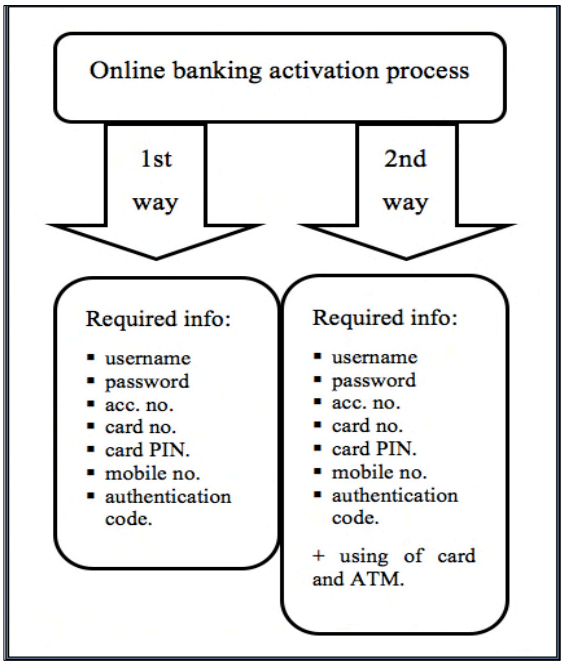


Figure 3: Online banking registration process

A few banks use the second method illustrated in Figure 3, which is exactly the same as the first with the addition of a final step, where the customer must use an ATM to activate the service. This obviously increases the level of security, but it also reduces the usability of the service for female customers, who suffer from limited mobility, as explained in Section 2.3.2.

The quality of the internet connection is an essential component for any internet-based application. Internet use was first allowed in Saudi Arabia in 1998 and is controlled by the Saudi government, which uses firewalls to block users from accessing material that violates Islam or encroaches on Saudi culture (e.g. pornographic sites). Sathye (1999) used internet access as one of the factors affecting the adoption of online banking in her research. Without a proper internet connection, online banking is not possible. Almogbil's (2005) study confirms that there is a significant relationship between the speed of connection and the use of online banking services. He found that 63% of customers in Saudi Arabia accessed the internet through dial-up services. Al-Somali et

al. (2009) found that only 22% of respondents indicated that online banking was their preferred method for performing banking transactions. One factor that the authors invoke to explain why 78% of respondents preferred some method other than online banking is that most of the respondents had never received information about online banking from their bank; the implication is that low awareness of online banking is a critical factor in causing customers not to adopt or use online banking. Their conclusion is that Saudi commercial banks should use means including leaflets, brochures, SMS messages and email to promote online banking, thus educating existing and potential customers about its benefits and encouraging its use by increasing their familiarity with the service. In a study of Australian customers, Sathye (1999) found that participants were unaware of the benefits, advantages and disadvantages associated with online banking. This is consistent with the finding of Howcroft et al. (2002) that lack of awareness of the online banking services offered by banks and their benefits explained consumers' reluctance to use them. It is also related directly to one of the findings of this thesis, reported in Sections 5.3.1.1 and 5.3.3. All of these factors contribute to explaining why few participants reported using online banking, as noted in Section 4.5.

Another service provided by Saudi banks is mobile banking. A study by Sohail and Al-Jabri (2014) shows that mobile banking users in the KSA tend to be young, educated males, not necessarily with high incomes, and argues that banks should target these groups of customers. Bank customers need to use the same account credentials as for online banking to access the mobile banking services (Al-Jabri and S. 2012). As mentioned previously, online banking was not widely used by participants in this study and this might be one of the factors affecting the adoption of mobile banking, which none of the participants used, as shown in Section 4.5. The limited use of mobile banking cannot be related to the general level of smartphone use, since there were 22.2

million smartphone users Saudi Arabia in 2016 (Statista 2016). Al-Husein and Sadi (2015) examined factors affecting the adoption of mobile banking in the KSA and found that quality of internet connection, the degree of awareness among customers, trust in mobile banking, and resistance to change are among factors with a significant impact on consumers' attitudes towards adopting mobile banking.

- Telephone banking

Saudi banks also offer a telephone banking service, which has contributed to substantial cost savings for the banks and greater convenience for increasingly sophisticated consumers. With the growth in telephone banking, any activity that can be handled in a branch (with the exception of withdrawing cash) should ideally be available via the telephone. In addition, adoption is intensive when services are made easy to access and to use. The telephone banking facility reduces the time customers must spend travelling to and from a branch, provides convenience in making their transactions and improves the speed of the service (Marr and Prendergast 1991). As a result, customers enjoy more time and place utility and perceive more value for the service. A study by Alashban and Burney (2001) found that Saudi consumers' income levels and education were decisive in their adoption and usage of telephone banking. Based on these findings, bankers should concentrate the marketing of their telephone-based delivery systems on more affluent and educated customers. (Al-Somali, Ghlami et al. 2009) found that 21% of bank customers in the KSA who responded to their survey used a telephone banking service to perform transactions. This would explain the common use of telephone banking among participants in this study, as detailed in Section 4.5. However, registration for this service requires the customer merely to provide an account number and national ID number and to choose a password; the process does not require physical authentication of the account holder's identity.

2.3.3.3 Saudi banking policies

As mentioned before, bank systems can be treated as socio-technical systems, where computer technology is used to offer technical services that millions of bank customers use daily. To guide users of bank systems in learning which activities are acceptable when using bank technology and which are not, banks issue policies and regulations. Policies govern practices, serving as a guide in the decision-making process when using a system (Sloman 1994). Bank systems offer a range of services to household customers and the recent evolution of technology for financial transactions has moved towards supporting cashless transactions; however, the focus here is on conventional banking, because this is still the predominant form in the KSA. The policies and regulations of Saudi banks regarding household customers will be explained in Chapter 7 (Section 7.3), as they constitute an essential element in the conceptual framework to be presented in that chapter.

All of the studies reviewed above have focused on bank customers as individuals, while in this thesis the unit of analysis is household bank customers; therefore, the next section discusses the terms ‘family’ and ‘household’.

2.4 Families and Households

Anthropologists often use the terms ‘family’ and ‘household’ loosely without attaching rigorous definitions to them, although at the same time they recognise the difference between the two (Yanagisako 1979). The difference that appears to be accepted by anthropologists is that the essential defining features of membership of family and household respectively are kinship and propinquity (Bohannan 1963, Bender 1967, Buchler and Selby 1968, Bender 1971, Hammel and Laslett 1974, Cohen 1976). For example, Bender (1967) argues that the concepts of family and household are both

"logically distinct" and "empirically different" (p. 493). The logical distinction is that family membership depends on kinship, while the household is based on geographical closeness or shared residence. Yanagisako (1979) adds that families "are as much about production, exchange, power, inequality, and status" (p.199). An examination of the literature in different fields shows that some researchers have used 'household' to refer to people living "under one roof" (Dallos 2003), while others have included people who are temporarily absent and dependent children away at school (Martins 2007), but that most use it without any specification and as a synonym of 'family' (Ranjan 2000, Vyas 2003, Cohen 2011, Lee 2011). A household in the KSA usually consists of a married couple and their unmarried children of either sex; it is against the rules of Islam and culture for an unmarried couple to live together or to have children. Each household is usually headed by a male, while the role and position of each individual in this type of structure are defined according to sex and age (Al-Garni 2000). Some features of households in the KSA, such as size and economic characteristics, have changed over time, for various reasons. The average household size fell from 6.08 persons in 1992 to 5.84 in 2010 (AlBawaba 2010). In general, the economic level of households in the KSA has improved, especially since the oil revolution of the 1970s and 1980s. Recently, the KSA was ranked first in the world in terms of density of ultra-wealthy households (18 per 100,000), due to the strong national economy (The South Asian Times 2011).

Tribal relations also have a great influence on Saudi life and practices. Islamic principles and traditions are closely intertwined with a historical tribal culture, resulting in the modern structure of the KSA. A Saudi tribe is a collection of families who share the same surname and for which there is a leader or head of the tribe. The tribal system retains a fundamental influence on Saudi life and practices, whereby a person's tribe is

seen as a source of support and security. In 1932, King Abdul-Aziz united the mutually hostile tribes of Arabia into a single nation (Anthony 2005, Anthony 2006). There was a further transformation in the 1970s, as the oil boom resulted in the rapid growth of the urban population from 16% of the total in 1950 to 49% in 1970 and 80% in 1990 (Krimly 1999). At the same time, the membership of nomadic tribes, which had formed a majority of the population in the early 20th century, fell to less than a quarter by 1993 (Champion 2003). The rate of urbanisation in the KSA was roughly double that of other Arab states such as Jordan, Tunisia, Egypt and Morocco (Arab Monetary Fund 1991) and although the tribes still exist in Saudi Arabia today, they have less impact than before.

A few studies of the use of computer technology have taken the household as the unit of analysis. For instance, the VOME project studied users' privacy and how they used ICT within family settings across the UK. Coles-Kemp and Ashenden (2012) recruited pairs of granddaughters and their grandmothers, some of whom were great-grandmothers, to participate in a number of family workshops. They concluded that it is vital to understand end users and the contexts that determine their attitudes and behaviours from their own perspective, rather than that of the researcher's imagination. Another example where the household was the unit of analysis is that of research into bank system use carried out by Singh (2006) (2008) and Singh et al. (2006) (2007a) (2007b). These studies investigated the financial and banking practices of Australian households by interviewing couples, or individual members of couples in some cases. Their findings highlight the need to go beyond the individual use of digital banking systems to shared use in the household context; otherwise the mismatch between bank customers' practice and security design might weaken the security of bank systems. Also interviewing couples used in a study of the using of technology to help and support families

separated by prison to re-esablish and adjust family relationships and roles (Coles-Kemp, Angus et al. 2013, Coles-Kemp and Kotova 2014). The following section discusses the area of human-computer interaction (HCI), which is the area of research that focuses primarily on studying the practices of computer users and the interactions between users and computer systems.

2.5 Human-Computer Interaction

As stated in Chapter 1, the aim of this research is to develop a conceptual framework that can be utilised to evaluate the security of household bank customers in the Kingdom of Saudi Arabia. Constructing the framework required a deep qualitative investigation and analysis of the banking practices of household customers of Saudi banks. The findings of this investigation then had to be integrated with knowledge of the systems operated by these banks. This study therefore falls broadly within the discipline of HCI, which concerns the manipulation and experience of human users when using computer software. This discipline's main goal is to use an understanding of users' actions, motivations and experience to guide the development of new computing technology (Carroll and Campbell 1989), supporting the creation of usable computer systems by generating a knowledge base to be utilised by system designers (Preece, Rogers et al. 1994). Research into HCI explores those factors that affect the interaction between humans and computers. Dourish and Anderson (2006) have shown that any adequate account of computer users' practices must satisfy two requirements: firstly, there must be a deep understanding of the practices and the social and cultural context within which the practices take place; secondly, these practices must be associated with the concepts of risk, danger, trust, secrecy, identity, morality and power that collectively give them meaning.

A commonly discussed successful case of the application of HCI by a bank is that of the UK bank First Direct (Devlin 1995). This company decided to comprehensively profile its customers in terms of their past actions, their needs, expectations and intentions, believing this to be essential in determining what kind of services it should provide. First Direct was launched in 1989, offering its services all day every day, and is a model of telephone banking. More than a million people held First Direct accounts by the end of 1998. It has no branches, doing all of its transactions by computer and telephone. Whenever a customer calls the service provider there is effective two-way dialogue. The company logs all comments, queries and suggestions received, providing direct input into service improvement. As a result, nine First Direct customers in ten say that they are very or extremely satisfied with its service, against a mere 1% dissatisfaction rating. This example of a bank which explored and used the customers' practices and needs to improve the service provided, with the result that the majority of customers were satisfied, strongly supports the need to consider HCI in the banking sector.

In addition, the interaction between a user and an interactive computer system would occur within a specific context that can influence the practices and the motivation of the user. Dix et al. (1998) argue that this wider context may involve factors which the designers of interactive systems cannot control; nonetheless, it is important to be aware of such factors in order to fully understand the problem domain and the users within it. Many studies have sought to identify the factors that might influence users' practices and specifically those affecting security. The related literature can be divided into three main domains, addressed in the following subsections: usability (2.5.1), human values (2.5.2) and social factors (2.5.3). Each subsection discusses the influence of its respective factor on the security of the interaction between users and computer systems.

2.5.1 Usability and security

Schneier (1996) originally argued that a system can best be made secure by using technologies such as the encryption of data. However, he later revised his opinion (Schneier 2000), asserting that "…the fundamental problems in security are no longer about technology; they're about how to use the technology" (p. 398). To move from theoretical to actual secure systems requires taking account of system users; indeed, one of the main elements in building a secure system is the close and concentrated examination of its users (Tognazzini 2005). It has been found that users do not typically focus on security, their main goal being to perform some task (Norman 1998, Renaud 2005). In addition, users' perception of security when doing online transactions depends "on the simplicity of the site and on the availability of user support" (D'Hertefelt 2000). Security system developers must therefore take system users into account and place them at the centre of usability (Karat, Karat et al. 2005) and aligning usability with security (Yee 2004, Cranor and Garfinkel 2005).

On the other hand, Bishop (2005) discusses the belief that having a secure system means that it must employ complex security mechanisms and therefore be difficult to use, whereas the principle of ease of use must be followed to ensure its usability. However, when using a security mechanism such as a password, the user must make it easy to use but difficult to guess (Dhamija and Perrig 2000). Researchers into users' practices have often considered the user as expert (Bishop 2005) or in the role of employee in an organisational context (Friedman and Grudin 1998, Weirich and Sasse 2001, Olson, Grudin et al. 2005, Sasse and Flechais 2005, Inglesant and Sasse 2010a). For instance, Inglesant and Sasse (2010a) explored the use of passwords in the workplace and found that it affected users' productivity and ultimately that of the organisation.

It is indubitably important to ensure the usability and security of experts and employees in organisations, but considering household users is also important, as proven by the examples of Sony (Zetter 2011) and Yahoo! Voices (Goldberg 2011, Hunt 2012) mentioned previously.

Returning to Schneier's opinion (2000) mentioned above, the usability of a technology is a fundamental factor influencing the security of that technology. Furthermore, as this technology is used by human beings, their values and social elements are factors influencing users' practices and the security of computer systems; research in these areas is discussed in the following subsections.

2.5.2 Human values and security

Like usability, research has highlighted the importance of exploring human values and beliefs as factors also influencing users' practices. It has been argued that if those designing the security of a computer system ignore these factors, there is a risk of undermining or subverting that security. For instance, Friedman and Grudin (1998) write:

> *The common good of our information infrastructure depends on designs through which users can establish and maintain trust and accountability. Without preserving such human values, users will be reluctant to embrace this infrastructure as a means for conducting their daily affairs – commerce, communication, health, work, and education* (p. 213).

They emphasise the importance of human values such as trust for the effectiveness of the information infrastructure that will be used in daily affairs. Having explored the relevant literature, Williamson (1993) argues that trust has many meanings, which may cause confusion, whereas it is clearer what is meant by "lack of trust". This is especially

true in cases where information availability is limited (Singh and Slegers 1997). Trust is found to play an important role in shaping people's willingness to share information within an organisation (Olson, Grudin et al. 2005) and although trust relationships motivate the breaking of security policies and practices, adhering strictly to security policies can undermine social relationships between co-workers (Sasse and Flechais 2005). Thus, security designers in organisations must consider trust, because ignoring this human value may undermine or subvert the security of the system. However, it is important to distinguish between security and trust, because even "usable security" is not always a sufficient condition for trust. Making this distinction, according to Bollier (1996), means distinguishing between

> *...issues of 'hard trust,' which involve authenticity, encryption, and security in transactions, and issues of 'soft trust,' which involve human psychology, brand loyalty, and user-friendliness...* (p. 21).

Important studies have discussed trust and the use of electronic money (Luhmann 1988, Lee and Allaway 2002, Hsiao 2003, Barr, Knowles et al. 2004, Liu, Marchewka et al. 2005), relating this to issues of soft trust. On this topic Singh and Slegers (1997) found that in order to be comfortable in using a service or a channel, the user has to feel that he or she is in control of the information. Controlling the sharing of personal information and presenting our version of ourselves is an aspect of the human value of privacy (Agre 1998, Palen and Dourish 2003, Singh and Cassar-Bartolo 2004); Karat et al. (2005) state that the intersection of HCI, privacy and security must be considered "a critical area for research amid the backdrop of recent world events" (p. 1). In the banking context, major privacy issues are the fraudulent use of bank cards and the leaking of information such as internet banking credentials, which can lead to the impersonation of an account holder and the loss of money. However, Singh et al. (2006)

assert that privacy in banking should lead to personalisation and users' control over their personal information.

Culture also influences how people behave and practice. Hofstede (2003) classifies Arab societies as collectivist culture rather than individualist, showing as they do a long-term and close commitment to their family, extended family or extended relationships. Loyalty is critically important in collectivist cultures, overriding almost all social rules, which means that it is pointless to adopt an information security standard without customising it to the culture concerned. AlKaabi (AlKaabi 2014) cites Chadwick (2002) as stating that various issues which are usually considered private are shared in Arab culture and that this characteristic can extend to making the privacy of the individual subordinate to the community's interests or those of the family. Respect for seniority also favours older people in Arab societies (Koocher 2009), where the invocation of seniority may cause the inferior party to divulge his or her private details. An interesting study by AlKaabi and Maple (2012) found that Arabs were willing to share 73.5% of their information with certain people (such as credit card or social security details with trusted colleagues, best friends, siblings, spouses, or parents), keeping only 24.3% for themselves, examples being transgressive behaviour such as accessing pornographic images. There was uncertainty about sharing or withholding only 2.2% of information, such as credit card or social security numbers with extended family members. This attitude towards sharing sensitive information is believed to have a strong relation with cultural attitudes. A subsequent study (Alkaabi and Maple 2013) of the sharing of passwords for online accounts in Gulf Cooperation Council countries found a significant level of sharing of sensitive information, which eventually put users' accounts at risk. It identified credential sharing with co-workers and family members as one of the information security awareness issues that needed to be dealt with.

A final significant value discussed here that has been found to affect users' practices is religion. Many researchers have explored the role that religion plays in consumer purchasing behaviour. Mokhlis (2006) reports that the buying behaviours of Muslims gravitate around the culture, norms, attitudes and values influenced by their religion. A study by Bonne et al. (2007) suggests that the decision processes of Muslims differ from those of non-Muslims, a suggestion supported by the results obtained by Shaari and Afirin (2010), who add that religion dictates the lifestyle of religious individuals. This finding is in turn confirmed by Khraim (2010), who agrees that individuals' lifestyle depends on their level of religiosity. Souiden and Rani (2015) have also shown that a person's fear of divine punishment can make him or her see Islamic banks more favourably, as can the strength of his or her belief in Islamic laws. Islamic banks may thus suggest in their literature that it is sinful to obtain the services of conventional banks or interest-based credit. The early scepticism of the Saudi population regarding credit cards, reflecting the religious sensitivity of the connection between credit and interest, has been discussed in Section 2.3.3.2. (Abdulmuhmin and Umar 2007) offer evidence of a gradual change, however, recording that 63% of consumers now owned one or more credit cards, up slightly from the 58% recorded by Abdulmuhmin (1998).

Notwithstanding the obvious effects on Arab countries of globalisation and Western mores, Islam remains the most prevalent influence, affecting almost every aspect of daily life and practices. Among the values strengthened by Islam are honesty, loyalty, flexibility and trust (Obeidat, Shannak et al. 2012). Al-Hamar et al. (2010) maintain that this introduces a social vulnerability which those concerned with information security must be aware of, in the context of the rapidly growing use of technology and the internet. Any conflicts between security practices and religious beliefs may result in the subverting of security, according to Algarni (2013), who carried out an in-depth

study, observing the practices of government representatives in response to incidences of cybercrime, then interviewing them in their workplaces. He found that Saudi governmental organisations appeared unready to confront and control the problem, citing the influence of religion as preventing government representatives from taking certain security steps, such as gaining access to and using images produced by online surveillance of an ATM to target fraudsters proactively. The reason given is that this use of surveillance techniques would involve *tajassus* (spying), which is clearly forbidden by the Qur'an.

All the above studies confirm that adopting security standards in a computer system without consideration of human values is unlikely to yield the intended results; therefore, there is an urgent need to investigate the impact of these values on the practices of Saudi bank customers and consequently the security of both customers and banks. Such an investigation would be of considerable value to bank developers in general and Saudi developers in particular, helping them to understand this impact and consequently to develop bank systems with improved security.

The next subsection will discuss different social factors influencing the security of computer systems.

2.5.3 Social elements and security

As shown in the two previous subsections, usability and human values must be considered as factors influencing users' practices and the security of computer systems; researchers have highlighted the risks of ignoring these factors as the undermining or subverting of the security of the system. In addition to these factors are social elements such as age, level of education, income and gender, which have been found to affect the interactions between humans and computers. In the area of banking, Filotto et al. (1997)

investigated the demographic characteristics of ATM users and non-users in Italy, reporting a general reluctance among the Italian public to accept the offer of innovative service delivery mechanisms, despite relatively high rates of adoption by young people. Information literacy has also grown, according to these authors, marking the close familiarity of a new generation with computers and the Web, while those who remained less favourably disposed towards technology nonetheless happily adopted telephone banking and similar services. Chan (1997) conducted a study in Hong Kong of the effect of demography and attitudes on how active people used their credit cards. Income turned out to be the variable that most strongly affected how often a card was used, while the attitudes of users were also positively related to frequency of use. Similarly, Saudi consumers' income levels and education have been found to play a vital role in their adoption and usage of telephone banking (Alashban and Burney 2001); however, this study focused on male bank customers only because of the cultural constraints to be discussed in Section 3.4. A Canadian study (Marshall and Heslop 1988) classified ATM users and non-users on five predictors; ATM use was found to be positively related to convenience, positive familiarity with other technology and education, whereas non-users had more social orientation. Meidan (1996) found evidence that the older generation was less receptive to credit cards and that financial constraint was a major factor governing their usage frequency. Related research for the Bank of America in 1995 found that the younger the customers were, the more comfortable they were in utilizing non-branch service delivery systems; conversely, older customers were more attached to the traditional branch system (Barrett 1997). More recently, (Abdulmuhmin and Al-Abdali 2004) found that online shopping was more strongly adopted among older, non-Saudi, highly educated, high-income respondents.

Focusing now on gender, gender studies concern relations between the sexes in the context of various social and political practices (Sjoberg 2009). They deal not so much with how many women obtain government appointments or how many books women write, but rather with the substance of the problems associated with the relationship between men and women as social groups. Gender democratizes the research field of security, makes it more multidimensional and polyarchal, continuing the traditions of the constructivist approach to understanding social processes as the results of various kinds of intangible (cognitive and communicative) practices (Butler 2011). Gender studies make it possible to move away from the state-centred paradigm in the study of security problems and international relations. Gender specialists refuse to view world politics exclusively through the prism of diplomatic relations between states and they draw attention to problems that do not fit into traditional concepts of security. In this sense, gender studies share one of the most important principles of the so-called critical geopolitics: that instead of the security of states it is necessary to talk about human security, a concept that focuses on the community of people, considering them as the main objects of security (Butler 2011).

Some of the studies conducted in the area of gender and security have concentrated on understanding gender differences, while others have focused solely on women. Feminist research has made a significant contribution to understanding the relationship between security and development, especially in postcolonial countries (Wajcman 2010). It is an economic imbalance, from their point of view, that provokes violent, revolutionary actions in the developing countries of the third world (Wajcman 2010). In her book "Feminist Security Studies" Wibben (2011) claims that the importance of varied everyday experience, through the telling of women's stories is that it "*provides a corrective to the generalizing and universalizing tendencies in traditional science that*

work to institute bias and obscure responsibility" (p. 2). To help investigate the effects of gender imbalance in ICT, Webb and Young (2005) adopted a feminist epistemology based on the experience of women working successfully in this field; they conclude that societal expectations around balancing work and family life places considerably more pressure on women than men. Their findings show that family support, especially from partners, was crucial for women in their ICT career endeavours, however, they also found that the extent of this support was less than ideal.

At the intersection of gender, HCI and security, Sieger and Möller (2012) discuss gender differences in the perception of the security of mobile phones, especially on authentication and payment-related features, while Satchell and Foth (2010, 2011) examined the use of mobile technology to maintain users' personal safety at nights by connectivity to closely co-located persons. Yet other studies have described the greater vulnerability of women than men to phishing attacks (Jagatic, Johnson et al. 2007, Kumaraguru, Sheng et al. 2010). Fewer studies have addressed the impact of gender differences on security and ICT within quite different cultural contexts. Recently, however, some authors (Ahmed, Jackson et al. 2014, April, Eunus Ali, Rishta et al. 2015) have discussed how ICT can promote women's personal security and minimise gender harassment in Bangladesh, where women often remain silent about such experiences for fear of shame and social disgrace.

The above work highlights the value of exploring gender issues in ICT and security, helping to provide important insights into significantly underexplored problems, as well as challenging our assumptions about common norms, attitudes and practices surrounding secure system use. A key characteristic of the security of a system is that it is an emergent property: an edifice in which each component needs to behave according to its expected parameters. Within secure systems, security-relevant components depend

on multiple assumptions and expectations about the context of use, both implicit and explicit. Gender and cultural attitudes towards gender roles are key elements of the context of use of a secure system; this thesis explores the relationship between gender and the security of banking systems in the Kingdom of Saudi Arabia.

2.6 Chapter Summary

This chapter has set out the background to the study by considering three domains, beginning with banking systems and services. Next, it gave a detailed description of the Kingdom of Saudi Arabia, focusing on the aspects of Saudi culture that influenced the findings of the research. The Saudi banking sector and its components were then discussed. Finally, it reviewed the literature in the area of HCI security, to which this research is directly related. The following chapter presents the methodological approach taken and notes the challenges of applying it in the research context.

3 METHODOLOGY

3.1 Introduction

As stated in Chapter 1, the aims of this research are to investigate the banking practices of household customers of Saudi banks and to explore how the findings can best be integrated into a conceptual framework associated with the Saudi banking system. Its main contribution is the development of a conceptual framework that can be utilised by developers and security analysts of Saudi banks to evaluate the banking security practices of household customers in the Kingdom of Saudi Arabia. Constructing the framework required a deep qualitative investigation and analysis of the banking practices of household customers of Saudi banks. The findings of this investigation had then to be integrated with knowledge of the systems operated by these banks. The previous chapter introduced the background to human-computer interaction as the research discipline within which the work documented in this thesis is situated and this chapter starts by introducing the methodological approaches to HCI in Section 3.2. After that, Sections 3.3 and 3.4 explain several issues that had to be accommodated

when designing a suitable methodology for this research. These are i) that the collected data must provide a rich description of banking practices, reasons and attitudes, ii) that the construction of the framework must be grounded on these data and iii) that data collection methods must be matched to the unique setting of the KSA. In order to address these issues, much effort was spent on studying different methods of data collection and in choosing and designing a methodology to gather the data necessary for the building of the required framework. The first and second issues are explored in Section 3.3 on grounded theory, then the research context and its complexity are discussed in Section 3.4. Section 3.5 introduces the methods used to collect the data in this context. Finally, Section 3.6 gives a detailed account of the conduct of the research and the challenges faced when using each method.

3.2 Human-Computer Interaction

This research is related directly to HCI, the main goal of HCI research being to use an understanding of the actions, motivations and experience of users to steer the development of technology (Carroll and Campbell 1989), assisting the creation of maximally usable computer systems through the production of knowledge that system designers can use (Preece, Rogers et al. 1994). According to Carroll and Campbell (1989), the key characteristic of HCI is that it is multidisciplinary, overlapping social and behavioural science on one hand and information technology on the other, employing theories and methods from both areas. Thirty years ago, many new scientific ideas entered the HCI mainstream, resulting by the mid-1990s in it encompassing most social and behavioural sciences (Preece, Rogers et al. 1994).

HCI concerns not only the analysis and design of user interfaces and new user interface technologies, but also the enhancement of the work and organisational processes of

technology development in general (Carroll and Campbell 1989). HCI scholars have developed many different methods for understanding the tasks and work practices of organisations and their members, which can be used to apply technology in new ways in support of human activities. The methods that HCI employs include: developing checklists and cognitive walkthroughs, performing field studies and experiments, conducting interviews and surveys, and using a variety of analytic models. Participatory and ethnographically driven designs are both often tested in an HCI context, with users participating in design work and/or having their actual use of new technology studied in order to ensure that real-world use rather than normative description underlies design. The wider physical, social and cultural context within which HCI occurs can influence users' motives and actions. Dix et al. (1998) warn that while designers of interactive systems may have little or no control over elements of this context, they must be aware of them if they are to understand fully the user's behaviour within the problem domain.

The influx of new ideas into HCI has widened the scope of the discipline in ways that are relevant to the research documented in this thesis; the methodology and the tools used to collect data from participants (grounded theory, interviews, focus groups and diary studies) have emerged mainly from the social sciences. These methods are detailed in the rest of this chapter, starting with grounded theory.

3.3 Grounded theory

As mentioned previously, constructing the framework to evaluate the banking security practices of household customers required a deep qualitative investigation and analysis of the banking practices of household customers of Saudi banks. Qualitative research is primarily exploratory and used to gain an understanding of underlying reasons, attitudes and motivations, whereas quantitative research is used to quantify the problem by way

of generating data that are numerical or can be presented statistically (Glesne and Peshkin 1992, Morgan 1996). Therefore, a qualitative investigation was conducted so that the framework would support the detailed reporting and description of the banking practices of household customers, factors influencing their adoption of these practices and the views and opinions of both customers and bankers. To give sufficient and full answers to the research questions posed in Chapter 1, the methodology of the investigation was chosen carefully and several features were considered, for three reasons. The first is that this investigation was exploratory, its main purpose being to investigate a new area where there was no pre-existing theory, i.e. the banking practices of household customers of Saudi banks. We are unaware of any conceptual framework which integrates details of the systems of Saudi banks with the banking practices of their household customers. Secondly, it was to be conducted, as mentioned above, by gathering empirical, qualitative data, which, importantly, would concern both the practices and beliefs of these customers. Finally, the resultant theory or framework should be grounded on the data, not on suggestions or thoughts. For these reasons, grounded theory was selected as meeting its requirements, being a methodology for generating a theory, rather than testing an existing one (Glaser and Strauss 1967), and a means of understanding a problem that has not yet been explored deeply.

Grounded theory is “a research method that involves creating conceptual frameworks or theories by analysing the data collected” (Charmaz 2006), p. 187). It originated with the work of Glaser and Strauss (1967) and requires the researcher to undertake the iterative process of data collection, coding and analysis to provide an analytic account of qualitative data. Saldana (2011) defines a code as “a word or short phrase that symbolically assigns a summative, salient, essence-capturing, and/or evocative attribute for a portion of language-based or visual data” (p. 3). In general, there are three coding

stages in grounded theory: open, axial and theoretical coding (see Appendix 12 for a full list of codes generated). ATLAS.ti, a hermeneutics analysis package, was used as a tool to support these analytical steps (see Appendix 8 for an example of using ATLAS.ti in analysing an interview transcript).

- Open coding

The first stage of coding is open coding, where a code is assigned to each chunk of data, which usually means a small number of sentences. The coder does not use pre-existing categories but closely follows the data, identifies actions in each segment, then applies the codes that are most significant and/or assigned most often in sifting through a large dataset. The coder must decide which codes are most useful in incisively and completely categorizing the data. Finally, he or she should identify the *properties* and *dimensions* of each category: "Whereas properties are the general or specific characteristics or attributes of a category, dimensions represent the location of a property along a continuum or range" (Strauss and Corbin 1998). This means that properties are attributes, while dimensions show how large or important a property is. In grounded theory, the researcher can use open coding to identify where there is a need for additional data, before deciding where to collect them from. Collecting and analysing the data simultaneously is therefore helpful in deepening and extending the research and in the development of categories.

- Axial coding

Next, axial coding involves relating categories to subcategories, then identifying the higher-level phenomena in the data. This is essential for deciding structural and processual matters. The structure is the conditional context of a category or phenomenon, while a process is a sequence of action and interaction that applies to a phenomenon as it evolves. In other words, structure relates to the conditions that explain

the occurrence of a certain event, while process is concerned with the responses to these conditions.

The analysis must relate structure to process, so the first step in axial coding is to identify the *conditions* applicable to each phenomenon in question, whether causal, intervening or contextual. Causal conditions directly influence the phenomenon and are amended or mitigated by intervening conditions, often as a result of contingent events (i.e. ones that are not predicted), while contextual conditions arise when causal and intervening conditions interact; in other words, they occur when causal conditions are mitigated by intervening conditions.

These conditions must be identified so that the network of events that preceded the phenomenon can in turn be specified. The analyst's next task is to identify the *action/ interaction strategies* that people engage in under these conditions, meaning how they react to them, which makes these strategies a good way of relating process to structure. Finally, the coder identifies the *consequences* of applying *action/interaction* strategies in response to conditions.

A category is defined as *theoretically saturated* in grounded theory when no new information of the kinds defined above emerges from further analysis (Glaser and Strauss 1967).

- Theoretical coding

In this stage, the researcher finds and specifies theoretical links between categories, a process known as theoretical coding, which Glaser (1978b) defines as identifying how categories "may relate to each other as hypotheses to be integrated into a theory" (p. 72). The final step is a description of the storyline of the theory, comprised of the key elements and their interrelationships.

Grounded theory also makes use of theoretical memos. During data collection and analysis, researchers will develop ideas or tentative hunches as they write notes on what they have seen and heard. Glaser (1978b) urges them to write down their ideas immediately in the form of memos, while Corbin and Strauss (2008) advise researchers not to see memo writing as wasting time. Its importance lies in the need to keep a record of all ideas so that they are not forgotten or lost. These ideas can then be improved and connected together as the analysis moves forward. Memos have been used in this study and a full list is given in Appendix 12.

3.3.1 Validity of grounded theory

There has been some debate about the usefulness of grounded theory because it lacks repeatability (Morgan 1996), which is an important criterion in a research method to ensure that findings can be generalised to participants in similar situations. Strauss and Corbin (1990) claim that if the data used are comprehensive and if the interpretations and analysis of these data are conceptually broad, then the theory developed must be abstract enough and generalisable to a variety of different phenomena in related contexts. The validity and uniqueness of the grounded theory approach lies in two elements (Glaser 1978a) (Glaser 1992) (Strauss and Corbin 1998) (Whitman and Woszczynski 2004). First, theory is based on empirical data, not on suggestions, preconceptions or thoughts. In addition, data triangulation is used to increase the trustworthiness and validity of the data and to obtain multiple perspectives by using multiple methods of data collection: in this case, focus groups, diaries and interviews. Glesne and Peshkin (1992) describe triangulation as a technique to improve the reliability of the data analysis by using multiple methods of data collection so that the limitations of any particular methodology or the conditions of any of the rounds of collection do not confound the final theory. In addition, to increase data reliability, data

were collected from both household bank customers and bankers, thus providing multiple perspectives. Each of the methods used in the present research was adapted in a certain way (detailed in Section 3.6) to suit the research context as explained in the next section. The second distinguishing characteristic of grounded theory is the constant relation between emergent theory (codes and categories) and new data, until theoretical saturation is reached. This ensures that the researcher always connects any model developed to the data and that it remains close to and grounded in empirical reality (Denscombe 2007).

Grounded theory seems a reliable method of eliciting and investigating users' practices and has been used before by experts in the field for the purpose of grounding the findings on users' practices in reality. For instance, Adams and Sasse (Adams and Sasse 1999) used grounded theory to study computer users' behaviour relating to password systems, while Dourish et al. (Dourish, Grinter et al. 2004) used it to investigate the everyday security practices of users of ubiquitous and mobile technologies; in a third example, Inglesant and Sasse (Inglesant and Sasse 2010b) studied the impact of unusable password policies on users' primary tasks.

Once grounded theory had been chosen as the methodological framework for this research, considerable effort was expended in selecting the appropriate methods to collect data from participants. These are explained in Section 3.5, which presents the methods chosen for collecting the data, the challenges faced and the amendments made to adjust each method to the research context. In preparation for this account, Section 3.4 first presents a detailed account of the context of this research and describes the difficulties and the challenges which can affect the conduct of research in the KSA.

3.4 Research context

The context in which this study set out to elicit information about users' practices was methodologically challenging from the outset for a variety of reasons, including limited foreknowledge of household banking practices and the sensitive nature of the topic of banking activities, arising from the intimate context of the household as the unit of analysis. Another major consideration was that in the context of the conservative and religious culture of Saudi Arabia, specifically the gender segregation practiced in the KSA (Section 2.3.2), it would have been difficult for a female researcher to collect data directly from male participants, which ruled out methods such as face-to-face interviews. These constraints have affected many studies conducted in the KSA; for example, when Alashban and Burney (2001) investigated customers' adoption of telebanking technology in the KSA, they chose to collect data from male respondents only. Other studies in which the number of female participants was significantly limited include those of Abdulmuhmin (1998) into demographic differences in usage of and attitudes to the Saudi Arabian EFTPOS system, and of Abdulmuhmin and Umar (2007) concerning the extent and nature of credit card ownership and usage. Only 6.4% of participants in a study seeking to identify the factors influencing the loyalty of Saudi consumers towards e-commerce (Eid 2011) were female, while research into the adoption of online purchases in the KSA by Abdulmuhmin and Al-Abdali (2004) was dominated by male respondents, at 86% of the sample. To circumvent the gender constraints and to obtain information from female respondents, the authors of this last study adopted an interesting solution. The data collection involved focus group discussions and in-depth interviews. The focus groups were conducted among students of a marketing research course taught by one of the authors (at an all-male university), while students conducted the in-depth interviews with their friends and relatives for

course credits. The latter method was especially geared towards obtaining data from female respondents.

In the studies reviewed above, all the researchers were men, while one of those who conducted a study of the acceptance of online banking in the KSA (Al-Somali, Ghlami et al. 2009) was a Saudi female. Having a male and a female among the research team may help to explain the relatively good gender balance among respondents (44% male and 56% female) to the survey they conducted in public areas like shopping centres, universities and workplaces. It would have been difficult for a male researcher to collect survey data from females in such places, as explained by Abdulmuhmin (1998)

> *It is almost considered taboo for a man to walk over to a Saudi woman he does not know (who will most likely be totally covered) to request her to complete a questionnaire*. (p.4)

One potential way to overcome these constraints in order to collect data from both male and female participants is suggested by Cole (1975) who, as a male ethnographer, could not collect data from female participants; he concludes that a solution "must necessarily await a male-female team" (p.80), where male researchers collect data from male participants and female researchers collect data from female participants. However, a foreseeable feature of such an arrangement is that the research team members must agree in advance on a certain protocol for collecting and analysing the data to avoid any differences which would introduce gender bias into the results.

When methods for collecting data from participants were investigated, it was found that some did not suit this study. For example, Mathiasen and Bodker (2011) discuss the use of exploratory workshops to examine in depth a number of concepts and findings. However, this approach requires a certain amount of foreknowledge of the problem

domain and we did not feel that we had enough information to adopt this method. Moreover, researchers emphasise the importance of directly observing actual and potential users (Karat 1988). However, the delicacy of this investigation and the intimate context of the household made the use of direct observation difficult, if not impossible. Coupled with the sensitivity of discussing banking and financial affairs, this placed multiple constraints on the choice of methodology.

On the other hand, previous work in this area which has aimed to elicit data on the practices of domestic users has used questionnaires to collect data from participants (Abdulmuhmin 1998, Alashban and Burney 2001, Abdulmuhmin and Umar 2007, Al-Somali, Ghlami et al. 2009, Eid 2011, Kaye 2011). For instance, Kaye (2011) conducted a Facebook and Twitter survey about password sharing practices. Whilst providing interesting insights into self-reported password sharing, this approach was reported to have experienced problems in recruiting participants due to the sensitive nature of the topic. Similarly, Alashban and Burney (2001) used a questionnaire to investigate the relationship between bank customers' demographic characteristics and their adoption of telephone banking. However, the researchers acknowledge that the six factors that they selected for incorporation into the questionnaire as potentially affecting customers' adoption behaviour did not fully cover the phenomenon and that in particular, they did not address all of the factors affecting the adoption of telephone banking. Depending upon the approach taken, determining in advance of the study specific factors that have an influence on users' practices makes it less likely that other emergent factors will be identified. In addition, it does not make it possible to determine the way in which the interaction of different factors causes specific practices. It was concluded that a survey would not be an appropriate method.

A study in the KSA comparing the response rates of telephone interviews with those of a Web survey (Al-Subaihi 2008) reports three main findings: firstly, the response rate to the Web survey was significantly lower (approximately 70%) than to the telephone interviews; secondly, although male and female participants had the same level of Internet access, males participated significantly more than females, especially in the Web survey; thirdly, the average response rate of the telephone interviews was significantly above 95% for both genders, whereas that of the Web survey was about 30%.

These findings support the decision not to use surveys and motivated the use of telephone interviews in the pilot study with household customers (detailed in Section 3.6.1.1) and with bankers (detailed in Section 3.6.2). The interview method was adopted because it is useful to investigate a given topic in depth, both eliciting participants' opinions about the topic and discovering why they hold these opinions. The trustworthiness and validity of the data were enhanced by means of triangulation, which involved the use of multiple methods of data collection; thus, data were collected from household customers using focus groups in the second round, then the diary/interview method in the third round. Focus groups enabled the examination of participants' perceptions and concerns by allowing them to create new questions and concepts, while the use of diaries and interviews was important to reflect real day-to-day banking practices, the people involved and their motivations. Each method was adjusted in a certain way in response to the difficulties of collecting data from participants of both genders, as detailed in Section 3.6, which also explains the reasons for choosing each method in turn.

3.5 Research methods

As explained above, three different data collection techniques were used across the three rounds: interviews were used to collect data from household customers in the pilot study and again to collect data from bankers in the second round, when focus groups were used with customers; in the third and final round, data were collected from household customers using the diary/interview method. Each of these methods is introduced in turn in this section, then Section 3.6 details the use of each of them in the present study.

3.5.1 Semi-structured interviews

Because of the balance between the structure and flexibility of data obtained from a semi-structured interview, Gillham (2005) argues that this technique is "the most important way of conducting a research interview". Interviews are useful to investigate a given topic in depth, both eliciting participants' opinions about the topic and discovering why they hold these opinions. In semi-structured interviews, the questions are open; that is, the interviewer directs the interviewee to the research topic but does not guide the answers to match her own expectations. Within this flexible framework, all participants are asked broadly the same questions and are given approximately the same interview time, to ensure equivalence among the interviews (Gillham 2005).

Face-to-face interviews, also called in-person interviews, are "the best form of data collection when one wants to minimize nonresponse and maximize the quality of the data collected" (Dialsingh 2008). Although face-to-face interviews are generally preferred for research into sensitive topics such as the banking practices of households being examined here, telephone interviews were considered more appropriate in this case, for cultural and religious as well as practical reasons (Section 2.3.2). The

telephone medium increases response rates by improving participants' availability (Holt 2010); it removes the need for travel, so reducing both time and cost; it allows participants to remain anonymous if desired; interviewees may feel the process to be less emotionally intrusive; and there may be advantages of physical safety for both researchers and participants (Irvine 2010). The drawback of using telephone interviews is that the researcher is unable to see interviewees' nonverbal responses, which can help in directing the interview. In addition, telephone interviews can be intrusive, as calls are usually made at arbitrary times and may interrupt the interviewee during a meal, for example. Interviews are usually recorded and transcribed, so that the researcher can consult the transcripts to identify repeated words and phrases; this also helps the researcher to recover data that might have been missed in written notes taken during or after the interview (Charmaz 2006) (Rubin and Rubin 1995).

3.5.2 Focus groups

Focus groups are good for exploring and examining participants' perceptions and concerns by allowing them to create new questions and concepts (Kitzinger and Barbour 1998). Focus group sessions are social gatherings, usually of 6-8 participants (Bloor, Frankland et al. 2001). Morgan (Morgan 1998) reports that it can take up to 32 calls or visits to recruit just eight participants for a group. Participants are encouraged to debate the issues and to develop their opinions and thoughts, as in real-world situations (Lunt and Livingstone 1996). A moderator presents the focus of the discussion and helps to elicit conflicting arguments without judging the participants' opinions (Puchta and Potter 2004). The approach used to analyse the data was to categorise quotations from the focus groups into types of description, i.e. concepts, then to compare them against targeted concepts of privacy perspectives (Kitzinger 1995).

3.5.3 Diary/interview

A diary is a document written by an author for personal use to record events and ideas related to his or her personal life, which can be useful in research, providing data relevant to the topic. Researchers using this method usually ask participants to keep a diary for a specific time and give them guidance on what events and ideas are to be included (Scott 2006). Recording these events and ideas daily is very important in order to provide rich data relevant to the research topic. One advantage is that the data may be more objective and generalisable because they reflect real day-to-day events, in contrast to other methods where the data are collected in contrived situations (Rieman 1993). Zimmerman and Wieder (1977) argue for a method of data collection from a combination of diaries and interviews in situations "where participant observation is difficult or impossible, e.g. due to unconventional activities, unsociable hours, or diffuse behaviour within a social scene or space, as was the case in their study of a counter-culture community". This method was useful to gather data "in the wild" (Dourish, Grinter et al. 2004, Inglesant and Sasse 2010b) on the banking practices of household bank customers. These were factual data, such as a log of participants' practices when using bank systems, decisions made and people involved. Snowden (2015) discusses the disadvantages of using diaries, noting that considerable time and effort is required by both participants and researcher to ensure that dairies take on a certain shape that fits the research purpose. In addition, participants may become fatigued with the process if the effort required is complex, the timescale is long, or the frequency of the diary entries is very high. Moreover, Alaszewski (2006) states that diary participants must be trained first to know what to include in the diary and how it should be recorded, and that they will require ongoing support.

This section has introduced the three data collection techniques in turn; the next section explains in detail how each was used in the present research.

3.6 Research in Action

As explained above, grounded theory was chosen as the methodological framework for this study, involving two phases of data collection. In phase one, data were collected from household bank customers in three rounds, each using a different method: semi-structured telephone interviews in the pilot study, focus groups in the second round and a diary/interview method in round three. Table 2 lists demographic information on participants in phase one related to the analysis of the data; for instance, participant's income is related to the motivation coded `little money`, which motivated participants to adopt certain banking practices (for more information, see Section 4.5.2.4).

Table 2: Demographic information on household customers

	Method	**Participant no.**	**Demographic information**	**Age**	**Education**	**Income in GBP**
Pilot study	Telephone interviews	P1 - P6	All participants, three males and three females, were married. Some had been married for only two years and some for more than ten. Two were married to each other but were interviewed separately. All the participants were employed except one, who was the partner of an employee.	**26-35** 2 **36-45** 4	**Bachelor's** 4 **Master's** 2	**<215** 1 **216-2130** 1 **2131-4270** 3
Second round	Focus groups	P7 - P12	*Daughters' focus group*: the main selection criteria were that each participant must be unmarried and still living in her parents' house, to reflect the daughter's role.	**19-25** 6	**Bachelor's** 6	**<215** 6
		P13 - P17	*Sons' group*: none of the participants was married and all were still living with their parents, reflecting the son's role.	**19-25** 5	**Bachelor's** 5	**<215** 5
		P18 - P23	*Wives' focus group*: four participants were employed and two were housewives. The main selection criterion was for the participating women to be married. Some participants had children whilst others did not.	**36-45** 2 **46-55** 3 **>56** 1	**High school** 2 **Bachelor's** 2 **Master's** 2	**<215** 2 **216-2130** 2 **2131-4270** 2

	Method	Participant no.	Demographic information	Age	Education	Income in GBP
		P24 -P 29	*Husbands' group*: five of the participants were employed and one had retired. All were married to reflect the husband's role and not all had children.	**36-45** 3 **46-55** 2 **>56** 1	**High school** 3 **Bachelor's** 3	**216-2130** 1 **2131-4270** 2 **>4270** 3
Third round	Diary/ interview	P30 - P32	*Household 1* comprised a remarried husband, his new wife and his son from the previous marriage.	**19-25** 1 **46-55** 2	**High school** 1 **Bachelor's** 1 **Master's** 1	**<215** 2 **>4270** 1
		P33 - P35	*Household 2*: a widow and two of her sons.	**26-35** 1 **36-45** 1 **>56** 1	**High school** 1 **Bachelor's** 2	**<215** 2 **2131-4270** 1
		P36 - P38	*Household 3*: a widow, her son and her daughter.	**19-25** 2 **>56** 1	**High school** 2 **Bachelor's** 1	**<215** 2 **2131-4270** 1
		P39 - P42	*Household 4*: a husband, both his parents and his wife.	**26-35** 2 **>56** 2	**High school** 1 **Bachelor's** 3	**<215** 1 **216-2130** 2 **2131-4270** 1
		P43, P44	*Household 5*: a father and his daughter.	**19-25** 1 **>56** 1	**Bachelor's** 2	**<215** 1 **>4270** 1
		P45 - P47	*Household 6*: a widow, her daughter and her son.	**19-25** 1 **26-35** 1 **>56** 1	**High school** 1 **Bachelor's** 2	**<215** 2 **2131-4270** 1

The median age (an index that divides the population into two equal groups, one older and the other younger than the median) in the KSA was 29.8 years in 2015 (Statista 2017). Participants' ages ranged from 19 to over 56 years, thus including some older and some younger than the Saudi median age. The education level of most participants was relatively high, because the literacy rate among Saudis in 2013 was 94.43%, while in 2014 the gross enrolment ratio for secondary education was 108.29% and for tertiary education, 61.11% (UNESCO 2014). The General Authority of Statistics (2016) reports

a gross national income per capita in the KSA of £3,800; it was important to include some participants in the sample earning more and some less than this mean value. Thus, the sample was selected to include a variety of participants reflecting major variations across the Saudi population, to enhance the validity and applicability of the results.

Phase two involved conducting semi-structured interviews with bankers. All participants had received full information about the study, how their data would be kept secure and who would have access to the data; each participant then gave explicit consent to his or her participation in the study (see Appendix 7). Each phase of data collection is now described in turn.

3.6.1 Eliciting data from customers

The mail system of Umm Al-Qura University in Makkah was used to advertise the study and recruit its participants, so they were all students or staff of the university, or their relatives. The invitation letter is reproduced in Appendix 6. All participants were also household bank customers, i.e. each held one or more personal bank account(s). This phase of data collection lasted from November 2012 to March 2015. To explore the area of research, a pilot study with six participants was first conducted (see Table 2). The preliminary findings of the pilot study helped to guide the researcher during the rest of the study.

3.6.1.1 Pilot study

In the pilot study, telephone interviews were used after considering the research context explained in Section 3.4. The interviews were semi-structured. All six bank customers were married Saudi citizens, three males and three females. Some had been married for only two years and some for more than ten. Two were married to each other but were interviewed separately. The participants were from various cities across the KSA and all

were employed except one, who was the partner of an employee. Each interview lasted 35 to 50 minutes and was audio recorded. Recordings were transcribed in Arabic, then translated into English to prepare for coding. I began by doing the transcribing myself and found that I was able to note problems and similar themes arising from the increased focus on transcriptions. This helped me not only to compare incidents and statements encountered in later interviews, but also to define the focus of future interviews for other participants. However, I found that making my own transcripts was difficult and time consuming, as I required up to 10 hours to transcribe a one-hour interview. I soon decided that hiring a transcriptionist would be far more sensible. After much research and effort, I found someone skilled in transcribing the Saudi accent, which both the researcher and interviewees used; this was important to avoid any misunderstandings in transcription or in following my instructions on formatting the transcripts. After interviewing each participant, I sent the transcriptionist a copy of the sound recording by email, then after receiving the Arabic transcript I checked its accuracy against the sound file, which allowed me to assess the precision of the work. Transcripts were acceptably accurate and finished far more quickly than my own efforts. I next sent the Arabic transcripts via email to a translator, who generated English versions. The translator held a PhD from a UK university and had considerable experience in academic research projects. Both transcriptionist and translator were well aware of the need to ensure the privacy of the participants and to preserve the security of the interview data files as part of their professional code of conduct. I discussed these issues with both of them and as neither had personal or professional contacts with any of the participants or venues, I was satisfied that anonymity and privacy could be maintained.

The English transcripts were next analysed using the ATLAS.ti computer-aided qualitative data analysis software (CAQDAS) package (see Appendix 8 for a sample of data coding using ATLAS.ti and Appendix 1 for pilot study questions).

3.6.1.2 Second round

After completion of the pilot study, focus groups were used to explore in more detail the participants' practices and attitudes that emerged from the telephone interviews. Twenty-three household bank customers were divided into four groups (see Table 2): husbands, wives, sons and daughters (see Appendix 2 for focus group questions). These group interview sessions were segregated by gender, an arrangement which was necessary for two reasons: firstly, to conform to the gender segregation that is fundamental to Saudi society; secondly, to explore the impact of different roles within households as factors influencing participants' practices. The female researcher ran sessions for the wives' and daughters' groups, while a male moderator ran those for husbands and sons, as seen in Figure 4 and Figure 5. The moderator was a relative of the researcher; this arrangement offered a convenient way to overcome the constraints of gender segregation and allowed us to discuss the questions and the protocol that would be followed in running the groups. To ensure consistency in their operation, the researcher and the moderator discussed the questions in advance and agreed on the protocol for running the sessions. The specific advantage of this method for this research was the ability to divide the sample into separate groups of husbands, wives, sons and daughters, in order to explore the different family roles as factors influencing participants' practices. This division also served to give every participant the opportunity to speak freely without being influenced by the attitudes expressed by those with different household roles.



Figure 4: The researcher running the wives' focus group.



Figure 5: The moderator running the husbands' focus group.

The daughters' focus group had six members, whose main selection criteria were that each must be unmarried and still living in her parents' house, to reflect the traditional daughter's role. The sons' group comprised five participants, none of whom was

married and all of whom were still living with their parents, reflecting the typical son's role. There were six members of the wives' focus group, four of whom were employed and two who were housewives. The main selection criterion was for the participating women to be married; some had children while others did not, allowing the data to reflect the opinions of wives in both situations. Finally, the husbands' group also had six members, five of them employed and one who had retired. As with the wives, all were married, to reflect the husband's role, and not all had children. Participants were contacted via WhatsApp (a cross-platform mobile messaging app) to schedule and reschedule the sessions. Each session lasted an hour and a half, and as with pilot interviews, each session was voice recorded and transcribed in Arabic, then translated into English by the transcriptionist and translator mentioned above. Again, the English transcripts were analysed using ATLAS.ti.

3.6.1.3 Third round

In the third round, the diary/interview method was used to collect data from household bank customers. The main benefit of this technique is to reflect real and factual day-to-day data about each participant's banking practices. A variety of households were studied in round three, to allow the effect of different family roles and genders to be assessed as factors influencing banking practice. Six households participated, four having three members each, the others having four and two members respectively (see Table 2). There were thus 18 participants in total (nine females and nine males). The composition of the households was as follows. Household 1 comprised a remarried husband, his new wife and his son from the previous marriage. Household 2: a widow and two of her sons. Household 3: a widow, her son and her daughter. Household 4: a husband, both his parents and his wife. Household 5: a father and his daughter. Household 6: a widow, her daughter and her son.

To gather the data, each participant was first asked to keep a diary for a certain period of time, recording brief notes on his (or her) practices every time he accessed a bank account, whether this was his account or not. The diaries were then sent to the researcher to be analysed. Next, each participant was interviewed by telephone, using a semi-structured format. The purpose was to gather factual data, such as a log of participants' practices when using bank systems, decisions made and people involved. It was important to test this method with one household before applying it to the others, so initially only the members of the first household were asked to keep banking dairies during the last ten days of a month. This period was chosen because most employees in Saudi Arabia are paid on the 25th of each month and many do most of their banking transactions in the following days. The diaries would thus capture the (presumably contrasting) practices of the participants immediately before and after payday.

Before the start of the diary period, the members of the first household were shown examples of diaries written in Arabic by the researcher (see Appendix 3 for English translations of these examples) to clarify what they were being asked to write. During the diary period, WhatsApp messages were sent every three days to the participants to motivate them and to remind them to write their diaries. It also provided a useful opportunity for participants who wished to ask questions or seek clarification about the diary to obtain a quick response from the researcher. Thus, on the sixth day of the diary period, the father of the family used WhatsApp to ask the researcher whether a specific transaction should be included in his diary. At the end of the period of ten days, the diaries were sent to the researcher to be analysed. WhatsApp was then used again to set dates and times for separate telephone interviews with each member of the household (see Appendix 4 for household interview questions). This pilot test of the diary/ interview method made it clear that the diary period should be extended to a whole

month to fully reflect participants' banking practices, even if they used their accounts only during the last days of that month. Therefore, the same procedure was followed for the other five households, except that they were asked to keep a diary for a whole month, rather for ten days only as the first household had done.

The mother and son in the third household submitted diaries for analysis, but then dropped out of the study before the interviews. All diaries were written in Arabic and the interviews were conducted and transcribed in Arabic. Written English versions were produced by the transcriptionist and translator mentioned above, then the English transcripts were analysed using ATLAS.ti.

3.6.2 Eliciting data from bankers

The second phase, in which data were collected from bankers, lasted from July 2015 to April 2016. In total, 23 Saudi employees of different banks, covering all of the 12 mentioned in Section 2.3.3.2, were interviewed by telephone (see Appendix 5 for bankers' interviews questions). Table 3 lists details of the 23 bankers—13 males and 10 females—who were interviewed by telephone in order to explore the bankers' perspective on the influence of gender on banking security.

Table 3: Demographic information on participating bankers

Participant	Gender	Bank	Position	Participant	Gender	Bank	Position
P48	F	Riyad	BM	P60	M	Alahli	CSO
P49	M	SABB	BM	P61	F	ANB	CSO
P50	F	Albilad	BM	P62	M	Aljazira	CSO
P51	F	SHB	CSO	P63	M	Riyad	SM
P52	M	Alrajhi	CSO	P64	M	Alinma	CSO
P53	M	Albilad	BM	P65	M	Alahli	SM
P54	M	Alahli	BM	P66	F	ANB	BM
P55	F	Samba	CSO	P67	F	Alfransi	SM
P56	M	Saib	BM	P68	M	SHB	BM
P57	F	Samba	CSO	P69	M	Saib	SM

P58	F	SABB	CSO	P70	M	Riyad	CSO
P59	F	Aljazira	CSO				

The bankers were selected from all 12 banks that operate in the KSA and each was either a branch manager (BM), customer service officer (CSO) or sales manager (SM). Some had worked in the Saudi banking sector for more than 15 years, while others had less than three years' experience. The data were collected in three rounds of telephone interviews; the first with four male bankers and four females, the second with six males and four females, and the last with three males and two females. As with the first phase, the mail system of Umm Al-Qura University was used to advertise the study and recruit participants for the first round of data collection, all of whom were relatives of students or staff at the university. Recruitment for the second and third rounds used the snowballing technique, asking existing participants to suggest potential recruits. All interviews were conducted and transcribed in Arabic, then translated into English and subjected to a grounded theory analysis using ATLAS.ti.

3.6.3 Challenges of using interviews in the research context

This subsection considers the use of semi-structured interviews to elicit data from household bank customers and, in phase two, to elicit data from bankers. Initially, a Skype interview was tried with one pilot study participant, but this was unsuccessful because of the slow Internet connections in the KSA, consistent with the finding of Almogbil (2005) that 63% of bank customers in Saudi Arabia accessed the internet through dial-up services. Thus, we moved to telephone interviews. I was very sensitive to the people I wanted to interview and to the type of information I wanted to elicit. For these reasons, it did not seem appropriate to rely on a male collaborator to interview male bankers in the second phase. Telephone interviews were preferred as offering a method of identifying and discussing customers' practices related to the use of bank

systems that was convenient for both them and the researcher. Since the researcher is a female outsider, it was deemed preferable (especially for male participants) to conduct the interviews by telephone rather than face to face, for two cultural reasons. First, the gender segregation practiced in the KSA (Section 2.3.2) extends to the provision of separate areas for males and females in schools, universities, government departments and banks, so it was easier to conduct the interviews by telephone than in a workplace or public area. Second, as a cultural norm, it is also unusual to conduct interviews with strangers in the home of either party, even if both participant and researcher are of the same gender.

At this stage I felt the need to build rapport with participants, to help in creating a level of trust and understanding and making it likely that they would take the study seriously. Building rapport generally involves a "harmonious, sympathetic connection to another" (Newberry and Stubbs, 1990 cited in (Kieckhaefer, Vallano et al. 2014) and I did this during the interviews by sharing my status as a married woman and mother, studying at the well-known and prestigious University of Oxford. However, because the pilot study participants were recruited via a social network, this element of prestige was not required. When it came to recruiting participants for the second and third rounds, it was clear that it could not be done by networking or snowball sampling, especially when I spent much time and effort in recruiting participants for the male groups. It was both awkward and embarrassing for me to ask female relatives and friends to allow me to interview their male relatives, especially husbands. This was made clear when I asked a female participant to help with recruiting other participants, especially males, to which she replied: "I can't ask any of my friends to allow you to interview their husbands… Even if this is for academic purposes, it would not be acceptable for a woman to speak to a non-relative man." Having accepted the strength of this argument, I decided to try

recruiting participants via the mail system in Umm Al-Qura University, where I am a lecturer and known to many of the staff, academics and students. This turned out to allow me to recruit participants quite easily. The fact that all of the participants were students of the university or their relatives, who therefore knew me to some extent, reduced the perception of the researcher as a stranger or outsider. In addition, I noticed that the fact that I am a Saudi, which is obvious from my surname, helped to make participants feel relaxed and comfortable, since they would expect me to be able to understand them and their practices and motivations without lengthy explanation.

Semi-structured telephone interviews were also used to elicit data from bankers. In order to collect in-depth data, it was originally intended to conduct face-to-face semi-structured interviews with men and women working in Saudi banks. However, because of the gender segregation principle in the KSA, participants could not be interviewed face to face by members of the opposite sex. This made it difficult for the researcher, a female, to interview male bankers, while she could interview female bankers. To preserve the consistency of the research method and thus of the data, we could not interview female participants face to face and males by telephone. The consistent approach that we devised was to interview all participants by telephone, thereby remaining sensitive to the constraints of the research context.

All interviews were carried out and transcripts made in Arabic, because this was the participants' language of choice; then the transcripts were translated into English for CAQDAS analysis. This facilitated the coding of data and writing of memos, by providing analytical and visualisation tools to create representative views of the data, helping the researcher to reach a deeper understanding of the data, to obtain the results and to draw out the findings.

3.6.4 Challenges of using focus groups in the research context

Gender-segregated focus groups were used in the second round of phase 1 to collect data from household bank customers, for the cultural and practical reasons explained in Section 2.3.2. Focus groups are useful to investigate and reflect on how different groups think and feel about the research topic and why they hold certain opinions, without them being influenced by the opinions of the members of other groups. The specific advantage of this method for this research was the ability to divide the sample into separate groups of husbands, wives, sons and daughters, in order to explore the different family roles as factors influencing participants' practices. This division also served to give every participant the opportunity to speak freely without being influenced by the attitudes expressed by those with different household roles.

There were some challenges to running focus groups in the KSA, the first being one of recruitment: in order to recruit sufficient participants, it was necessary to invite up to 40 people to join each group. This difficulty arose mainly because the method is relatively new and less well known than questionnaires. The principle and operation of the focus groups therefore had to be described carefully to potential participants in an invitation letter. It was noticed that it was easier to recruit younger participants, for the daughters' and sons' groups, than older ones, for the wives' and husbands' groups. It happened many times that a recruit thought that she might convince one or more of her parents to participate in the study but failed. This may have been because young people accept new things more easily.

The cultural and religious constraints mentioned in Section 2.3 make conducting mixed-gender focus groups very difficult—if not impossible—in Saudi Arabia. Discussions with fellow Saudi researchers reveal that this was one of the reasons for doing such fieldwork in the UK rather than the KSA. For example, Alamri (2012) conducted three

mixed-gender focus groups in the UK, having recruited Arab participants from among English language students.[3] Given that this research seeks to reflect the different roles of the various family members, it was essential to have participants of both genders and therefore to run separate male-only and female-only groups. The researcher, being female, had to recruit a male moderator to run the male groups, while she ran the female groups herself. As explained in Section 3.6.1.2, the fact that this moderator was related to the researcher overcame the cultural constraints and facilitated advance discussion of how the sessions would be run, which helped to ensure consistency. Then, after each of them had run one group, the researcher and moderator met again and listened together to the recordings they had made of each of these. This collaboration was important to ensure that all groups were run in a similar way, so that the data they generated would be reliable and comparable. The use of a male moderator to run male focus groups was a good idea; however, after hearing the recordings of the resultant sessions and analysing them, I was frustrated by the lack of the necessary probing by the moderator. This experience motivated me to use telephone interviews with subsequent male participants in preference to enlisting the assistance of a male researcher.

A further challenge was finding a place to conduct the sessions. This might not be a problem in other countries, but the researcher spent a great amount of time and effort on this issue. There was no difficulty in the case of the daughters' group, which met on the

[3] Mentioned in a personal conversation with the researcher in the Sixth Saudi Student Conference, October 2012, Brunel University, UK.

female campus of Umm Al-Qura University, where the participants were students and the researcher worked as a lecturer, so they all had access. However, the same arrangement could not be made for the other groups, whose participants were neither students nor staff of the university. Given the cultural norms arising from the religious and cultural constraints referred to above, it was necessary to find public places to conduct the three sessions, as the use of private premises, such as the researcher's home, would not have been acceptable. This was particularly difficult because there are no neighbourhood community centres in the KSA, while in order to hire a meeting room in a hotel, the researcher would have needed to obtain approval from Makkah City Council, which would have taken up to three months. After much research, a closed meeting room in a restaurant was found, although such facilities are not common in Saudi Arabia. The room was suitable because it was accessible to the public but could be closed for the sessions, it was quiet enough for clear recordings to be made and finally, no official approval was required. Participants were contacted via WhatsApp to schedule and reschedule the focus group sessions.

Despite the many challenges, the focus groups proved useful in capturing and explaining some of the banking practices of bank customers and their motivations. In addition, conducting focus groups in this part of the study was useful in recruiting participants for the rest of the study. During the focus group sessions, the researcher and the moderator took the opportunity to acquaint the participants with the next part of the study, which again involved the use of uncommon methods: diaries and interviews. The aim was to introduce these methods and discuss them personally to avoid any misunderstanding, then to recruit participants for the main phase. Detailed information about the diary/interview method is presented in the following section.

3.6.5 Challenges of using diaries in the research context

The main benefit of the diary/interview method, which was used to collect data from household bank customers in the third round, was that questions about each participant's banking practices were based on factual data about his or her practices for a month. As mentioned in Section 3.4, it would have been impracticable to collect data on participants' banking practices by direct observation, so it was necessary to find another method. Thus, it was decided to collect data by means of diaries, followed by in-depth interviews (Bogdanovic, Dowd et al. 2010).

As mentioned in the previous section, during the focus group sessions the researcher and the moderator had taken the opportunity to acquaint the participants with this part of the study, as it involved the use of uncommon methods. The aim was to introduce these methods and discuss them personally to avoid any misunderstanding, then to recruit participants. One important outcome of these discussions, and of consulting the literature on the use of diaries in research, was that the researcher modified the diary method, having decided that an audio diary would be more suitable than a written one in the present context. Each recorded diary would then be sent to the researcher via email. The purpose of the diary in this study was to capture realistic and empirical data on participants' practices each time they used their bank accounts. Based on a study by Palen and Salzman (2002), there were four main reasons why the most appropriate way to do this would be for participants to record their diaries in spoken form using their smartphones. First, they were more likely in the normal course of events to be carrying a smartphone than a pen and a paper diary. Secondly, recording their thoughts on a mobile device suited the nature of the data, which concerned their use of bank accounts, including by means of ATMs or EFTPOS. Thirdly, smartphone technology would allow each diary entry to be sent to the researcher by email immediately after recording,

giving her the advantage of monitoring the participation of participants and analysing their diaries daily. Finally, smartphones are used widely in the KSA, where there were 22.2 million users in 2016 (Statista 2016).

However, the discussion with focus group members raised two unexpected challenges regarding the recording of diaries. First, participants warned that parents were likely to use older phones, which cannot be used for connecting to the internet or sending emails, and that even if they did have smartphones, they might find it difficult to use the functions necessary for recording a diary and sending it via email. More importantly, some participants objected to the recording of women's voices which could then be heard by men such as supervisors, transcriber, or examiners, asserting that it is forbidden in Islam for a woman's voice to be heard by a non-mahram man, as discussed in Section 2.3.2.

Nevertheless, there was significant disagreement on this second point among participants, as there is in the wider Saudi society and among religious authorities (Al-Munajjid , Al-Qaradawi). There is no clear rule on the female voice in the Holy Qur'an or the Prophet's Hadith, so people's beliefs are based on the ijtihad of Islamic scholars. Reflecting this disagreement, none of the females who had participated so far in either the first or second rounds of data collection had any objection to recording their voices for the purpose of this research and all gave their explicit consent (see the consent form in Appendix 7). In the third round, no female participant in any household had any objection either, except for the fourth household (see Table 2), whose two female members did object to the recording of their voices. In order to respect this minority objection and to maintain consistency in the collection of all data, the researcher decided that pen-and-paper diaries would be used, despite the advantages of recorded diaries noted above. In addition, as a special arrangement for the two female members

of the fourth household only, the researcher undertook to take notes during their interviews, instead of recording the interview as with other participants.

3.7 Chapter Summary

This chapter began by discussing the criteria for the methodology to be used in this study, then the choice of the methodology based on these criteria. Grounded theory was used in this research as a means to investigate the banking practices of household customers in the KSA. Data were collected from both household bank customers and bankers by means of interviews, focus groups and diaries supplemented by interviews. The use of each of these methods in the present research has been discussed in detail.

The next chapter begins by presenting and describing a model of the non-gendered aspects of the household customers' perspective.

4 MODEL OF HOUSEHOLD CUSTOMERS' PERSPECTIVE

4.1 Introduction

The previous chapter described the research approaches and discussed the challenges of using such approaches in the unique setting of the problem domain for the present research. As stated in Section 2.2, banks can be considered socio-technical systems, using computer technology to provide technical services that are used by millions of bank customers daily. To ensure the secure use and operation of such systems, their technical and social components must operate in harmony and these must also be considered when building a framework for evaluating security. A key aim of this thesis is to present a conceptual framework for evaluating the security of household bank customers in the KSA, comprising the three essential building blocks depicted in Figure 1: the household context of the use of the bank system in the KSA, the Saudi banking policies and infrastructure that guide the use of the system, and banking technologies and processes. This chapter and Chapters 5 and 6 present the first block of the framework, i.e. the household context of use, while chapter 7 will present the second and third blocks of the framework.

4.2 Household Context of Use

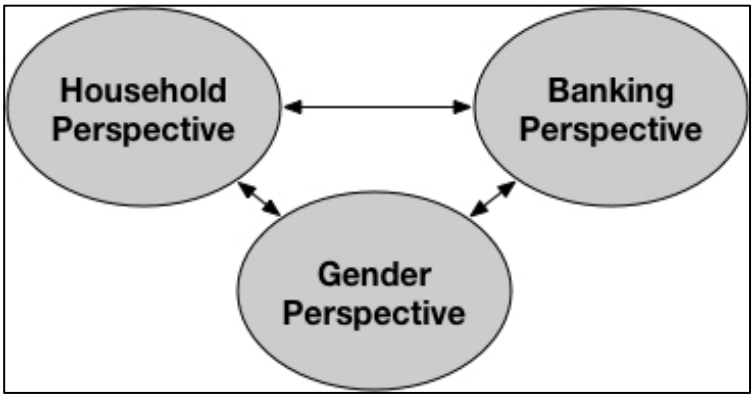


Figure 6: Household context of use.

The analysis of the data collected from household bank customers and bankers in the KSA drove the development of a model of the household context of use of the bank system in the KSA. A model is used in this thesis as a graphical representation of the findings of the data analysis and its purpose is to facilitate the understanding of the structure of the findings and the relationships between them. Since it would be very complicated to present all of the numerous parts of the findings and much too complex to comprehend the entirety of their dense interconnections, the model contains only those features that are of primary importance. The model of the household context of use of the bank system in the KSA is a multi-perspective model addressing the perspectives of household customers, banking and gender, as depicted in Figure 6 (for a detailed model, see Appendix 11). Household customers and bankers are important users of the bank system; therefore their perspectives are detailed in the household context of use, while the essential impact of gender in shaping these two perspectives is recognised by treating the perspective of gender as an independent factor in the household context of use. The first model, of the household customers' perspective on banking security, is presented in this chapter; the banking and gender perspectives will be presented in Chapters 5 and 6 respectively.

In this chapter, Section 4.3 details the process of collecting the data from the participants and building the model. Section 4.4 sets out the semantics of the grounded theory models presented in this thesis. Then Section 4.5 presents the findings of the grounded theory analysis of the data collected from household customers under four of the five main categories: the extent of sharing practices, motivation, conforming practices and challenging practices. The influence of the role of gender, the fifth category, is discussed separately in Chapter 6.

4.3 Model Building

To build the model of the household customers' perspective on banking security, data were collected from household customers in three rounds of data collection (Section 3.6.1): a pilot study, then a second round of focus groups and a third round involving a diary study and further interviews. The pilot study comprised telephone interviews with three male and three female household customers. In the second round, four focus groups were conducted with 23 participants in total: six daughters, six wives, five sons and six husbands. A combination of diary study and interviews followed in the third round to collect data from six households, four having three members each, the others having four and two members respectively. There were thus 18 participants (nine females and nine males) in the third round. In total, 47 household customers participated in the three rounds. The benefit of using multiple methods is to triangulate the data to increase its trustworthiness and validity and to obtain multiple perspectives. In addition, the limitations of any particular method or the conditions of any of the rounds of collection would not confound the final results. As explained in Section 3.6.1, each interview and focus group was audio recorded and transcribed in Arabic then translated into English. The English transcripts were next analysed using ATLAS.ti, following the iterative process of grounded theory that involves the use of three coding stages

(described in Section 3.3): open, axial and theoretical coding. The process was repeated until it reached the theoretical saturation point, when repeated analysis produced no new information. The full list of categories, subcategories and memos generated from the coding process is presented in Appendix 12. The final resulting model of the household customers' perspective is presented and discussed in Section 4.5, after a brief explanation of the relevant grounded theory semantics.

4.4 Grounded theory semantics

All of the models presented in this thesis were generated using ATLAS.ti and consist of network diagrams that relate the different categories and subcategories identified. The semantics of the notation are as in the example in Figure 7.

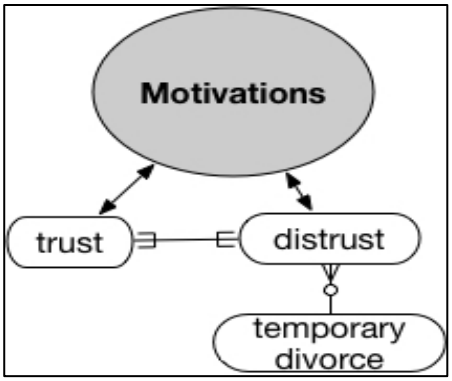


Figure 7: Example of a grounded theory network diagram.

This diagram means that **Motivations** is a category, while `trust`, `distrust` and `temporary divorce` are subcategories. `Trust` and `distrust` are contradictory and both are associated with **Motivations**. `Distrust` is a cause of `temporary divorce`.

4.5 Model of Household Customers' Perspective

The analysis of the data collected reveals that the banking practices of household customers were generally limited to opening and using a running bank account, obtaining an ATM card and using it in ATMs and for the Electronic Funds Transfer at

Point of Sale (EFTPOS) transactions, and using online banking and telephone banking. All participants had running bank accounts and some had more than one, but it was noted that the use of joint accounts and savings accounts was rare. Indeed, none of the participants had a savings account, although some said that they might use their running accounts for savings. Similarly, joint accounts were not popular: only one couple, who participated in the pilot study, claimed to use a joint account. None of the participating household customers reported using a cheque book, none reported using mobile banking and few reported using online banking. All participants held and used ATM cards, while only one female and two male participants held credit cards and as mentioned before one of the reasons for the popularity of ATM cards over credit cards is that the former are debit cards, whose use is unaffected by the long-running debate as to whether the prohibition of interest under Islam extends to credit cards. According to the participants who had credit cards, they used them only when travelling abroad or to obtain liquidity in urgent cases. As mentioned in Section 2.3.3.2, ATM cards cannot be used in online shopping, while the use of credit cards is rare, with the result that only two participants of each gender said that they used online shopping. An alternative reported by four participants in the present research was to use the services of an intermediary with experience in online shopping. The customer would contact such a person by phone or email to request certain goods, then transfer the money to the account of the intermediary, who would purchase the goods online using his credit card and send them on to the customer.

The analysis of the data revealed five main factors shaping the perspective of household customers: the **extent of banking practices**, **motivations**, **conforming practices**, **challenging practices** and **gender roles**, as seen in Figure 8 below (see Appendix 9 for detailed model).

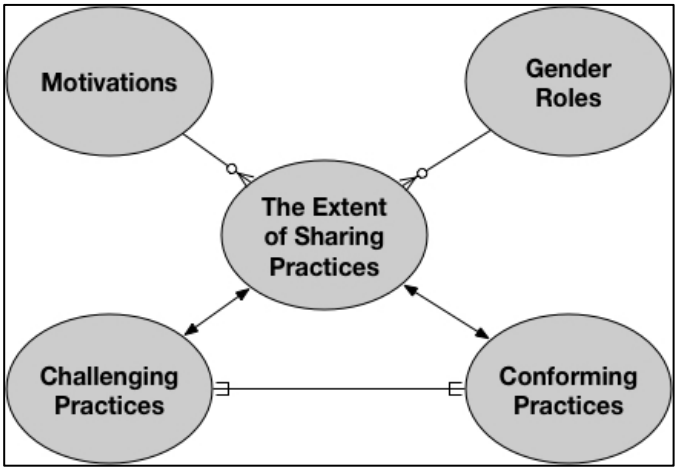


Figure 8: Model of Household Customers' Perspective.

However, because of the direct and very strong influence of gender in shaping the perspective of household customers, this factor is discussed only briefly in this chapter and will be considered in detail in Chapter 6. Throughout this chapter and those which follow, categories are in **bold** and subcategories are presented in a `different font`. The abbreviations P1, P2 and P3 stand for participants, while R denotes the researcher.

4.5.1 The extent of sharing practices

The first category highlighted by the analysis is the **extent of sharing practices** adopted by household bank customers. This represents the different sharing practices adopted by household customers, based on the data and seen in Figure 9 below. It was found that the sharing practices of household bank customers ranged from `no sharing` to `partial sharing` or `total sharing` of `credentials` and of `account control`.

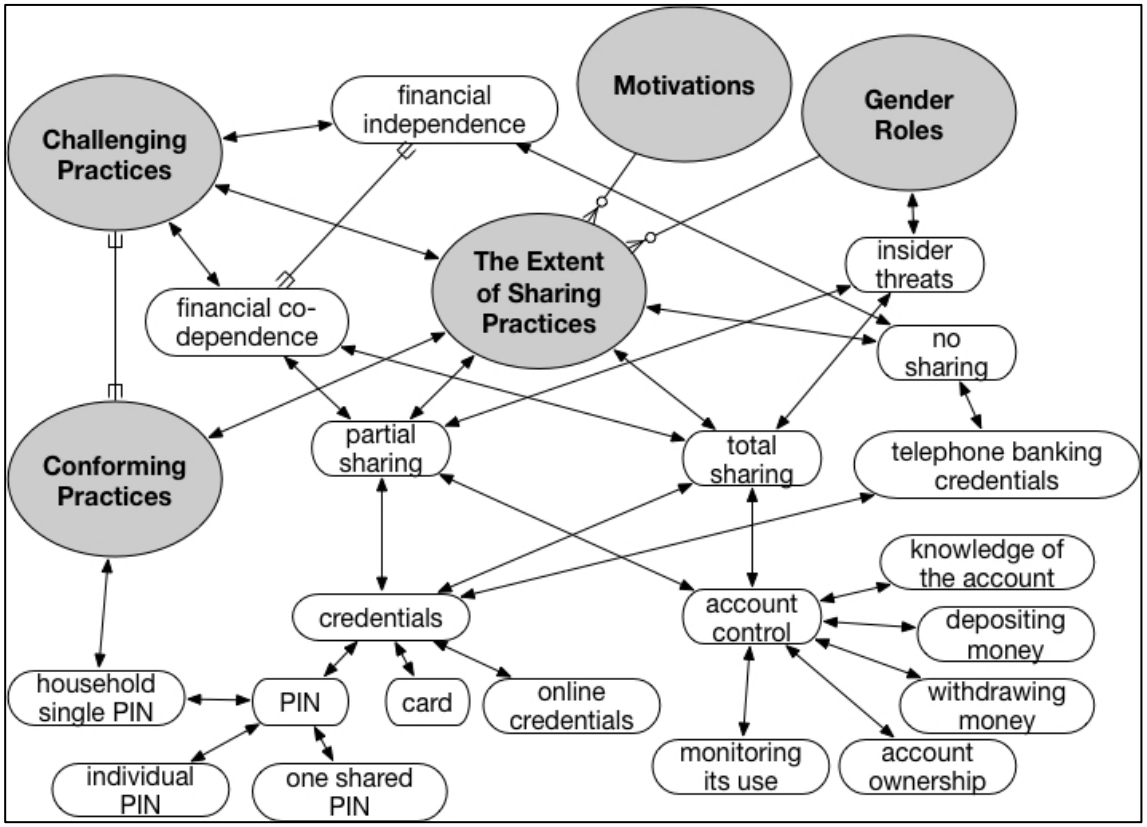


Figure 9: The extent of sharing practices.

The analysis of the data shows that the practice of sharing authentication `credentials` for household bank customers was adopted by most of the participants. This occurred when the account holder shared his or her credentials with family members. The authentication credentials that were shared most between family members were the `card` and its `PIN`. The shared PIN could be in three forms: an `individual PIN`, unique to one account and not used for other accounts; `one shared PIN`, a single PIN shared between the husband and his wife in the household, or a `household single PIN`, where a single PIN was used for all of the accounts held by the household members. Using the third form of PIN is a subcategory of **Conforming Practices** (see 4.5.3 for details). Regarding `online credentials` (username/password), some participants declared that they never shared their passwords. Those who did not share explained that because they used their ATM cards more than online banking, the need to share online passwords had not arisen and each was responsible for his or her own online banking, a situation

unaffected by sharing the same device to access online accounts. P2, a female participant, said:

I need to give my husband my card to get cash but I do not need him to access my account online ... But if we needed to I wouldn't mind giving it to him.

As for the participants who did share their online banking credentials, they did so with partners and explained that whichever partner in each couple had better IT skills was responsible for the online banking for his or her spouse, as will be explained in 4.5.2.3. On the other hand, aspects of sharing `account control` were also found to occur by sharing the account's credentials. Analysis of the data revealed five forms of sharing control over an account: `depositing money` in the account, `withdrawing money` from it, sharing the `account ownership`, sharing `knowledge of the account` and `monitoring its use`. Most of the participants shared control over their accounts with family members to deposit or withdraw money and only one couple shared the ownership of an account, a joint account which they used as a savings account. It is worth mentioning here that this is the only case of any of the participants in this research using a joint account. Sharing knowledge of the account occurred when the account holder informed family members of the existence of an account, or at least did not hide it from them. While sharing knowledge of the account is a common practice and all female participants adopted it, it was reported that some males did not share this information but kept it secret. This practice was observed in cases where male account holders had two accounts and shared knowledge of one of them with family members, allowing them to use it whenever they needed to by sharing its credentials with them, but where the family had no idea that a second account existed. This practice was mentioned by two participants in the wives' focus group and one in the sons' group. One reason given for this practice was that the husband was responsible for the family finances and kept one account secret in order to

control expenditure, as explained in 4.5.2.7. Another form of account control highlighted by the data analysis was monitoring the use of an account. This occurred when the account holder shared control of the account with family members so that they could monitor its use to protect the money in it. This might take the form of a father supervising his "*extravagant*" daughter and monitoring her expenditure as a way of "*teaching her not to spend all her money*", as mentioned by two wives and two daughters (see 6.3.3.1). Other participants described monitoring the use of an account as a "*safeguard*" to protect the daughter from others, such as a "*greedy husband*" (see 4.5.4.1 for details).

Based on the data, the sharing of `credentials` could be total, where the account holder shared with family members all three forms of credentials mentioned above: the account `card`, its `PIN` and the username/password for `online banking`. The sharing of `account control` could also be total, when all five aspects of account control mentioned above were shared: `depositing money`, `withdrawing money`, `account ownership`, `knowledge of account` and `monitoring of its use`. Meanwhile, the sharing of `credentials` and of `account control` could also be partial. `Partial sharing` of account credentials occurred when participants shared some of the credentials mentioned previously but not all of them. The same applies to partial sharing of account control, where the account holder shared part of the control over his/her account with a family member; for example, when a female shared control of her account with her husband to allow him to `withdraw money` from it but did not share `account ownership` with him. Finally, `no sharing` occurred where the account holder preferred to keep the credentials for the account secret and not share `account control` or `credentials` with anyone. Interestingly, none of the 27 participants who reported using telephone banking said that they shared their `telephone banking credentials` with family members, although all of them shared their

cards and card PINs and some also shared online credentials. Participants gave various reasons for making this distinction: (1) Some shared card credentials for reasons such as the restricted mobility of women, which did not apply to telephone banking; (2) some shared online credentials because they lacked the required IT skills, which was not the case for telephone banking, (3) some shared online credentials because accessing bank accounts online requires the use of a device such as a PC, to which not all participants had access, while telephone banking can be easily accessed by landline or mobile telephone, which was available to all of them.

4.5.1.1 Summary

The **extent of banking practices** (Figure 9) was found to vary from not sharing to total or partial sharing for card and online credentials, while participants who used telephone banking preferred to keep the relevant credentials secure and not share them at all. Total or partial sharing essentially means sharing control of the account for any of the reasons listed under **Motivations** (Section 4.5.2). However, the only possible way to share control of an account was by sharing credentials. The most common banking practice among participants was either total or partial sharing of credentials and/or account control, allowing participants to rely on each other in a situation of `financial co-dependence`, which is categorised under **Challenging Practices** (Section 4.5.4); however, these forms of banking practice are open to `insider threats` in that a family member of the account holder may misuse the shared credentials. `Insider threats` are gendered, involving **gender roles**, because such misuse tends to be perpetrated by men against women, as will be fully explained in Chapter 6, Section 6.3.1.3. By adopting the banking practice of `no sharing`, the account holder can preserve his or her `financial independence`, as described in Section 4.5.4.2.

4.5.2 Motivations

Based on the analysis of the data, the second main category to emerge was **Motivations**. As mentioned in the previous section, the data reveal that the majority of household customers shared bank credentials in order to share control of their accounts. However, participating customers did not necessarily regard this as a security problem, because they had alternative understandings of security. Rather than being about transactions and privacy, these security practices were seen as relational, affective and emotional, being grounded in family ties, relationships and human values such as trust and religious adherence. Most household customers expressed a belief that sharing is safe, especially given the various measures in place to ensure the security of their accounts (particularly SMS notification, discussed below in Section 4.5.2.2). Many declared that credentials could be shared securely because their relatives would never misuse the shared knowledge, for reasons of religion and culture. Participants described their partners, siblings and parents as religious believers for whom such misuse would be irreligious, as well as alien to Saudi culture. This general perception of sharing and security motivated the widespread adoption of the banking practice of sharing credentials. However, a deep investigation of this perspective on the sharing of bank credentials revealed ten specific factors (see Figure 10) identified by household customers as motivating them to adopt one or more of the banking practices mentioned in Section 4.5.1 on the **extent of banking practices**. Seven of these motivations will be considered here in detail, while the remaining three (`accessing cash`, `illiteracy` and `family finances`) were found to be affected by gender and are therefore covered only briefly here and discussed in detail in Chapter 6.

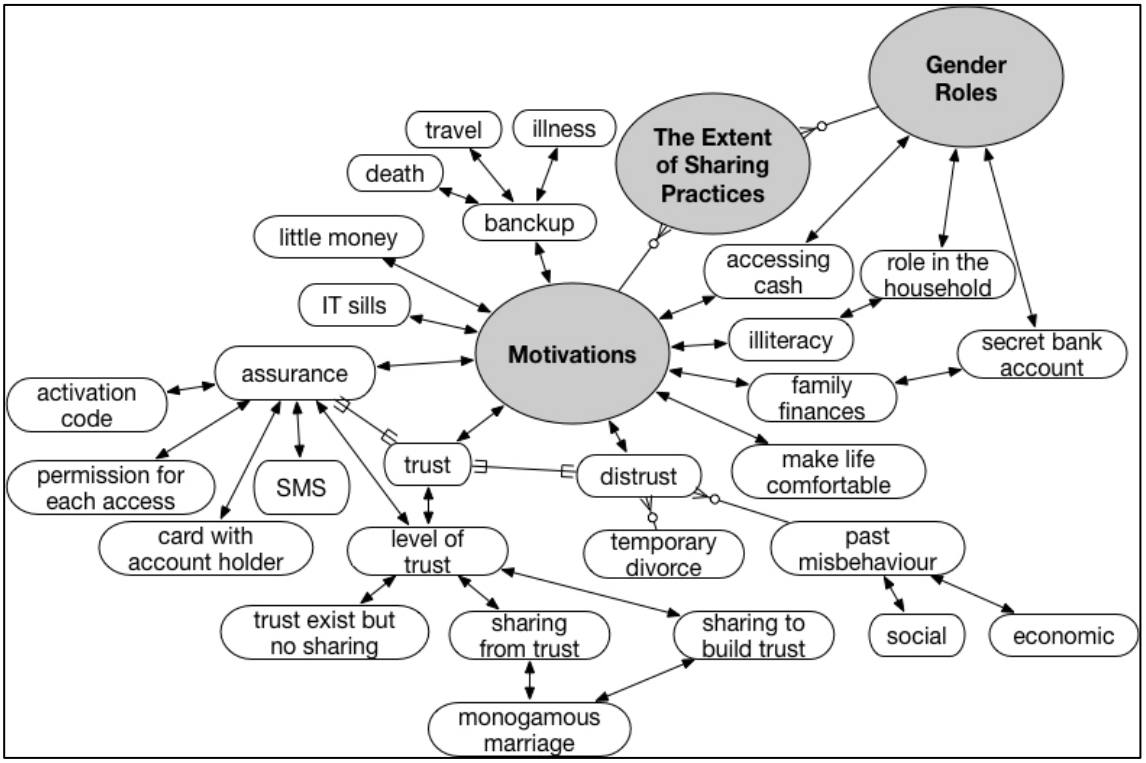


Figure 10: Motivations.

4.5.2.1 Trust and distrust

The main motivation given by household customers who adopted the practice of sharing credentials and control over their accounts with family members is `trust`, which motivated sharing between all family members: husband and wife, siblings, and parents and their children. Only if trust existed would any other additional motivations or issues be considered. Focusing on sharing practices in couples, most participants agreed that sharing was a sign of trust between husband and wife. For example, a male participant, P1, said:

It's all about trust between wife and husband … and this is more important than just a bank account … In our culture and with our priorities, this is much more important than materialistic belongings … and in our marriage, I have given her things more important than a bank account.

For this participant, trust between him and his wife was more important than their bank accounts and he referred to the cultural norms that defined his priorities. It is worth mentioning that according to Saudi cultural norms, most marriages are family arrangements. The groom's mother chooses the girl who she thinks will be most suitable for her son, then, usually after six to 12 months of engagement, they are married. According to the participants, trust and sharing arise during the first months of the relationship, which means that couples begin to share sensitive banking information when they have known each other for only a very short period of time. Another participant declared that he trusted his wife and decided to share such information with her from the fifth month of their engagement, even before they were married. It is noteworthy here that couples usually started sharing before having children, although having children increased the propensity to do so. Thus, a female participant said:

Sharing between me and my husband happened before we had kids. But if I want to be honest, I would say that having kids puts a big emphasis on the need for sharing. For instance, when I want to buy something for them and I don't want to go out, I just send them with their father and give him my card to use. [P3]

Similarly, another participant stated that she had shared her credentials with her husband from the first month of their marriage. One explanation is that marriage creates the expectation of mutual trust between husband and wife, which in turn creates the expectation that banking information will be shared, making sharing a consequence of marriage.

The findings discussed above suggest that trust is a necessary precondition to sharing; conversely, the mother in a household participating in the third round appears to have built a relationship of trust through the practice of sharing. This participant had two

stepsons and to initiate a trusting relationship with them, she decided to share her PIN with them. She chose to give them her card, asking them to withdraw some cash for her, although she did not need to do so, because her husband normally did this for her.

I want them to trust me, especially because I am not their mother. I am their stepmother… I did not force any of them to call me Mum, but they did so by themselves. They didn't call me Mum until they trusted me. [P31]

When one of the stepsons was asked about this, he said:

When she told me for the first time I was shocked. I didn't expect it at all … because I used to just use my father's card and now my mother's card too … Actually, I don't think it's had a big effect on my life. I had positive feelings for her before this, so sharing wasn't more than a complementary thing to the good feelings I had for her all along. [P32]

A contrasting finding was that `trust` can exist between family members who do not adopt the practice of sharing. The father in fifth household participating in third round of data collection stated that he considered any information related to his account to be private and would not share it with his family members, although he asserted that he trusted them. Moreover, this father taught this practice to his children, who adopted it.

On other hand, most participants felt that withholding banking information from a spouse would be a sign of `distrust`:

If she does not like to share such information with me, then she might have a trust problem … there is definitely a trust problem. [P6]

It's natural for couples to share everything … Otherwise, there will definitely be a trust problem. [P24]

Interestingly, one participant admitted distrusting her husband, stating that they used to share banking information, until she felt that she could no longer trust him after they had been temporarily divorced.[4] Although the couple had decided to reunite, she could not trust her husband again, so she decided not to share sensitive information with him. He, however, still shared his credentials with her:

I used to trust him and tell him everything about my account and how much I had. But after the first divorce, I became afraid; then after the second divorce, I got really afraid. Therefore, I think that divorce is the main reason why I am hiding everything, not just my money. ... I know his card password; he always tells me everything about his account and he is really honest with me about money and all his financial stuff. I know that even if he gave some money to his parents, he would tell me about it. So you can say that he trusts me more than I trust him. [P4]

Other participants added `past misbehaviour` as a reason for not sharing based on `distrust`. This could be either `economic misbehaviour` or `social misbehaviour`. Participants identified some cases where a daughter could refuse her father's request for sharing and such a refusal would be acceptable, such as where the father had a reputation for using money unwisely or treating his wife badly.

[4] In Islam, couples may obtain a temporary divorce for three months. If they are able to resolve their problems during this period, they can come back to each other and continue their married life. If not, this temporary divorce becomes permanent. This process can be used only twice during the life of a marriage.

4.5.2.2 Assurance

Most participants who shared their bank credentials saw no risk in doing so, claiming that the account holder would be informed by SMS of any operation on the account, such as transfers, withdrawals or online access. Participants considered that this service would protect the account from any fraudulent transaction by allowing the account holder to monitor it. SMSs are also used by some banks to protect their online banking: account holders receive a one-time authentication code by mobile phone when they request access to an account online; again, this service protects bank customers as well as allowing them to monitor access requests to their accounts.

Another reason that some participants gave for believing that sharing was relatively safe was that the card would be kept by the account holder at all times and no one would have access to the account without the card, even if he knew the card PIN. A member of the daughters' focus group sharing her card with her brother and said:

Why would I stop this sharing? He doesn't have the card with him all the time… and if he has the card, he just makes the withdrawal and brings it back to me. He doesn't take anything. [P8]

Furthermore, sharing was seen as safe because, according to the participants, permission must be obtained for every transaction:

Even if my wife's card is with me all the time, it is unacceptable to use it without her permission... In Islam even if she is rich the man has not got the right to take money from his wife without her permission. [P25]

4.5.2.3 IT skills

As mentioned in Section 4.5.1 on the **extent of sharing practices**, when discussing the sharing of `online banking` credentials, it was found that the partner with more IT

experience within a couple was responsible for the online banking for his or her spouse. In one case the wife was responsible and in the other it was the husband. Those who did not share explained that because they used their ATM cards more than online banking, the need to share online passwords had not arisen, and each was responsible for his or her own online banking, a situation unaffected by sharing the same device to access online accounts. In addition, an account holder might ask someone to help him with online banking because he did not have sufficient internet competence, for example. This might require details to be shared only once, when first accessing the online banking service, after which the account holder would manage alone; alternatively, he might count on such help every time he wanted to use the service.

4.5.2.4 Having little money and making life comfortable

Participants declared that they adopted the practice of sharing because the money in their accounts did not amount to much, so if anyone misused an account and stole the money from it, the participant would lose relatively `little money`.

On the other hand, many male and female participants were happy to share their credentials with others, both female and male, in order simply to `make life comfortable`.

Sharing is a way of supporting each other … a kind of solidarity where we help each other to make our lives easier. [P26]

4.5.2.5 Accessing cash and illiteracy

Female participants declared that they shared their credentials because they suffered from limited freedom of movement, as mentioned in 2.3.2. However, if that limitation did not exist, they stated that they would still share, but not as much as they did now. This subcategory is discussed in detail in Chapter 6, Section 6.3.1.2. Meanwhile, many

participants cited illiteracy as a factor motivating parents to share with their children. More specifically, this was the motivation for mothers to adopt the practice of sharing with sons and this subcategory is discussed in detail in Chapter 6, Section 6.3.3.1.

4.5.2.6 Backup

Some participants saw sharing as a necessity in order to have a backup of their credentials, given the perceived importance of this information. Many participants expressed the view that a wife would need to know about her husband's assets and obligations, in order to avoid any unpleasant surprises if he should die suddenly. A participant in the daughters' focus group said that her father had gathered the family together before he died and told them everything about his money and his bank accounts, because he used to help certain people with donations and wanted to be sure that this help would not stop after his death. A related reason for sharing this information was to avoid problems with the family of an account holder who had died, as illustrated by the personal experience of a member of the wives' focus group:

Actually, it is important that the wife asks frankly about those things, given what I have learned from the situation I went through after the death of my husband. I didn't know anything, not even his card PIN, and all those things had to be taken care of by his brother, and there were a lot of problems. I couldn't do anything and I couldn't get out, as I was in mourning, so the wife should know these things. [P18]

Participants also mentioned the importance of needing to share credentials in cases such as the account holder's illness or travel.

Once I had heart trouble and I got sick. During that time, my family needed to spend money and I trusted my wife who was careful – thank God – so although I stayed at the hospital for more than a month, my financial situation was fine, thank God. [P27]

My sister shared her credentials with me because she is sick. She can't get out frequently as she suffers from arthritis. Sometimes she needs things and she can't do it. For example, the last transaction I did for her two weeks ago was to pay her daughter's school fees. [P7]

I share my credentials with my wife because sometimes I travel abroad so I couldn't be there if she needed money to transfer to someone or to pay for electricity or something of this sort. [P28]

4.5.2.7 Family finances

As mentioned in Section 4.5.1, sharing `knowledge of the existence` of an account is a form of sharing control over an account. Analysis of the data reveals a pattern of behaviour whereby a man would hold two accounts and share knowledge of one of these with his family, allowing them to use it whenever they needed to by sharing its credentials with them, but where the family would have no idea that the second account existed. One stated reason for this practice is the religious obligation and cultural expectation that the male head of a household is responsible for the `family finances`. As a way of controlling family expenditure while maintaining his financial independence, a man will have more than one bank account, one of which will be used specifically for family expenditure; he will transfer money monthly to this account and share its credential with other family members. This pattern of practice will be discussed in detail in Chapter 6, where it is related to the category of **Workaround**: `secret bank account`.

4.5.2.8 Summary

Household bank customers perceived their own practices of sharing bank credentials and security as governed by family ties, trust, relationships and religion, rather than

these practices being perceived as matters of the security and privacy of transactions. Many felt that credential sharing was safe because religion and cultural norms would prevent their relatives from misusing shared credentials. Since the people with whom they shared were religious believers and members of Saudi culture, it would be unthinkable that misuse would occur. This section has discussed seven of the ten factors which household customers identified as motivating them to adopt sharing practices (see Figure 10). Female account holders might be motivated to share their credentials for `accessing cash` and withdrawing money, because of the law against women driving in the KSA. Among other reasons given by participants for sharing banking information with family members was `making life comfortable`. Some said that they did not mind sharing their banking information with family members because they had relatively `little money` in their accounts. Others were prepared to share their credentials because of their weak `IT skills`. Deficiency in IT skills has been reported as a factor for not adopting online banking in the KSA (Al-Somali, Ghlami et al. 2009). Credential sharing because of `illiteracy` mostly involved the sharing of mothers' credentials. Some participants saw sharing as a necessity in order to have a `backup` of their credentials, given the perceived importance of this information and to avoid difficulties which might arise if the account holder fell ill, travelled abroad or died suddenly. However, participants saw `trust` as the main precondition for sharing; only if trust existed would any other motivation mentioned above be considered. If there was `distrust` between household members, the banking practice adopted was to withhold credentials. Such `distrust` might arise from the `temporary divorce` of a couple or the `past misbehaviour` of one party, either social or economic.

Various methods of gaining `assurance` were reported, including receiving `SMS` notification of any operation on the account, keeping the `card with the account`

holder at all times, receiving an activation code for online banking authentication in an SMS and giving permission for each access. The purpose of such assurance was to confirm trusting relationships; the use of these methods can strengthen trust between family members if no misuse of credentials occurs. The analysis reveals three ways in which trust can be related to banking practice: first, as mentioned above, credential sharing can depend on trust; conversely, credentials can be shared as a means of building trust; lastly, trust can exist but not lead to credentials being shared between family members. The data show the first and second forms of trust to apply to monogamous marriages, whereas no case of polygamy occurs in the data.

4.5.3 Conforming Practices

The third category identified by the grounded theory analysis of the data was **Conforming Practices**, which denotes practices adopted by household customers that are consistent with those normally followed in their particular household. This category comprised five subcategories as seen in Figure 11 below: inherited household practice, men are guardians of women, opening an account at the same bank, treating credentials in the same way and household single PIN.

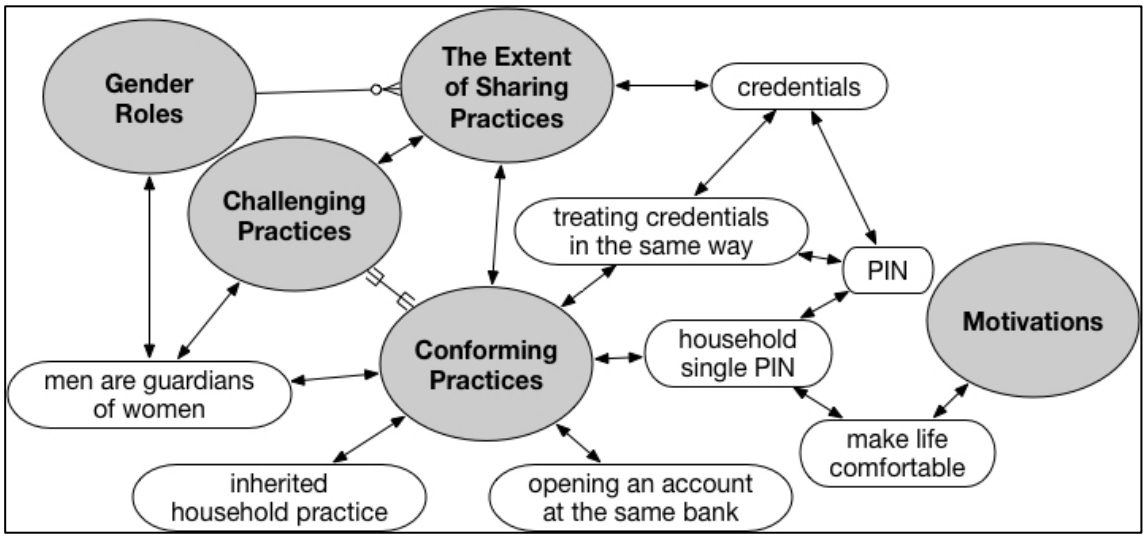


Figure 11: Conforming Practices.

All Saudi women are required to have a male guardian, as explained in 2.3.2. Analysis of the data shows that this obligatory relationship, whereby `men are guardians of women`, is reflected in the dynamics of households. It was found that each would normally be headed by one person and that it was usual for the head of the household to dominate the banking practices of other members to some extent. This dominant person was usually a man, often the husband/father. Alternatively, if the father was elderly or had died and the eldest son was old enough, then the dominant role would pass directly to him and he would be considered the father's successor. As this subcategory is directly and very strongly influenced by gender, it is covered in detail in Chapter 6. In addition, data analysis revealed a pattern of following the banking practices of other members of the household, labelled `inherited household practice`. It would be expected for a new bank customer to follow the banking practices adopted by other members of his or her household who had longer experience as bank customers. This pattern of behaviour was indicated by many participants; for example:

I share my credentials with my husband because I used to see my father and his wife exchanging their PINs . . . and there were no problems. [P19]

In this case, the participant adopted the banking practice of sharing credentials, following the practice she used to see daily from her father and her stepmother. In another case, an unmarried son in the second household, when asked about the future and whether he would stop sharing bank details with his brothers when he was married, said:

No, I don't think I'll stop … because my older brothers … are married and they didn't stop sharing with us… So I will do the same thing. [P35]

Other participants also referred to following practices accepted as normal in their households, especially by older members. In all cases the practice was to share credentials among family members, with one interesting exception: the daughter in the fifth household declared that she did not share her credentials with anyone, following her father's preference for privacy:

No one knows my credentials because I consider this as private information… so neither my parents nor my siblings know this information… I used to see my father doing this and I wanted to be like him. [P44]

Moreover, when her younger brother opened an account, she taught him to follow the same practice, treating his credentials as private and not to be shared with anyone.

Another pattern emerging from the data is that when a person wanted to open an account, he would tend to choose the same bank as other members of his family: `opening an account at the same bank`. For example,

I opened my account a year ago and I chose [Bank X] *because all my family use this bank … so if I need to I can make money transfers to any of them easily and without a transfer fee.* [P13]

This point was supported by many participants, with several explaining that the advantage was that they could avoid transfer fees. Others noted that this arrangement also saved time, as transfers between accounts in different banks could be time consuming. As well as inheriting banking practices, such as either sharing or not sharing credentials, the data show that some participants had also inherited their perceptions of banking `credentials` as private information or otherwise, `treating their credentials in the same way`. It is worth mentioning here that the participants' attitudes towards credentials did not originate with the banks, since according to the participants the only

warning given by the banks was when a customer used a card device to register the PIN and was told not to disclose it to bank employees.

A third pattern identified was the use of a `household single PIN` for all of the family's different cards. A reason for this practice was to `make life comfortable` and easier for the dominant person, who would need to remember only one PIN for all of the accounts held by family members. Thus, the mother in the second household reported that her son had used an ATM to change the PIN for her card, to make it similar to his own, and that he had done the same thing with his wife's card:

My son made the PIN for his card, mine and his wife's the same number… he said this was easier for him, to remember only one PIN and not to get confused. [P33]

This practice was mentioned by other participants, despite the fact that it exposes all of the accounts held by a household to a higher risk of misuse. An example of this exposure is a participant who used the same PIN for her own card as for her husband's, then made his account vulnerable by sharing her card and its PIN with her brothers.

4.5.3.1 Summary

Conforming practices are practices adopted by household customers which are similar to those normally followed in their particular household. Examples are the `inherited household practices` of sharing or not sharing credentials, `opening an account at the same bank` as other family members, or `treating their credentials in the same way`. In an extreme form of **conforming practice**, there will be `household single PIN`. An individual customer may choose to follow this practice because of affection for the head of the household, who is usually a man.

4.5.4 Challenging practices

In contrast to conforming practices, the practices of household customers are said to be challenging when they contradict the dominating practices, i.e. those of the head of the household. As noted in the previous section, this person was usually a man and would tend to dominate the banking practices of other members to some extent, as `men are guardians of women`. As this subcategory is influenced directly and very strongly by gender, it is explored in detail in Chapter 6.

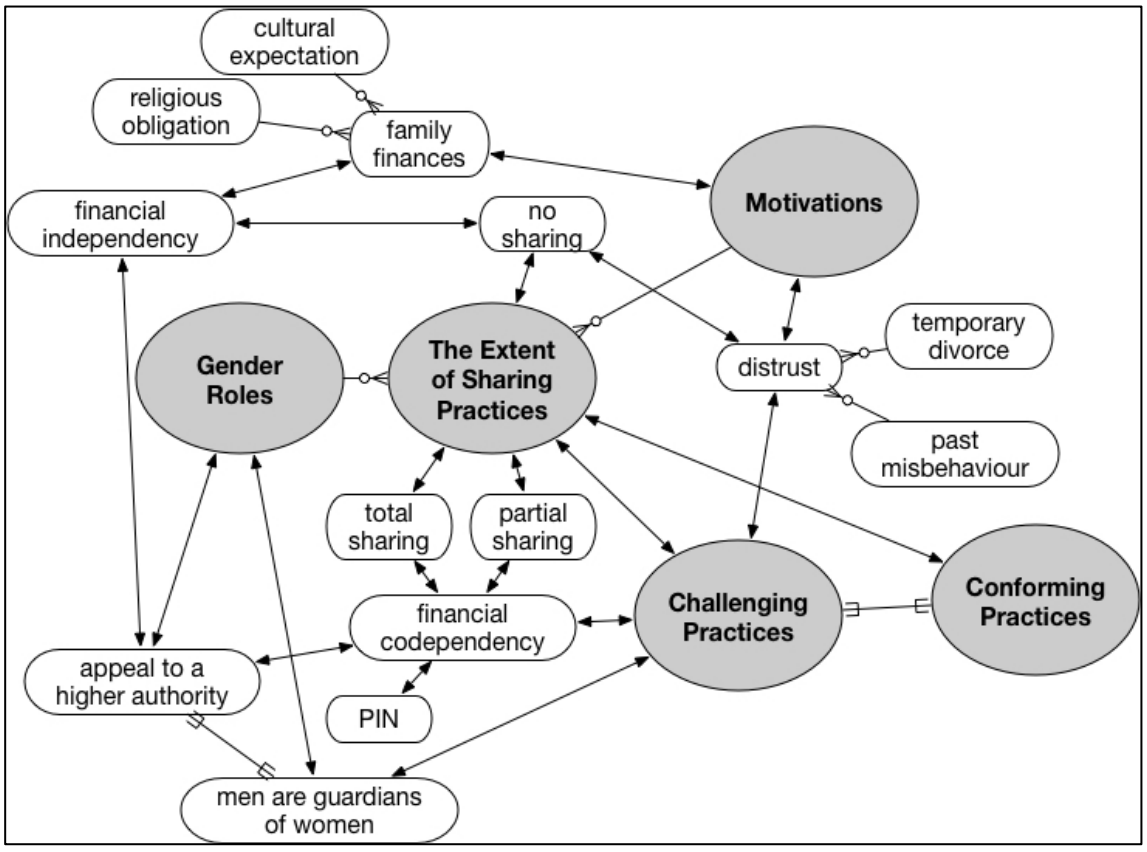


Figure 12: Challenging Practices.

`Distrust` was one of the motivations for adopting **challenging practices**, as seen in Figure 12. A case mentioned in Section 4.5.2.1 is that of a female participant who distrusted her husband following a `temporary divorce` and who stopped sharing credentials with him, although the husband continued his practice of sharing his credentials with her, even after she had stopped sharing with him. By her actions, the

wife challenged her husband's adoption of the practice of sharing banking credentials and as a result, she avoided counting on her husband to withdraw cash from her account by keeping cash with her all the time. Participants added `past misbehaviour` as a reason for challenging the head of the household. If the dominant person had misbehaved in the past either economically or socially, then challenging the head of the household would be acceptable.

4.5.4.1 Appeal to a higher authority

The practice of a bank customer challenging the authority of the head of the household by appealing to an authority higher than him is designated `appeal to a higher authority`. This practice was raised in the analysis as a security measure to protect a daughter and her money. A participant in the daughters' focus group recounted that her friend had shared control of her account with her widowed mother in order to protect her (paternal) inheritance from her husband. The husband had repeatedly tried to convince his wife to give him part of her inheritance so that he could use it to expand his business. To avoid direct conflict with him and to protect her money, the wife made her mother a joint account holder. The husband now recognised that his mother-in-law was supervising her daughter's account and monitoring every transaction, which stopped him from attempting to persuade his wife. The daughter thus challenged her husband as head of the household and to keep her `financial independence` from him she appealed to her mother. The data indicate that parents are in a position of authority in relation to their offspring, this parental authority being derived from religion and culture; this is supported by the assertion of Koocher (2009) that Arab culture respects elders and seniority. This practice is explained in detail as a **workaround** in Chapter 6.

4.5.4.2 Financial co-dependence and financial independence

Financial co-dependence is manifested when people rely on each other and practise either total sharing or partial sharing, as explained in Section 4.5.1, for instance when a daughter operates the account of her illiterate mother, in which case the PIN would be shared. It also includes the challenging practice of a person appealing to a higher authority to protect his/her financial independence. An example of such an appeal is the case mentioned above of the wife who challenged her husband and appealed to the authority of her mother, whom she made a joint account holder to protect her own financial independence. This appeal made mother and daughter financially interdependent, as they shared control over the daughter's account to protect her financial independence from her husband. Financial independence is asserted when a customer seeks a high degree of control over his own finances and adopts the banking practice of no sharing as the appropriate **extent of sharing practices**. An example of this from the data is that of a husband who adopted the challenging practice of maintaining his financial independence while exercising his responsibility for family finances, in conformity with religious obligations and cultural expectation, as explained in Section 4.5.2.7. Another example is the case mentioned in Section 4.5.2.1 of the wife who temporary divorced and decided to stop sharing her credentials with her husband and keep her financial independence as a consequence of distrusting him. A final example is the case of participant P40, the wife in the fourth household (see Table 2). Before her marriage, P40 maintained her financial independence by not sharing her banking credentials with anyone. According to her, she inherited this household practice from her father, who taught her to keep such information private. As a married woman, P40 managed to sustain this independent practice for seven years, although her husband insisted many times that they should share credentials. Maintaining her financial independence and not sharing her credentials with her

husband placed a burden on her, as she had to keep cash with her at all times. However, in their eighth year of marriage, it eventually happened that P40 forget to keep cash in her wallet and needed money urgently from her account while she was in the car with her husband. He stopped the car at an ATM and asked her to hand him her card and divulge its PIN so that he could operate the ATM, which as always in Saudi Arabia was on the driver's side. P40 felt obliged to do so because asking him to pull over so that she could walk to the ATM and withdraw the money in private would be inappropriate and unacceptable (see Section 6.3.1.2 for more information about accessing cash). According to P40, she regretted forgetting to keep cash with her as usual, which caused her to share her bank credentials with her husband. She reported now feeling uncomfortable for sharing them, which put her in a position of `financial co-dependence`, especially as she had always kept her credentials secure and did not share them with anyone, although she admitted trusting her husband. In addition, P40 said that she could not change the PIN for her card now, as she felt that it would convey the suggestion that she did not trust her husband and preferred not to do so.

4.5.4.3 Summary

The practices of household customers are said to be challenging (see Figure 12) when they contradict those of the head of the household. Among the motivations for such practices are the desire to maintain financial independence. An indirect challenge can be made by appealing to a higher authority, to avoid direct conflict with the head of the household while at the same time remaining financially independent.

4.6 Chapter Summary

The investigation of the banking practices of household customers has revealed the common practices to be opening and using a running bank account, obtaining an ATM

card and using it in ATMs and for EFTPOS transactions, and using online banking and telephone banking. Alashban and Burney (Alashban and Burney 2001) found Saudi consumers' income levels and education to play vital roles in the adoption and use of telephone banking; however, their study was limited to male bank customers because of the cultural constraints discussed in Section 3.4.

The present study found the use of running bank accounts to be very common, whereas joint accounts and savings accounts were rarely used. None of the participating household customers reported using a cheque book, perhaps because of the phenomenon of bounced cheques mentioned in Section 2.3.3.2. Nor did any participant report using mobile banking, contrary to expectations, given that smartphones are used widely in the KSA. Mobile banking may be seen as a special case of online banking, which a few participants did report using. In some banks in the KSA, mobile banking involves the use of online banking credentials. The reasons for not using mobile banking may thus be similar to those reported in the literature for not commonly using online banking, including a lack of awareness that the service is available and of adequate information about its use (Sathye 1999, Howcroft, Hamilton et al. 2002).

All participants held and used ATM cards, consistent with the high popularity of ATM cards as evidenced by their daily use in 1.56 million transactions (International Monetary Fund 2013). Only one female and two male participants held credit cards, which is inconsistent with the findings of Abdulmuhmin and Umar (2007) that almost two-thirds of their participants held credit cards and that credit card use was more common among females and positively related to income, education, age and religious attitudes to debt. This difference may possibly be connected to the fact that most of the 24 females in our sample were either students or housewives with no income. Those participants who did hold credit cards reported using them only when travelling abroad

or to obtain liquidity urgently, which is consistent with the usage of credit cards reported by Abdulmuhmin and Umar (Abdulmuhmin and Umar 2007). Given that ATM cards cannot be used for online shopping in Saudi Arabia and that few participants in the present study used credit cards, it is unsurprising that only two of each gender said that they used online shopping. This is again inconsistent with the literature; Eid (Eid 2011) states that 75% of respondents used online shopping in 2011; however, only 6.4% of participants in Eid's study were female. An alternative reported by many participants in the present research was to use the services of an intermediary with a credit card and experience in online shopping, who upon request and prepayment by bank transfer would purchase the goods on the customer's behalf.

The model of the household customers' perspective (for detailed model see Appendix 9) shows that the banking practices of household customers in the KSA can be categorised in terms of the extent to which they do or do not share control of their accounts. The elements of control are knowledge of the account, monitoring its use, making deposits and withdrawals, and account ownership. Where all of these elements are shared, there is total sharing of account control, the alternative being partial sharing. In either case, a possible way to share control over an account is by sharing its credentials, which again can be partial or total, involving the sharing of some or all forms of credentials: PIN, card and online credentials. The practice adopted is strongly influenced by the gender of the account holder (see Chapter 6 for more information) and by the motivations discussed above. A significant factor in individual practices within a household revolves around the individual's conformance with or challenging of the practice of the head of the household. This is related to the fact that men are guardians of women, which is a complex issue; discussion in this thesis is limited to those aspects that pertain to

banking practice. However, there is a clear theme in our data that ties elements of control and dominance in relationships with sharing practices in banking.

This chapter has presented the model of the household customers' perspective, built by conducting a grounded theory analysis of data gathered from household customers in the KSA in three rounds of data collection, each using a different method. To complete the image of the security of household bank customers in the KSA, another model was built, showing the banking perspective, which is presented in the next chapter.

5 MODEL OF BANKING PERSPECTIVE

5.1 Introduction

As mentioned previously, the model of the household context of use of bank system in the KSA is a multi-perspective model taking account of the perspectives of household customers, banking and gender. The previous chapter gave details of the collection and analysis of the data pertaining to the household customers' perspective, discussing all of the related factors except that of gender roles. The current chapter presents a model of household banking practices from the perspective of banks and bankers which must be taken into account to complete the image of the security of household bank customers. The building of the model is described in Section 5.2, which explains how the data were collected from bankers. The model of the banking perspective is detailed in Section 5.3. As was the case with the household customers' perspective, gender was found to have a direct effect on the banking perspective; the effects of this factor are addressed separately in Chapter 6.

5.2 Model Building

To build a model from the perspective of banking in the KSA, data were collected by interviewing bankers, as described in Chapter 3, Section 3.6.2. Given the constraints of the context of the research, specifically gender separation (discussed in Section 3.4), the female researcher interviewed both male and female bankers by telephone rather than face to face. The possibility of conducting face-to-face interviews with female bankers and telephone interviews with their male counterparts was considered, but rejected in order to maintain consistency in the dataset. There were three rounds of data collection, interviewing respectively four males and four females, six males and four females, then three males and two females, making a total of 23 bankers who participated in the interviews. As explained in Section 3.6.2, each interview was audio recorded and transcribed in Arabic then translated to English. The English transcripts were next analysed using ATLAS.ti. The iterative process of grounded theory was used, as described in Section 3.3, involving the successive open, axial and theoretical coding stages until theoretical saturation was reached. The full list of categories, subcategories and memos generated from the coding process is presented in Appendix 12. The final resulting model of the banking perspective is presented and discussed below.

5.3 Model of the Banking Perspective

Analysis of data from the three rounds of interviews identified five main categories, depicted in Figure 13 and shown in detail in Appendix 10: **Responsibility Confusion**, **Customers' Authentication Concerns**, **Gender Roles**, **Banking Services and Infrastructure** and **Risks to Banking Security**. These categories, which emerged from the interview analysis, shaped the model of the banking perspective presented in this chapter. The following subsections discuss the analysis of each category except **Gender Roles**, to be discussed separately in Chapter 6.

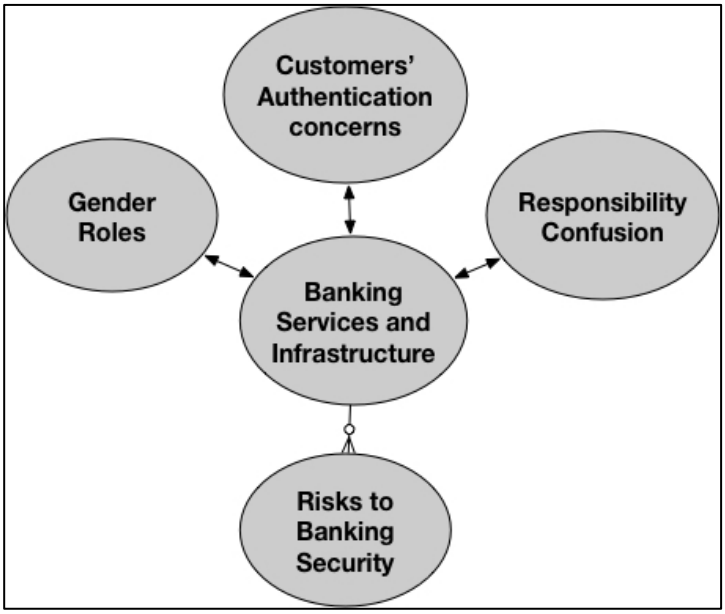


Figure 13: Model of the banking perspective.

5.3.1 Responsibility confusion

It emerged from the bankers' interviews that there was some confusion regarding two aspects of responsibility (see Figure 14): defining the `boundaries of bankers' responsibilities`, and responsibility for maintaining the `confidentiality of credentials`. The resultant subcategories are now discussed in turn.

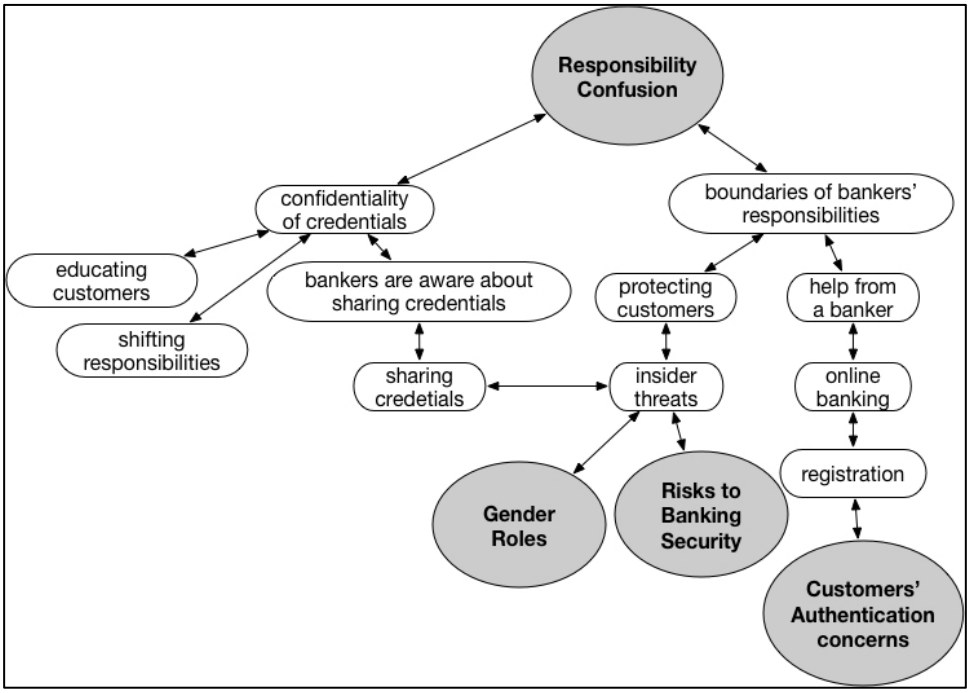


Figure 14: Responsibility Confusion.

5.3.1.1 Boundaries of bankers' responsibilities

The first aspect of bankers' responsibilities where there was confusion about boundaries was `help from a banker` for a customer to register for `online banking`. Despite its importance in saving money and effort for both the banks and their customers, online banking was the subject of complaints by customers, especially females, about the difficulty of `registration` and the lack of cooperation by bankers. When asked about this in interview, the majority of bankers declared that they did not help customers to register but merely introduced them to the online service and explained the details of the registration process. Similarly, Al-Somali, Ghlami et al. (Al-Somali, Ghlami et al. 2009) found that most of their respondents had never received information about online banking from the bank; the implication is that low awareness of online banking is a critical factor in causing customers not to adopt or use online banking. When this was raised with bankers, some claimed that their bank's policy prevented them from registering customers, while others denied this and stated that the only reason for not doing so was the risk that the banker, having been exposed to the customer's online

credentials, would fall under suspicion if money went missing from the account. One of the implications of this attitude is that bankers are not trusted by customers and so need to ensure they cannot be accused wrongfully.

The process of registering and using `online banking`, described in Section 2.3.3.2, was discussed with the interviewees, who were reminded that even if a banker knew the username and password for a customer's online account, it would still be necessary to have the authentication code. Some bankers identified two ways to circumvent this security requirement, which they suggested could be used with naïve, elderly or poorly educated customers. During online registration, the banker could enter their own mobile number instead of the customer's, allowing them access to the online account at any time. Alternatively, the banker might enter the customer's mobile number as required, then ask the customer to hand them the phone so that they could check the authentication code and use it to complete the registration procedure. If the banker could persuade the client that this process would take several minutes, they would have time to transfer money from the customer's account to their own personal account and delete the SMS notification of this fraudulent transaction from the customer's phone before returning it to the customer. In fact, only two of the 23 bankers declared that they had helped customers to register for `online banking`. They stated that there was no clear rule from the bank regarding this, that it was therefore up to the banker to decide whether to help customers in this way and that they saw no risk in doing so. This aspect of **responsibility confusion** is related the second category, **Customers' Authentication Concerns**, in that registering a customer for `online banking` is a concern for the banking system, as explained below. It is worth mentioning here that none of the participating household customers mentioned any problem with the registration of telephone banking, the reason according to them being that most household customers

use telephones, whereas computer and internet use is less widespread. Furthermore, telephone banking was seen as easier and more flexible by nature, as the customer deals with another human being, which is not the case in online banking.

A second confusion about defining the boundaries of bankers' responsibilities was identified when most of the bankers declared they had witnessed cases of `insider threats` against household customers, where the banker either could not become involved in helping the victim or preferred not to do so, to avoid problems in `protecting customers`. A female banker gave this example:

A customer came to the bank to apply for a loan of 50,000 SAR [£9150].[5] *After filling in the application and while we waiting for the final approval she told me that she was forced by her husband to take the loan. He was waiting for her at the door of the women's branch and she was obliged to give him the money. In this case, I couldn't do anything to help her. I could only advise her. I didn't know what to say to her. Should I say "These are personal problems, it's not my business", or should I call the police? Or advise the customer to call her brothers to protect her? All the other employees said this was not my business. Don't get involved, because the customer might say that the banker has told her to do so and so, and I would get into trouble. I was unable to do anything, but I advised her to call one of her brothers. When the loan application was approved and the customer received the money she decided to call her brother and asked him to come and protect her, then she filled an envelope with brochures to make it look like it was filled with money and sealed it. The customer had a physical disability and she couldn't walk properly, but she went out, gave her husband the fake envelope, then ran barely to her brother's car with the money.* [P51,F]

Unfortunately, the banker did not contact the customer after that and did not know what happened to her or how this incident affected her relationship with her husband. However, it can be foreseen that divorce may have been a consequence of her

[5] The currency was converted using the online XE currency converter, accessed 27 May 2017 (http://www.xe.com/currencyconverter/)

disobeying her husband.[6] A similar case was recounted by a male banker, who said that a man came to the branch with his three daughters to open accounts for each of them so that they could receive the monthly allowance from the government. From the banker's experience of over 20 years working in banking and from the way the father was treating his daughters, the banker believed that the father intended to keep the bankcards in order to divert the money for his own use, but felt that he could do nothing to help the daughters. This threat of insiders to household customers is explained under **Risks to Banking Security** below and because it is affected by **gender roles** in that it is mostly perpetrated by men against women, it is discussed in Chapter 6.

5.3.1.2 Confidentiality of credentials

The interview responses revealed that almost all bankers were aware of customers sharing credentials with family members, creating the subcategory `bankers are aware of credential sharing`; moreover, some indicated that `sharing credentials` was a common practice for a majority of customers. When participating bankers were asked what they would do if a customer admitted sharing his credentials with someone else, six replied that the most they might do would be to advise the customer about the risks of this practice, while seventeen interviewees said that they would not even give such a warning. According to them, the need to keep credentials secure was "*general knowledge*" and they were sure that their customers already knew this; therefore, there was no need to worry them by discussing the risks. Indeed, one female banker

[6] Culturally, Saudi society accepts a divorced man more readily than a divorced woman. A man can usually divorce his wife without bringing shame on his family, but the converse is not generally true.

considered such warnings "*rude*", as they could be seen as interfering in the customer's business.

I cannot interfere and worry my customers about sharing credentials with their family members if they want to do this ... this could be considered rude ... Customers must be warned about such things when they open an account and I think this is enough. [P48]

Other bankers declared that they would not report these incidents of sharing to managers or any bank committees, because, as one put it, "*everyone knows this is common practice among customers and it happens regularly*".

When maintaining the confidentiality of credentials was raised, all of the participating bankers assigned full responsibility for this to the customer, thus `shifting responsibility`. According to these participants, the banker's responsibility was limited to warning the customer about the security of this information during the process of opening the account. Surprisingly, nine of the 23 interviewees declared that they did not even warn customers who were opening an account about keeping credentials secure, did not advise them not to share these with anyone, including family members, and did not explain that a consequence of doing so would be to lose the legal right to protection by the bank. Rather than properly `educating customers`, these participants said that they would rely on the customers themselves to read the instructions to this effect on the application form. Seven bankers admitted that the official procedure required them to warn customers verbally about confidentiality when opening an account, but stated that most did not do so for different reasons, including that the branch was very busy and that they had other clients to serve.

5.3.1.3 Summary

Figure 14 summarises the details of the **Responsibility Confusion** category and its subcategories of the `boundaries of bankers' responsibilities` and `confidentiality of credentials`. A banker's responsibility for helping a customer to register with a service such as online banking was not clearly defined; some bankers helped customers and some did not. Nor was it defined clearly to what extent a banker should become involved with protecting the customer in a case of insider threat. Finally, bankers were aware that customers tended to share credentials, but considered themselves to have no responsibility for educating them about the inherent risks, as they believed customers to be solely responsible for maintaining the security of their own credentials.

5.3.2 Customer authentication concerns

The second category to emerge from the data was that of concerns regarding customer authentication, which also comprises two subcategories (see Figure 15): `registration` and `proof of identity`. As differences were evident in proof of identity between male and female customers in bank branches and the consequent granting of authorisation, discussion of this subcategory is postponed for inclusion in Chapter 6, which deals with the gendered perspective.

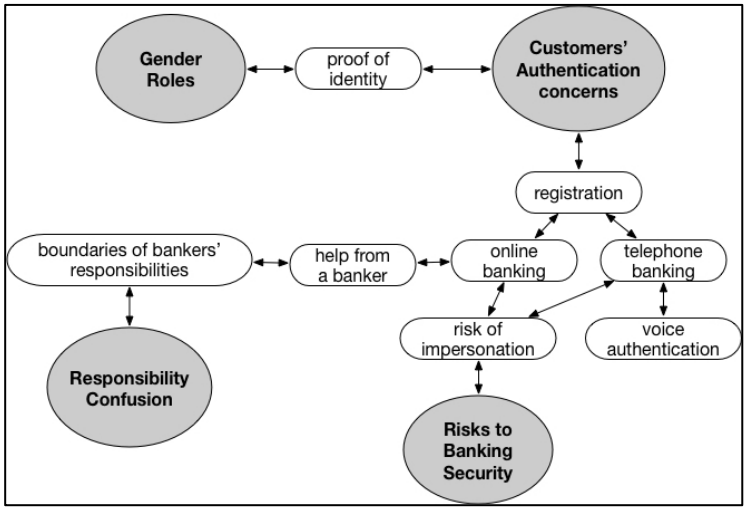


Figure 15: Customer Authentication Concerns.

Registering a household customer for a service such as `telephone banking` requires `voice authentication`; a female voice is expected if the account holder is female, and a male voice for a male account holder. According to the participants, registration for `telephone banking` was easier than for `online banking`, because most household customers use telephones, whereas computer and internet use is less widespread. Furthermore, telephone banking was seen as easier and more flexible by nature, as the customer deals with another human being, which is not the case in online banking. Finally, registering for online banking and telephone banking raised concerns about the `risk of impersonation`. As mentioned in Section 2.3.3.2, the physical authentication of the account holder's identity is not required in order to register for either of these services, which increases the `risk of impersonation`; this is discussed in Section 5.3.4.1 on **risks to banking security**. In the case of telephone banking, this problem is partly addressed by the requirement of `voice authentication`, but there remains a chance of impersonation. Concerns were also raised about the complexity of registration for online banking compared to telephone banking, especially where some banks required the additional step of ATM activation mentioned in Section 2.3.3.2. The complaints of some household customers that bankers were unhelpful with registration

for this service, amounting to inadequate `help from a banker`, are supported by the responses of bankers concerning `the boundaries of bankers' responsibilities`, discussed in Section 5.3.1.1 as a subcategory of **Responsibility Confusion**.

5.3.2.1 Summary

Figure 15 illustrates the detailed concerns regarding customers' authentication, including when registering them for online or telephone banking. Bankers tended not to help customers with this because of confusion about defining the boundaries of their responsibilities. In addition, the nature of the registration process adopted by banks in the KSA introduces a potential risk of impersonation. The second concern raised regarding customers' authentication was gender differences, which are discussed in Chapter 6.

5.3.3 Banking services and infrastructure

The third category to emerge from the analysis, **Banking Services and Infrastructure**, also comprised two subcategories (see Figure 16): `recently launched services` and `segregated branches`. The second of these concerns the differences and similarities between men's and women's branches and is discussed in Chapter 6 with other aspects of gender, while services recently launched by banks in the KSA are considered below.

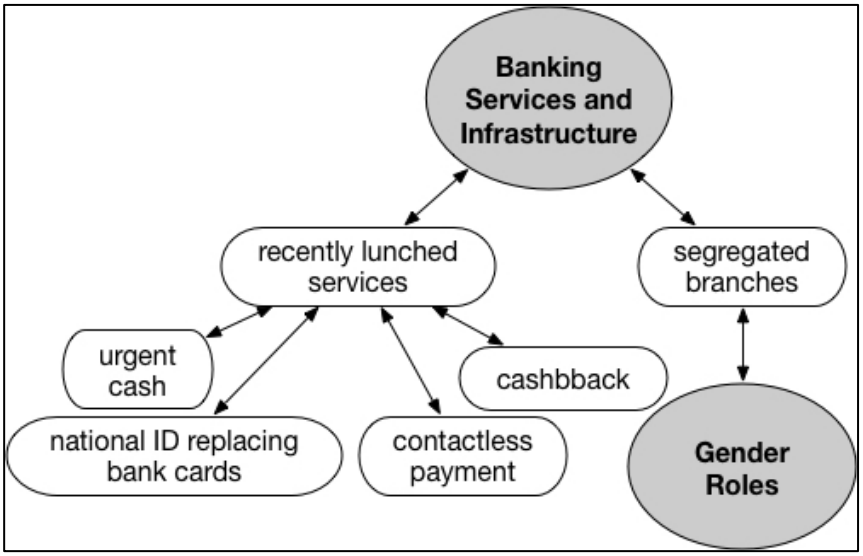


Figure 16: Banking Services and Infrastructure.

The analysis of the data highlighted two services introduced recently by Saudi banks: `cashback` and `urgent cash`. At the beginning of 2015, a cashback service was launched in the KSA allowing customers to use their bankcards at EFTPOS terminals to withdraw a maximum of 400 SAR (£75) per day in cash, with no limit on the number of transactions. Earlier, it was reported that three banks, (Alahli Bank), (Alinma Bank) and (The Saudi Investment Bank), had introduced a new service called "urgent cash" (AlRiyadh newspaper December 2014), allowing their customers to withdraw money from an ATM without a card. The customer logs into the bank app on a smart phone, specifies the account number and the amount of money required, then chooses a 4-digit passcode, valid for two hours. The bank sends an activation code by SMS, then the customer can withdraw cash from an ATM using the passcode, the activation code and the account holder's national ID number. This service is limited to 1000 SAR (£187) per transaction and three transactions per month. Most bankers participating in this research had no information about the urgent cash service, although some were employed by the three banks mentioned above.

Two further new services were identified from data: `contactless payment` and using `national ID to replace bankcards`. Contactless payment using a bankcard was introduced in May 2015 by two banks only: (Riyad Bank) and (Alahli Bank). Surprisingly, only three of the participating bankers were aware of this service, including those employed by the two banks. The main issue affecting this service was said to be the scarcity of the necessary card readers at EFTPOS terminals, most of which were still equipped with PIN pads and could not read contactless cards. In interview, a branch manager of Riyad Bank declared that his bank had recently begun the introduction of this service by issuing compatible cards to its customers and that customers could use the new cards for contactless payment outside the KSA, but that the service had not been activated in the KSA because of the shortage of suitable EFTPOS readers. The interviewee stated that no merchants were yet using the new card-readers and therefore few bankers or customers were aware of the service. Contactless payment was reported to be limited to 225 SAR (£42) per day and 75 SAR (£14) per transaction, with no limit on the number of transactions. The Saudi press has reported a debate about using national ID cards to replace bankcards for EFTPOS (Alarabiya News). When asked about this, only two bankers had heard of this debate, from newspapers, and none had enough information to discuss it in detail.

It has been noted in Section 5.3.1.1 that many participants did not adopt online banking because of inadequate information and help offered by bankers; from the responses of bankers themselves it now appears that some were not aware of services such as urgent cash and contactless payment, despite some of these services having been introduced long ago. These findings are consistent with reports in the literature (Sathye 1999, Howcroft, Hamilton et al. 2002, Al-Somali, Ghlami et al. 2009) that lack of awareness

of bank services and their benefits were critical determinants consumers' reluctance to use the services offered by banks.

5.3.3.1 Summary

Figure 16 shows details of the factors related to **banking services and infrastructure**. The direct effects of **gender roles** in the existence of `segregated branches` are discussed in Chapter 6. This section has considered four services recently launched by Saudi banks: `contactless payment`, `cashback`, `urgent cash` and the use of `national ID cards to replace bank cards`.

5.3.4 Risks to banking security

When asked about the potential **risks to banking security** arising from the practices currently adopted by household customers, interviewees mentioned three kinds of risk: `risk of impersonation`, `lack of auditability` and `insider threats`, as depicted in Figure 17.

The category of `insider threats` refers to a threat to a household customer generated by one of his/her relatives. 22 cases of insider threats reported by customers and bankers (see Appendix 13). Aspects of `insider threats` were discussed in Section 5.3.1 on **responsibility confusion**, referring to uncertainty as to the `boundaries of bankers' responsibilities`. Specifically, if a banker witnessed a case of insider threat to a customer, then he or she might decide not to become involved in `protecting customers` as potential victims or might prefer not to do so. Participating bankers explained that the source of such insider threats to customers tended to be a relative of the customer; the customer must have made the mistake of exposing his/her credentials and should therefore be personally responsible for protecting him/herself. Moreover, such cases tended not to be reported to the security committee of the bank concerned, illustrating

the `selective reporting of attack cases`. Participating bankers declared that they would not report cases where the attacker was known to the customer but would do so where the attacker was unknown. This subcategory is related to **gender roles** and is therefore to be discussed in Chapter 6.

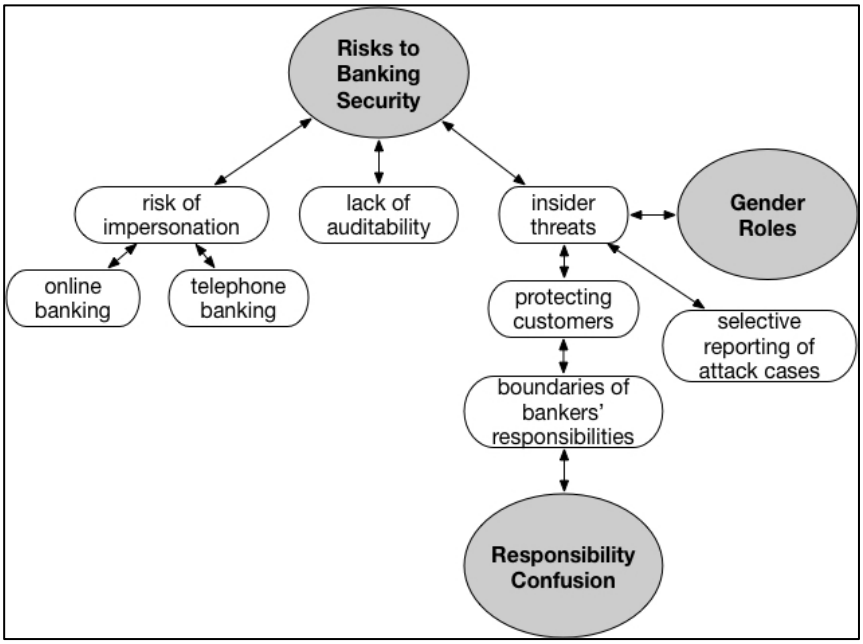


Figure 17: Risks to Banking Security.

5.3.4.1 Risk of impersonation

`Risk of impersonation` was found to apply to `online banking` and `telephone banking`. As explained in Section 2.3.3.2, registration for `online banking` with most banks requires the customer to choose a username/password, provide his/her mobile number, account number, card number and card PIN, then input a one-time authentication code which is sent to that mobile number; no physical authentication of the account holder's identity is required. Similarly, `telephone banking` registration requires the customer to provide an account number and national ID number and to choose a password, but this process does not require the account holder's identity to be physically authenticated. This risk of impersonation is high in this case, as a consequence of the lack of physical authentication and the widespread practice of sharing information. Different

impersonation cases reported by bankers see cases 10, 18, 20, and 21 in Appendix 13. For instance, case 10 reported by a female banker, P67, was that of two sisters: S1 and S2. S1 came to the branch to open a new account for herself, saying that she was expecting a money transfer from her sister, S2. After a few days, she received the transfer from S2's account. Sometime later, S2 came to the bank claiming that she had lost 26,300 SAR (£5,400) from her account. The detailed record of her account revealed that the money had been transferred to S1's account online. S2 was sure that she had not done this, because she had not registered for online banking. Since S1 and S2 shared bank credentials, as do most household customers, S1 had all the information she required to register her sister without her knowledge, then use online banking to transfer the money. Upon further investigation, it was discovered that S1 had registered S2's account for online banking with her own mobile number and misused this access to transfer the money. However, because S1 did not later change the mobile number, S2 and the banker were able to discover what had happened. This example illustrates a clear vulnerability associated with current enrolment practices in online banking, and the potential for any attacker (whether an insider or not) to exploit this weakness.

5.3.4.2 Lack of auditability

Only one banker mentioned poor auditability as a consequence of sharing credentials between household customers. Auditability, accountability and non-repudiation of banking activity are seriously compromised by the widespread practice of household customers sharing credentials with family members, making it no longer possible to assert that properly authenticated credentials uniquely identify a single individual, thus complicating both forensic analysis and fraud investigation.

Appendix 13 lists a number of cases where sharing credentials caused a lack of auditability, including case 19, reported by a male banker, P64, where a male customer

complained of missing 15,000 SAR (£3200) from his account. The customer said that he had not lost his card and had not shared it with anyone. An investigation revealed that the money had been withdrawn from the account using the card at three different ATMs. The authorities checked the CCTV connected to the ATM and it was found that the customer's son had withdrawn the money using his father's card without his permission, having taken the card while his father was sleeping. The father said, "*I am an old man ... every time I accompanied my son to withdraw cash for me from my account. Every time this happens in my presence"*. When the customer found that it was his son who had taken his money, he withdrew his complaint. P64 said that he did not know what happened after this. He also stated that the bank was not responsible for what had happened and that it was the customer's fault for having shared his credentials with his son. Moreover, because the father had shared his credentials, it had not been possible to determine whether he or his son had withdrawn the sums in question until the investigation was extended to checking the CCTV footage.

5.3.4.3 Summary

Figure 17 shows details of the three **risks to banking security** identified here: the `risk of impersonation` when registering for `online banking`; the `lack of auditability`, because when credentials are shared it is not possible to identify a single individual; and `insider threats` arising from the sharing of credentials. This last risk is closely connected with the issue of gender and is therefore dealt with in Chapter 6.

5.4 Chapter Summary

The model of the banking perspective (for detailed model see Appendix 10) shows that in the context of banking services in the KSA, with the unique feature of the existence of segregated branches, banks and their operations are influenced by gender roles. In

addition, banks strive to provide services compatible with the professional level of banking services available worldwide, although there is a need for them to review the education and training of bankers in newly launched services and the procedures for educating customers in the use of these services. Significant factors affecting banking in Saudi Arabia include confusion over defining responsibility for the confidentiality of credentials; banks should note that shifting this responsibility completely over to the customers concerned would neither solve the problem nor reduce the associated risks. Another important factor is the lack of physical verification of the account holder's identity during the registration of online and telephone banking, which increases the risk of impersonation; as a first step in addressing this weakness, banks must define bankers' responsibility for helping new customers to register for these services. The final essential factor is the lack of a procedure for protecting household customers in cases of insider threat, meaning a threat generated by a relative of the account holder. Because of the practice of sharing credentials found to be common among customers and because of the repeated cases of insider threats, banks must make serious efforts to address this problem. This complex situation in the current banking context causes possible risks to the security of both banks and their household customers.

This chapter has reported the grounded theory analysis of the data gathered in interviews with bankers. It has found that banking for household customers in the KSA is currently vulnerable to various risks that might compromise the security of banks and customers alike. This vulnerability is caused by three main factors: confusion about defining responsibilities, concerns regarding customers' authentication and finally, gender roles. This last factor is analysed in Chapter 6, which follows.

6 MODEL OF THE GENDER PERSPECTIVE

6.1 Introduction

As mentioned previously, the model of the household context of use of bank system in the KSA is a multi-perspective model compromising the perspectives of household customers, banking and gender. Chapters 4 and 5 have presented models of the household customers' and bankers' perspectives on banking security respectively. In both cases, the analysis revealed the significant role of gender, which is therefore detailed separately in this chapter.

As mentioned in Section 2.3.2, Saudi law, inspired by Islamic principles, adopts the binary view of gender as comprising male and female only, and the term 'gender' is used accordingly in this thesis to refer to the simple male/female dichotomy. In addition, many of the practices that this study examines are influenced by both culture and religion, which are difficult to separate, as argued in Section 2.3.1. This study therefore seeks to understand how participants invoke these large categories to account

for such practices using the principle of the qualitative methodology Membership Categorization Device Analysis (MCDA), whose aim is to understand how members of society invoke and use different categories to shape and describe the social world (Kelly 2008).

The building of the model of the gender perspective is discussed in Section 6.2, then, because gender is a factor affecting both household customers and the banks, Section 6.3 offers a grounded theory analysis of data collected from both sets of participants. The chapter ends with a discussion of the model and a summary in Section 6.4.

6.2 Model Building

The model of the gender perspective is concerned with the influence of gender on both household customers and banks, so the model was built on data elicited data from household customers and from bankers. As illustrated in Table 2, the household data were gathered using mixed methods in three rounds of data collection involving 47 household customers (see Section 3.6.1): in the pilot study; telephone interviews were held with six household customers: three males and three females. In the second round of data collection, four focus groups were conducted with 23 participants in total: six in the daughters' group, six in the wives' group, five in the sons' group, and six in the husbands' group. The diary/interview approach was adopted in the third round to collect data from six households, four having three members each, the others having four and two members respectively. There were thus 18 participants (nine females and nine males) in the third round of data collection. The benefit of using multiple methods is to triangulate the data to increase its trustworthiness and validity and to obtain multiple perspectives. In addition, the limitations of any particular method or the conditions of any of the rounds of collection would not confound the final results.

Then, there were three rounds of data collection with bankers, interviewing respectively four males and four females, six males and four females, and three males and two females, making a total of 23 bankers who participated in the interviews, as shown in Table 3 and detailed in Section 3.6.2.

As explained in Chapter 3, each interview and focus group session was audio recorded and transcribed in Arabic, then the transcripts were translated into English and analysed using ATLAS.ti. The three coding stages of grounded theory were used iteratively until theoretical saturation was reached. The full list of categories, subcategories and memos generated by the coding process is presented in Appendix 12. The final resulting model of the gender perspective is presented and discussed below.

6.3 Model of the Gender Perspective

The central theme of the grounded theory model focuses on gender as a factor influencing banking security. Four main categories have been identified from the data in which gender plays an important role: **Control, Infrastructure, Identity** and **Workaround**. The following subsections present the key points of each category, summarised in Figure 18.

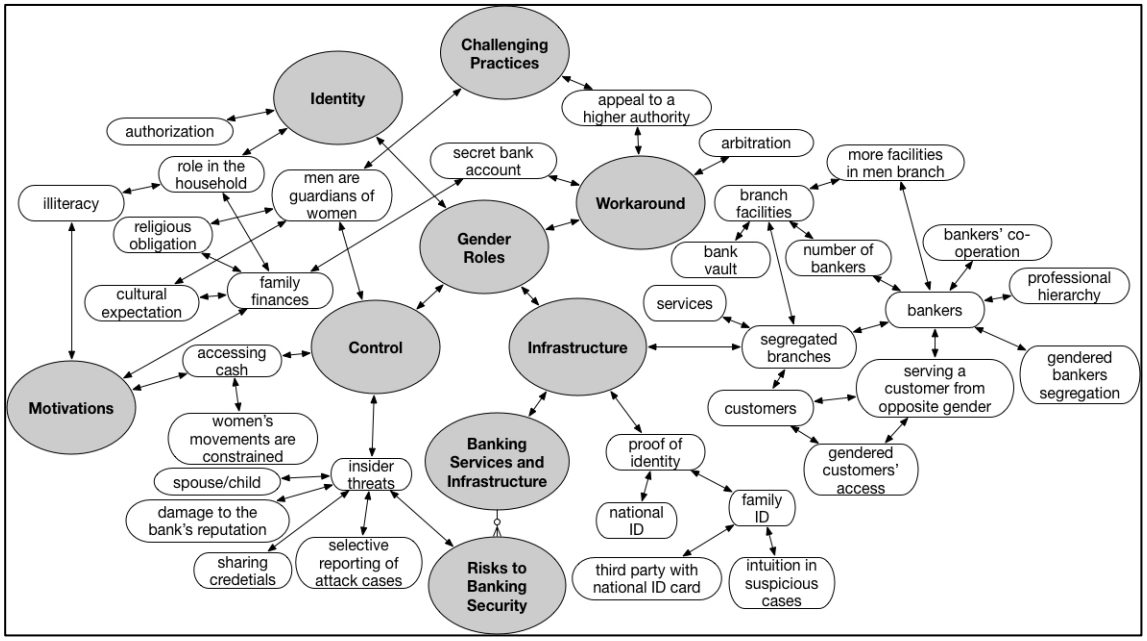


Figure 18: Model of the Gender Perspective.

6.3.1 Control

The data reveal a controlling practice grounded in two factors inherent in the male-dominant culture of the KSA: men's guardianship over women and constraints on women's movements. The following sections discuss the three subcategories related to control: `men are guardians of women`, `accessing cash` and `insider threats`.

6.3.1.1 Men are guardians of women

As explained in Chapter 2, Section 2.3.2, all Saudi women are required to have a male guardian; hence the subcategory `men are guardians of women`. This obligatory relationship is reflected in the dynamics of households, each of which is usually headed by a man who dominates the sharing practices of other members to some extent. This dominant person is usually the husband/father, or if the father is elderly or has died and the eldest son is old enough, then the dominant role passes directly to him and he is considered the father's successor. One reason for this is the combined `religious obligation` and `cultural expectation` that the male head of household is responsible for the family finances. It is common in Saudi families for a son to be raised with the

idea that he is his father's successor and that when the time comes he will be the one who manages the family's affairs. This expectation normally attaches to the eldest son, although in some families it may be the most trusted son, or the closest to his siblings, rather than the eldest, who succeeds his father. The data did not indicate that a female could be the dominant person except in one case: if her husband had died and the eldest son was too young to take care of the family, then the widow would govern the household and its banking until the eldest son turned 16 years old, when the widow would guide him and gradually begin to count on him to take care of the family's affairs. It would generally be the dominant person who would instruct other household members in financial matters and they would thus be expected to follow, among other things, his sharing practice. This practice would then be passed from one member to another. When other members followed the practice adopted by the leading person, it was found to take the form of **confirming practices**, but a family member could challenge the dominant person and adopt **challenging practices**, as discussed in Chapter 4, Section 4.5.4.

6.3.1.2 Accessing cash

As explained in Chapter 2, Section 2.3.2, `women's movements are constrained` by Saudi legislation which prevents them from driving and there are also restrictions on women walking unaccompanied. This is a very clear gendered difference that strongly affects a number of banking activities, but most evidently the routine banking practice of `accessing cash`. Gender and mobility restrictions lead to female customers being more likely to *share* their credentials with other family members to overcome these constraints. Because of these constraints, some female participants appeared to see sharing as a "*blessing*"; for them, sharing their bank credentials with a male family member resolved a major obstacle to withdrawing cash from their accounts. If a woman

needed to withdraw money from her account, she would go either to a bank branch or to an ATM. In either case, given the legal restrictions on the movement of unaccompanied females, she must use a vehicle driven by a chauffeur or mahram. If accompanied by a chauffeur, she could withdraw money herself from either a branch or an ATM, but if the vehicle was driven by her mahram then she might find that the ATM was on the driver's side; she would then feel obliged to hand the driver her card so that he could operate the ATM, because asking him to pull over so that she could walk to the ATM and withdraw the money in private would be inappropriate and unacceptable. A member of the wives' focus group said:

Sometimes I am with my husband in the car and he withdraws the cash for me because the machine is on his side of the car. [P20]

An alternative scenario identified was where a woman would ask her mahram to take her card and withdraw cash for her when she either could not accompany him (e.g. because it was too late in the day) or did not want to. A participant in the daughters' focus group said:

A girl shares her PIN with her brother to ask him to get cash for her from her account when she can't get out or she doesn't want to, but the brother doesn't need to share such information, because he goes out by himself. [P9, F]

Alternatively, sharing among females was said to occur for reasons of laziness or making life comfortable, as mentioned in 4.5.2.4. Thus, a female account holder might prefer to stay at home and ask a female member of her family to draw some cash on her behalf. A participating wife stated:

Sometimes I am lazy and I don't want to go to make a withdrawal. If for example I am at my family's house and my little sister is going out, I ask her to get me cash. [P21, F]

In this scenario, the wife is taking advantage of the fact that her sister is already going out accompanied by a chauffeur or a mahram, in order to avoid the effort of having to arrange this for herself. However, female participants saw trust as the main reason for sharing; only if trust existed would any other factors be considered, as explained by P22, a member of wives' focus group:

If you don't trust your family, would you give them your card? Even if you are lazy or there is a transport problem, you'd say 'No, I'll do it myself, even if I am tired'. If you didn't have this feeling of trust you would overcome your laziness and even the transport problem. You'd force yourself one way or another to go. I think that the first reason is that amount of trust between us, an excellent trust that makes me comfortable, and if I don't want to go it is easy to ask my brother to do it as long as there is no transport.

It is worth mentioning here that if movement restrictions did not exist, female participants stated that they would still share for other reasons, such as to make life more comfortable, albeit not as much as they did now.

The lifestyle in Saudi Arabia generally forces me to share my credentials with my husband or one of my brothers … I can't drive here and there is no public transport … and even if this situation changed, so there would be much less need for sharing, nevertheless I would still do it sometimes, to simplify my life. [P23, F]

6.3.1.3 Insider threats

22 cases of insider threats reported by customers and bankers (see Appendix 13). Bankers claimed that women rarely posed insider threats, because they are forbidden to drive, and because Saudi culture is male dominated.

I've witnessed many insider cases … mostly carried out by either husbands or sons … You know we are in a male-dominated culture and men control everything… I've never witnessed a case where the perpetrator was female… I think it would be difficult for a female to do this, especially with mobility limitations. [P66, F]

Most bankers also declared that they had witnessed cases of insider threats where the banker either could not or would not become involved in directly helping the victim, an example being the case reported by a female banker, P51, mentioned in Chapter 5, Section 5.3.1.1 (case 8 in Appendix 13).

Such cases of insider threats appear to be selectively reported to the banks' security committees. Bankers declared that they would not report cases similar to the one above, where the attacker is known to the customer, because it is the customer's personal responsibility to protect him/herself; bankers would report cases only where the attacker is unknown. Because of this `selective reporting`, there appears to be no official record of insider threats, although most bankers declared having witnessed many such cases. For example, a female branch manager stated that there were no official records of these cases, yet approximately five occurred each month in her branch, which served 200

female customers daily. Bankers argued that insider threats occurred because customers share credentials with family members, mostly to make their lives more comfortable, not expecting them to misuse this information or to present an insider threat, even when the customers know that it has happened to others. However, some bankers considered such threats damaging to the bank's reputation, because if an insider had performed an unauthorised transaction, the customer affected would first be likely to suspect that a banker had stolen money from the account, rather than immediately suspecting that the perpetrator could be a member of the family.

It discredits the bank, because the customer would not admit sharing credentials with anyone and he would accuse the banker of doing the transaction ... Any accusation against a banker is an accusation against the whole bank. [P53, M]

Both customers and bankers reported incidents where a spouse or a child misused shared credentials. If the insider is a spouse then this would usually be perpetrated by the husband. A female customer, P3, reported that her husband had twice misused her credentials but that she nevertheless continued to share her card PIN with him. When asked why, she replied that the misuse had happened four years earlier and she did not think it would happen again. Another female customer in the daughters' focus group, P10, reported the case of her sister who had designated her husband as a joint account holder; he misused his authority by taking out a loan of half a million SAR (£102,900), which the wife now had to repay.

On the other hand, most parents in this study declared that they saw no harm in sharing their credentials with their children, relying on the valued status of parents in Islamic and Saudi culture to prevent misuse, reinforced with other protection techniques such as keeping the card with the account holder at all times. Nevertheless, both customers and

bankers in this study described cases of a son misusing the credentials of his parents. For instance, P45 stated that her sister was illiterate and counted on her son to withdraw money; he withdrew more than his mother had asked for and kept the excess. The mother had kept her card with her at all times to protect and monitor her account, but this seems not to have been effective in this case.

In another example, P58, a female banker, described the case of a widowed mother who suffered from repeated insider threats from her son. He repeatedly took his mother's card without permission and withdrew the retirement pension of his deceased father. Because this money was the household's only income and the mother could not stop her son, the banker advised the mother to cancel the card and withdraw the money by visiting the branch. Although this solution stopped the son, it caused another problem for the mother, who had to travel to the bank to withdraw the money.

A third incident was recounted by a female banker:

A customer came to us two days ago. She was very angry and said that she would sue the bank because it had stolen money from her account … A detailed record of her account showed that money had been withdrawn from her account using her card in an ATM in Cairo. The customer became angry and said that she had not visited Egypt in two years …When the bank's representative suggested that her card might have been used by someone else "… your husband or your son… Has anyone from your family recently been to Egypt?", it was very clear that she had not thought about that possibility. Then, by comparing the date of the transactions that occurred in Egypt, she found that it was in the same period that her son was in Egypt with his friends … She admitted that she kept her card in her bedroom drawer with a piece of paper containing the PIN, online username and password. … She and the banker became more sure that

her son was the one who used her card when they checked the electronic services for her account. They found that he had changed his mother's mobile number to his, by using the information that he had found with the card. Once the mobile number had been changed, his mother would not receive SMSs for every transaction, so he could guarantee that she would not know what he had done. [P50, F]

6.3.1.4 Summary

The first category identified by the analysis where gender was found to have a major influence is **Control**. Because of men's guardianship of women, it would be expected for a household to be headed by a man, who would be counted on to take care of the family's affairs, and it would generally be the dominant person who would instruct others in the household. In addition, because women's movements are constrained in the KSA, there would be a series of obstacles to obtaining cash easily. Finally, the male-dominant culture was found to motivate some men to threaten women's banking security.

6.3.2 Infrastructure

The KSA banking **infrastructure** was discussed in Chapter 2, section 2.3.3.2 (Figure 2) and we discuss here those aspects of it where there are clear gendered differences: `proof of identity` and `segregated branches`.

6.3.2.1 Proof of identity

As mentioned in Section 2.3.3.2, all male customers are expected to have a `national ID` card to prove their identity, but the same is not true of female customers: 14 (58%) of the 24 female household bank customers participating in the present study had no national ID card, the data having been collected before November 2016, when Saudi law changed to require all females aged 15 years and over to hold one (Thakefni 2016).

In order to prove their identity in bank branches, those female participants without a national ID card used the `family ID` card and this involved the confirmation of their identity by a `third party with national ID card`, as explained in Chapter 2, Section 2.3.3.2. In most cases, this would be supported by a husband or a brother producing his national ID in the adjoining men's branch. However, one of our female participants reported always asking a female friend who held a national ID card to accompany her to the women's bank branch to confirm her identity.

When bankers were asked about female customers using family cards for identification, they noted that this procedure was open to fraud and some expressed the view that responsibility in such cases lay with the national ID cardholder who attested to the woman's identity. Interestingly, some bankers also referred to relying on `intuition in suspicious cases`, when they might seek to verify a customer's identity by asking her additional questions about the account, such as how much money was in it or when it was opened. The banker might also estimate the customer's age from her appearance and compare this with her date of birth given on the family card. However, one female banker, P61, illustrated a weakness of this method of verification by recounting the anecdote of a female customer who came to a branch to open a new account, saying that she was going to start studying at university and needed this account to receive the monthly allowance from the university. She did not have a national ID card and instead provided the family card, with her father supporting her claim by showing his ID in the men's branch. The banker noticed that the customer was claiming to be 18 years old, although from her face she appeared at least 40. After the customer left the branch the banker reviewed the papers and found that the customer was claiming to be her own younger sister, who was registered on the family card and was aged 18.

Another example of this kind of fraud was recounted by a female banker:

This case happened to my friend … a customer service officer in [bank X]. *... A female customer came to the women's branch to apply for a loan, claiming that her name was Sara and that she held an account at the bank. Sara did not have a national ID card, so she used the family card and her husband, Ahmad, was in the men's branch to support her claim. The banker did not suspect anything and Sara signed all the appropriate forms. The banker then told her that it would take two working days to process her loan application. Two days later, another woman came to the branch claiming to be Sara and asking about an SMS from the bank saying that the loan requested had been granted and inviting her to visit the branch, which surprised her because she had not applied for a loan. While the banker was discussing this problem with the second customer, the first woman came into the branch. Both claimed to be Sara, so the banker closed the main door of the bank branch to prevent either of them leaving and called the police. It turned out that both women were married to Ahmad, who was planning to steal money from his wife Sara with help from his other wife.* [P55, F]

Unfortunately, the banker did not contact the customer after that and was unable to say what had happened to Sara or how this incident had affected her relationship with her husband. It is worth mentioning here that what saved Sara in this case was the SMS notification that informed her about the loan. If the second wife had changed the saved mobile number to her own before applying for the loan (see Case 12 in Appendix 13, where a son changed the saved mobile number so that he could use his mother's credit card without her being alerted by SMS), then Sara would not have known anything was amiss until the first instalment became due. This confirms that the use of SMS notification to monitor the account is reliable to some extent, but that there is a weakness in this mechanism. To rectify it, banks should consider requiring that before

the account holder's mobile number could be changed to a new one, an SMS must be sent to the saved mobile number to notify the customer of the change.

It should also be noted that in the above case, when the banker noticed that something was wrong she responded immediately by detaining both women and calling the police, but this did not happen in other cases of insider threats, where bankers often did not respond at all, having no clear procedure to follow as discussed in Section 5.3.1.1.

6.3.2.2 Segregated branches

All of the bankers who participated in this study affirmed that men's and women's branches provided exactly the same services to their customers, including opening accounts, making withdrawals, depositing or transferring money, issuing cards and providing loans. Bank branches in Saudi Arabia are segregated by gender for both customers and bankers, so women cannot work in men's branches and vice versa. To serve a customer of the opposite gender, male and female bankers help one another; for example, a female banker [P57] stated that her uncle had applied for a loan through her to help her reach the monthly target set by the bank. The uncle completed the necessary forms in the men's branch with help from a male banker, who checked the identity of the uncle then sent the forms to the women's branch for P57 to process.

Participating bankers made it clear that women's branches are not subordinate to men's branches and that a female branch manager is not inferior to the male branch manager in the professional hierarchy, but works at the same level. Furthermore, a female banker has the same authority as any male banker in the same position; a female branch manager, for instance, exercises exactly the same authority as a male branch manager. However, there are usually fewer employees in a women's branch, and bankers explained that men's branches tend to be larger because there are normally more male

than female customers. In addition, bankers agreed emphatically that a male customer cannot in any circumstances gain physical access to a women's branch, but that banks differ in their policies regarding access for female customers to men's branches, which some allow and others prohibit. Even if the bank does permit a female customer to enter a male branch, she must be accompanied by a mahram or be willing to uncover her face for identification.

A relevant incident was reported by P40, the wife in household 4, who insisted on having access to the men's branch to renew her card. According to this participant, her card had expired and when she visited the women's branch the bankers told her that the system was down and that they could not serve her. She explained that she urgently needed to renew her expired card because she was going abroad the next day. She was advised to go to the men's branch next door but was stopped at the door by a security guard, who told her that women were prohibited from entering. The participant insisted and after consulting the branch manager, the security guard led her to the manager's office. The participant reported feeling tense and awkward as male customers stared at her through the glass wall of the office. When she had completed the application form, the manager asked for the participant's national ID to prove her identity. The manager was embarrassed to ask the participant to uncover her face to verify her identity, as in common with most women in Saudi Arabia, she wore the hijab. After waiting for 10 minutes in the manager's office, the participant finally received her new card.

Each bank branch usually comprises separate men's and women's branches, situated in the same building. Each men's branch will normally have safety deposit boxes and a `vault`, while its associated women's branch will not have a vault, and smaller women's branches will have no safety deposit boxes either. The `bank vault` in the men's branch thus also serves the women's branch. Each morning, the operations manager of the

men's branch will pass a certain amount of money to his counterpart in the adjoining women's branch; if the latter is a small branch, the operations manager and the branch manager will be the same person. At the end of the day, the female operations manager will return any money held in her branch to the male operations manager for storage in the vault. The reason for not having separate vaults, according to participants, is that cash will be supplied every morning by SAMA, whose employees are mostly men who therefore cannot have access to women's branches.

In some locations such as villages, there may be a men's branch without a women's section, but the opposite does not occur. As a result, several household bank customers reported that a man could singlehandedly open a new bank account for one of his female relatives in the men's branch by filling a form, providing the female's national ID or the family ID card, and showing his own national ID.

6.3.2.3 Summary

Overall, the **infrastructure** of banking in the KSA differs between genders. An example is the use of family ID cards to verify female customers' identity, which represents a major threat to women's banking security in that the procedure is clearly vulnerable to the account holder's impersonation by another woman. A further way in which gender influences banking infrastructure is in the segregation of branches.

6.3.3 Identity

The category of **identity** has two sub-categories: `role in the household`, which can shape the banking practices of household customers, and `authorisation`, which was also found to be affected by gender.

6.3.3.1 Role in the household

The data show that banking practices differed according to the account holder's role in the household. Thus, the banking practices of a daughter would be different from those of a son; likewise, the banking practices of a mother and a father would not be the same. For example, it was found that daughters and sons behaved differently and had different expectations with regard to sharing their bank credentials with their fathers. According to the participants, a daughter was more likely than a son to share her account credentials. A member of the wives' focus group said:

It is hard to refuse such a request even if I want to … I can't say no or I will lose my father … he will say 'I spent all my life supporting you and bringing you up and now you don't want me to have an authorisation on your account'. … Even if he takes all the money … you and your wealth belong to your father. [P20, F]

The participant here was quoting a Hadith which states: "You and your wealth belong to your father." This Hadith, which was mentioned by many participants in all four focus groups, refers to both daughters and sons. Although the hadith does not distinguish between sons and daughters in this matter, participants asserted that there was a difference in cultural norms between daughters and sons; as a member of the daughters' focus group said, "*a daughter is always under her father's wing*". This describes the relationship between a father and his daughter, asserting that she must always be under his supervision. When invited to consider the case of a father asking his daughter to share her bank credentials with him or to give him control of her bank account, all focus group participants (with one notable exception in the daughter's group, as explained below) declared that they could not refuse such a request, as to do so would be a sign of disrespect and ingratitude. Most participants felt that any such request would be made in the best interests of the daughter to monitor the use of the account and to protect her, as

mentioned in Section 4.5.1. Indeed, when one member of the daughters' focus group declared that she would refuse such a request because she considered her account and its information to be private, all other members of the group disapproved of this declaration, despite her asserting many times that her father was an open-minded man who would accept this refusal from his daughter and respect her privacy. However, some cases were identified where a daughter could refuse her father's request for sharing and where such a refusal would be acceptable, for instance when the father had misbehaved socially or economically in the past (see Chapter 4, Section 4.5.4).

Participants stated that boys were seen as different from girls and that this difference appeared to be more cultural than religious. The difference is that a son could legitimately refuse his father's request to share details and in this case, the father would accept the refusal and consider it a sign of maturity in his son. However, there was some disagreement among participants, with some saying that even boys would not refuse to share authority with their father as a sign of respect. Others recognised that there was a difference but believed it to be based on other factors. P29, a member of the husbands' focus group, said:

There is a difference, but it's based on caring and sympathy, that a father cares more for his daughter than for his son. This means that she might not be able to go to government offices but the boy can look after himself, so the father can share the credentials of his daughter's bank account to look after her needs.

A further difference in banking practices based on the account holder's role in the household is between mothers and fathers. A new pattern of sharing was identified from the data, where both a daughter and a son would use the parent's card for ATM or

EFTPOS transactions. However, because of women's mobility restrictions, it was more likely for a son to use his parents' accounts.

I don't know the PIN for my mum's card, but my brother does… She always counts on him to get cash from her account at any time but I can't… Even my younger brother knows the PIN of my mum's card. [P37, F]

The mother in this household thus counted on her sons, but not her daughter, to draw cash from her account, largely for convenience reasons. This pattern of children using their parents' accounts in order to help them was repeated frequently in the data for different reasons. Another reason for this pattern of sharing was to make life easier:

I know how to use my card at an ATM or a sales point... I used to do everything when my son was young, but since he grew up he has always used my card and keeps it with him all the time, to make things easier for me. [P45, F]

The above participant stated that when her son was young she did all her own banking. Being a widow, she used to have her brother take her to a bank branch, but she did not share her credentials with him. Now, by contrast, she allowed her son to keep her card at all times and said that he even received the SMS notification of each transaction. She was satisfied with this arrangement, despite being aware of cases of misuse among her relatives:

My sister had a problem of abuse of trust once with her son … But thank god, I know my son. I raised him well and I know he will never take money from anyone… He fears God. [P45, F]

When the son was asked about this, he said:

It started when I was 16, I think. I had a car and had started driving… I felt I had grown up and become a man. Frankly speaking, I started to take all the family responsibilities. I thought of myself as the man of the house, as you may imagine, especially as I was the only male in the household. [P47, M]

The mother in the above example was educated and employed, so she had no practical need to share her credentials with anyone. However, the same pattern of practice occurred in the data but for a different reason: `illiteracy`. A mother would rely on her children for all her banking transactions, because she could not read or write:

I would say that because I can't read or write, I have no knowledge of banks or things that are related to withdrawal or deposits, and my sons do all these activities for me. [P33, F]

This mother kept her card with her at all times and handed it to one of her sons only if she needed to have access to her bank account, to deposit or withdraw money. Because of her illiteracy, she did not know how to use an ATM card, but she could use cash. She said:

To be honest, I don't know anything about ATMs or about the card. If I go shopping with my son, he will use my card at the sales point. If my son is not with me then I can pay in cash.

When asked about this, her eldest son said:

I do all the bank transactions for my Mum … I also used to do this for Dad before he passed away… I started doing this when I was sixteen years old and I didn't have an account myself at that time… My [older] half-brother … got married and became busy,

so there was nobody to help the family. And my father didn't know how to use an ATM … so he counted on me to withdraw money for him and the rest of the family. [P34, M]

When the mother was asked whether the security of her account was affected by sharing her credentials with her children, she said:

I have the card with me all the time and when I need money I give it to them. They've never taken it without telling me. [P33, F]

Thus, the mother protected her account by keeping the card with her and giving specific permission for each transaction, which is a way of protecting a bank account mentioned by many participants (see 4.5.2.2 for more information). However, literacy does not always refer to the written word; in some cases, a parent may be able to read and write but have poor IT literacy, finding it difficult to use an ATM or a bank card. It is unsurprising that an illiterate parent would share bank credentials with a child, who would most likely be a son because of the movement restrictions discussed above. Another gender difference is that a parent who shares because of poor IT literacy is most likely to be a mother sharing her credentials with her children. The same movement limitations mean that a woman will have had less opportunity to visit an ATM to use her card by herself; she is therefore likely to consider it unnecessary to learn to use this technology.

6.3.3.2 Authorisation

Gender was found to play a role in customer authorisation, where bankers appeared to be more amenable to female customers than to males. Three incidents support this finding. In the first, P37, the daughter of household 3, explained that she used her mother's card for shopping and when the card expired she went to the bank branch to request a new one. After showing her own and her mother's identity cards and

completing the necessary forms with her mother's information, she was given a new card, without the mother ever being present. A similar incident mentioned in case 17 in Appendix 13.

This contrasts with an incident involving male customers. P39, the husband in household 4, reported that he had encountered difficulties in using online banking to transfer money from his account to that of his brother. He went to the branch and the banker who investigated found that the participant had entered the wrong IBAN code for the brother's account. When the participant asked for the correct IBAN, the banker refused to reveal it, stating that it was confidential information which could be given to the account holder only.

One implication of the case of P37 and case 17 that it shows the bank colluding in some cases in the 'illegal' sharing practices of household customers; however, the data are insufficient to identify the consequences of this collusion and to determine whether the bank would be liable and share responsibility with the customer or whether, as stated in Section 5.3.1.2, the entire responsibility would be shifted onto the customer.

6.3.3.3 Summary

The data show that an account holder's `role in the household` can shape his or her banking practices and expectations, in that a daughter or a mother will adopt different banking practices from those of a son or a father. On other hand, `authorisation` can be granted more easily for women than men, because of bankers' understanding of the cultural constraints affecting women.

6.3.4 Workaround

The **Workaround** category combines the findings regarding two interesting practices adopted by bank customers in the KSA where gender has a great influence: `appeal and arbitration` and `secret bank account`, as explained in the following subsections.

6.3.4.1 Appeal and arbitration

From a gendered perspective, differences were noted in the reported instances of a bank customer `appealing to a higher authority` as a means of protecting themselves from undesirable activities. For example, a wife can appeal to her parents to stop an insider threat from her husband, but the opposite situation is unlikely to arise: if the husband suffers an insider threat from his wife, he can usually address the threat directly by no longer sharing his credentials with her and does not need to appeal to his parents, especially because the husband is usually the head of the household. A participant in the daughters' focus group recounted that her friend had assigned her widowed mother as a joint account holder in order to protect her inheritance from her husband. The husband had repeatedly tried to convince his wife to give him part of her inheritance so that he could use it to expand his business. To avoid direct conflict with him and to protect her money, the wife passed control of the account to her mother. The husband now recognised that his mother-in-law was supervising her daughter's account and monitoring every transaction, which stopped him from attempting to convince his wife.

Another pattern was where a victim of such misuse appealed to the arbitration of family or tribe members for resolution. The system of tribal relations has a fundamental influence on Saudi life and practices; a person's tribe is seen as a source of support and security and can be used in certain cases to `appeal to a higher authority` or for `arbitration` in contentious cases. Two incidents recounted by the participants fit this pattern. The first involved an illiterate father-in-law who shared his credentials with his

son-in-law, whom he later found to be misusing his credentials by withdrawing money without permission. The victim asked his daughter to support him by divorcing her husband (the misuser); when she refused, the father disowned her. He then sought help from his tribe and family, was successful in recovering his money and stopped sharing his credentials with anyone.

The second case of arbitration was recounted in the third round by P34, a son in the second household (Table 2), who was asked by one of his female relatives to help her retrieve her bank card from her husband. The husband had kept his wife's card with him at all times and used her account without her permission. She was unwilling to confront her husband directly because she was afraid that he would divorce her[7], so she sought the help of her tribe and her family while keeping this appeal secret from her husband.

When my cousin asked me to talk with her husband about this matter, she asked me not to reveal that I knew about what he was doing… because she thought this would make the situation worse by revealing a secret of their house… Instead, she asked me to approach him indirectly by saying that this practice by a husband is forbidden in Islam and would be a mistake. But this did not work, and he is still using her salary as if it was his own money… My poor cousin … She could not even ask for money for herself from her account, but to get some money from him now and then, she says that she

[7] Culturally, Saudi society accepts a divorced man more readily than a divorced woman. A man can usually divorce his wife without bringing shame on his family, but the converse is not generally true.

needs money for charity purposes and of course she uses the money for herself. [P34, M]

Thus, seeking familial or tribal arbitration was not successful in this case and the security and control over the woman's bank account remained compromised. Comparing these two cases shows a clear gender difference in the practice of seeking help from family or tribe members. The male victim in the first case was successful in resolving the threat to his account in this way. He even expected his daughter to support him in this matter by divorcing the perpetrator. Moreover, in this case the victim (a man) sought help directly from the head of his tribe (always a man) without any fear of bringing shame on his family for revealing or sharing private family matters. Conversely, in the second case the female account holder could not plead her case directly to the head of her tribe. Because of the fear of being divorced or bringing shame to her family, she restricted her request for help to close family members only. While we cannot generalise from these two examples, anecdotal evidence indicates that men are more successful than women in resolving problems through arbitration.

In a final case, P41, the mother in household 4, had a husband who kept her card and used the account without permission for a long time and without any objection from her. However, after discussing this situation with female colleagues and under social pressure from them, the wife sought to change this situation and to keep the card with her. After a long and heated discussion with her husband, the wife managed to retrieve her card and keep it with her at all times, but still shared her credentials with her husband. It is important to highlight in this case that the social pressure was from women who were not happy with such male dominance.

6.3.4.2 Secret bank account

The data show that male account holders commonly have more than one account, sharing the access credentials of one of them with the family, while at least one other account is considered private and its credentials are not shared. One reason for this practice is the `religious obligation` and `cultural expectation` that the male head of a household is the guardian of his family and thus responsible for the `family finances`. As a way of controlling family expenditure while maintaining his financial independence, a man will have one account specifically for family expenditure and a separate personal account. Access to the family account will be shared with his family and he will transfer money monthly to it from his private account. A consequence of this practice is that a woman has no independent way of knowing how much money her husband has in his account.

However, in some cases the man's personal account is not merely private but secret, its existence hidden from the family. Husbands having secret accounts were seen as quite common and many wives accepted it. A member of the wives' group claimed that this was done for control rather than through distrust:

The problem is not lack of trust between them, but for instance he might want to build a new house or expand his business and if his wife knew how much he had in the bank she'd ask him to buy new furniture for their home or something else… and in fact that's what we actually do. [P19, F]

Another member of the same group thought that it was a matter of privacy for her husband, who had the right to keep his balance secret:

If he insists then it is his personal freedom. I shouldn't interfere. If he insists this is his affair, he can say: 'You have your needs and I fulfil them and you don't have to know my stuff. You can't interfere'. [P18, F]

However, not all wives accepted this practice:

Normal? I don't see it as normal. I do not consider it normal to have two accounts, because sharia says that he has to pay for my expenses. This is … a religious obligation … and I don't permit anything except what our religion permits. [P22, F]

Owning a secret account is clearly gendered in our data, as only men reported this practice. Some female participants reported not sharing the credentials of their own accounts as a means of keeping the account private, but hiding its existence altogether would be significantly harder for a woman. This can be explained in our model by reference to the categories of **Control** and **Infrastructure**. The realities of **control** mean that if a woman wants to open an account, she needs to overcome the guardianship of men over women, which requires her to have the permission of her guardian (husband, father or a brother) to visit a bank branch. Moreover, the mobility restrictions on women make it difficult to open or operate a secret account, since a woman cannot walk to the bank branch alone but must use a vehicle driven by her mahram. Thus, even her physical movements cannot be private. It follows from the nature of the guardianship system and the movement limitations imposed on women that using a secret bank account, for example to withdraw cash from it, is likely to lead to its discovery. Finally, the **infrastructure** hinders the freedom of independent (and therefore of covert) action of a woman who does not have a national ID card by requiring her to use the family ID card and her mahram (or a female friend) to support her claim.

6.3.4.3 Summary

The category of **Workaround** combines the findings on two practices adopted by bank customers: `appeal and arbitration`, mostly adopted by women to stop men threatening their banking security, with mixed success, and having a `secret bank account`, a practice seemingly restricted to men by the constraints on women of **control** and **infrastructure**.

6.4 Chapter Summary

As observed in Chapter 2, Section 2.5, the security of a system depends on its components operating within expected parameters. The banking systems and policies in operation in the KSA are modelled on Western banking systems and policies. Implicit in these are presumptions of equality and freedom of choice for men and women, which are thus specified without explicit consideration of gender. As we have seen, however, the context of use of KSA banking systems results in clear differences in the privacy and security of banking practices of Saudi men and women, despite the official policies and specific design of these systems being agnostic of gender.

Our model shows the key differences to be linked to four concepts (see Figure 18): **Control**; **Identity**; **Workaround**, which is different in practice for men and women; and the banking **Infrastructure**, particularly the availability of women's branches in rural areas, which makes accessing services more difficult for women. This leads individuals, predominantly women, to adopt compensatory practices, the most evident being sharing credentials as a means of overcoming mobility restrictions, but also appealing to informal higher authorities or arbitration in cases of dispute.

From a security perspective, we have evidence to suggest that insider threats to household customers arise relatively often but that these are not typically reported

within the banking context. These are enabled by the common practice of sharing credentials, by the availability of a family ID card that does not provide facial information about all family members for `proof of identity` and by the difficulties in accessing a women's branch (arising from mobility restrictions and from the **infrastructure** lacking women's branches in rural areas), which can lead to bankers facilitating practices where men act on behalf of their female relations. As a result, insider threats are more likely to result in fraud being committed by men than by women; participating bankers claimed that such offences were usually perpetrated by male children and spouses, although there is no official evidence to support this claim. The incidents of insider threats to household customers are not routinely recorded, as bankers shift responsibility for such incidents onto customers and the sharing practice that appears to be very common among them.

When disputes arise (whether from an insider threat or not), the mechanisms for resolving them are also uneven for men and women; in the case of a man having a dispute with a woman, the cultural norm of men being guardians of women tends to result in the man prevailing. Having said that, we uncovered cases of women subverting this by `appealing to a higher authority` in order to override the man's wishes (as seen in the example of a daughter who appealed to the authority of her mother to protect her inheritance, or in the case of the banker recommending that a female customer should contact her brother to avoid having to take a loan and giving it to her husband). Given our sample size, it is impossible to say how common this behaviour is, or how successful it tends to be, as we also saw evidence of women calling for arbitration from the family or tribe, but without success.

The insider threat problem is more elusive and perplexing than any other threat. Assessing the insider threat is the first step in determining the likelihood of any insider

attack. Technical solutions do not suffice, since insider threats are fundamentally a people issue. Therefore, in order to facilitate the prediction of insider threats and pre-empt any insider attack, thus improving the security of both banks and their customers against such threats, it is essential to adopt a three-pronged approach that makes assessments of technological issues, of customers' practices and of bank policies. Most participating bankers admitted being aware of many instances of insider attacks, but appeared to place the whole responsibility for these on their customers.

Based on the three separate models already discussed, of the customer, banking and gender perspective, a household context of use of bank system in the KSA will be build and present in the following chapter. This would form the first part of of the conceptual framework. In addition, chapter 7 discusses the building of this framework and its use to evaluate the security of household banking in the KSA.

7 A Conceptual Framework for Evaluating the Security of Household Bank Customers in the KSA

7.1 Introduction

As described in the three previous chapters, the grounded theory analysis of the data collected from household customers and bankers was used to build a multi-perspective model of the household context of use of the bank system in the KSA, from the perspectives of household customers, banking and gender, as depicted in Figure 19 (for a detailed model, see Appendix 11).

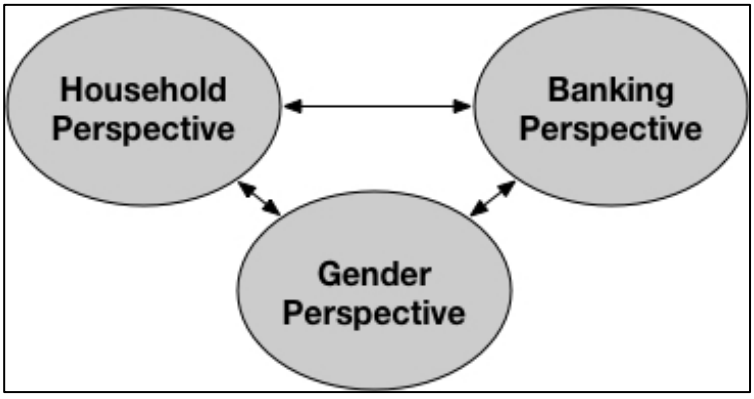


Figure 19: Household context of use.

The household context of use constitutes the first block of the framework for evaluating the security of household customers. As mentioned before, a key aim of this thesis is to present a conceptual framework for evaluating the security of household bank customers in the KSA, comprising the three essential building blocks depicted in Figure 1 and reproduced in Figure 18: the household context of the use of the bank system in the KSA, the Saudi banking policies and infrastructure that guide the use of the system, and banking technologies and processes. The motivation for this, as stated in Section 2.2, is that banks can be considered to be socio-technical systems, using computer technology to provide technical services that are used by millions of bank customers daily. To ensure the secure use and operation of such systems, their technical and social components must operate in harmony and these must also be considered when building a framework for evaluating security.

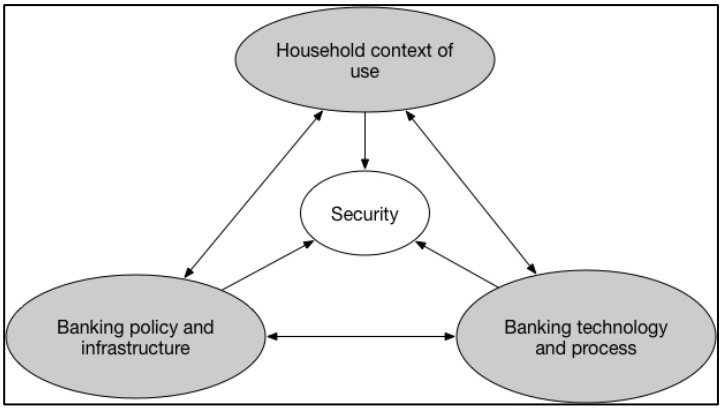


Figure 20: Framework for evaluating the security of household banking.

Section 7.2 presents the integrated model of the household context of use of the bank system in the KSA, constituting the first block of the framework for evaluating the security of household customers. Section 7.3 presents the second block, concerning Saudi bank policies and regulations affecting household customers. Section 7.4 deals with the third and final block, a security analysis of banking technology. The chapter ends in Section 7.5 with using the framework to evaluate of the security of household

banking, by applying the framework to two case studies. The first, presented in Section 7.5.1, evaluates the use of fingerprints as a new security mechanism with an existing technology, in the authentication of bank cards, whereas the second, discussed in Section 7.5.2, concerns the application of the framework to evaluate the security of mobile banking, a technology not used by the household customers who participated in this research.

7.2 Household Context of Use

In the household perspective, the analysis of the data revealed that the overall banking activities of household customers included online banking, telephone banking and the use of bank cards in ATM and EFTPOS transactions. An important banking practice, adopted by a large majority (87%) of participating household customers, both male and female, was the sharing of control over their accounts with family members and it was concluded that the only possible way of doing this was by sharing credentials. Customers did not necessarily regard this sharing practice as problematic, because they had an alternative understanding of security. Rather than being about transactions and privacy, these security practices were seen as relational, affective and emotional, being grounded in family ties, relationships and human values such as trust and religious adherence. In addition, different factors cited as motivating or justifying the practice of sharing included trust, the need to back up this important information, poor IT skills and there being little money in the account. Only three participating household customers of each gender chose not to share control over their accounts and to keep their credentials private. While the banking perspective constructed from interviews with bankers revealed that they were aware of the widespread sharing of credentials and the consequent vulnerability of customers and bank systems, they identified no effective procedures to stop this practice or even to minimise the attendant risks. As gender

segregation affects almost all aspects of life in the KSA, it was found to exert a strong influence on the household context of use of the bank system.

Given the current design of banking systems, sharing credentials is the only way for customers to share authority over their banking activities. Consequently, the auditability and non-repudiation of the banking activity are seriously compromised, because it is no longer possible to assert that properly authenticated credentials uniquely identify a single individual. A more flexible system, allowing explicit or implicit sharing of control, with different levels of permission, may prove to be more suitable to the needs of household customers. However, as with any authorisation mechanism, usability is a key issue: the additional security gained by protecting the identifiability of someone with the correct credentials needs to be weighed against the additional effort involved in sharing account control. Should the system of sharing account control prove complex, time consuming or unwieldy, it is unlikely that the current situation of credential sharing will improve. The use of a joint account for family expenditure may offer account holders an alternative to sharing the credentials of one of their accounts. However, our survey indicates that joint accounts are not widely used in the KSA, since only one of the 60 running bank accounts held by the 47 household bank customers in this study was a joint account. We can speculate that gender segregation makes it more difficult for a man and a woman to open a joint account, because they would both need to be present in a bank branch; a personal account held by one of them who shares its credentials will be significantly more convenient, as it can be opened more easily.

We would also like to highlight a subtle but very important issue regarding the ethical implications of trying to reduce the extent of credential sharing through policy and technical means. If changes were introduced to allow the sharing of authority while avoiding the total sharing of credentials, there is an argument that this might help to

protect individuals from fraud by ensuring that they remain in control of their banking activity. However, adopting this solution without consideration of the practical aspects of accessing banking services (which is currently significantly more difficult for women than for men) might cause additional problems that would need to be considered carefully and would be likely to undermine the effectiveness of the control. Furthermore, by providing the means of sharing control, the banks could be seen to be tacitly endorsing the sharing of control over accounts, thus weakening the arguments of those who may not wish to conform to the sharing practices of their household.

This investigation has revealed examples where the concept of privacy in the KSA does not always apply to individual privacy. A key factor underlying this is the strong influence of existing values related to gender roles and family hierarchy, most notably the guardianship of men over women. In a society where individual freedom, responsibilities and obligations operate to a diverse series of interrelated norms (cultural, social and religious), issues of privacy need to be considered accordingly. For example, in revealing their perceptions of privacy, participants placed strong emphasis on keeping family affairs private, with less emphasis on individual privacy. This was also evident in the sharing practices prevalent within familial hierarchies, where PINs and bank accounts were found to be shared with family members, but not with anyone outside the family. This opens up interesting new avenues of thinking around privacy for such cultures, where local practices suggest a more collective view of the concept, in contrast to a more individualistic viewpoint.

This section has presented the first block needed to build the framework for evaluating the security of household bank customers in the KSA; the next section considers the second block, regarding banking policies and infrastructure.

7.3 Banking Policies and Infrastructure

The second important element of the framework that this study seeks to build concerns banking policies and infrastructure which drive what banking technologies are available and how they operate. Details of the infrastructure of Saudi banking are given in Section 2.3.3.2, the main points being that there are 12 domestic banks supervised by SAMA and that the religious and cultural constraints mentioned in Section 2.3 oblige them all to have separate men's and women's branches, access to the latter being limited to female employees and female customers. Meanwhile, policies govern practices; therefore it is essential to review and include in the framework all banking policies relevant to household banking. Policies and regulations serve as a guide to making decisions when using a system (Sloman 1994), informing users of these systems which activities are acceptable and which are not. This stage of the research involved a deep analysis of the official policies and regulations related to the household context of use of bank technologies issued by SAMA as the leading authority of the Saudi banking sector; the following subsections present and discuss these policies.

7.3.1 Proving the identity of household customers

As noted in Chapter 2, Section 2.3.3.2, in order to make use of the services offered by a bank branch, SAMA's rules require the customer first to prove his/her identity by presenting a national ID card (SAMA 2012). However, some female customers do not have one, so to prove her identity such a customer must show the family ID card and engage a relative or a female friend (as women are not allowed to be accompanied by unrelated males) with a national ID card to support her claim.

7.3.2 Educating customers

The third of SAMA's Consumer Protection Principles, that of financial education and awareness (SAMA 2013) states:

> *Banks should develop the appropriate knowledge and skills of current and future customers, raise their level of awareness, guide them to an understanding of the basic risks, assist them in making effective decisions and direct them to the appropriate body in case they need more help.* (p.7)

The importance of this principle is indicated by its being repeated in sections 6 and 19.1 of the document. It refers to educating consumers about financial protection in general. The same document requires banks to educate their customers in specific financial matters such as the consequences of opening a bank account (section 11.5), the importance of bank cards and cheque books and the procedures in case of loss or theft (section 13.7) and choosing secure PINs and passwords for bank services (section 13.12).

The principle of consumer education also appears in section 3.2 of the Electronic Banking Rules (SAMA 2010), in reference to online banking services:

> *Banks must develop and implement education programmes about e-banking services to educate customers before using the services*. (p.11)

7.3.3 Bank credentials

SAMA regulations warn customers against sharing bank credentials and emphasise the responsibility of both banks and customers to protect their credentials (SAMA 2010, SAMA 2013). For instance, section 3.3 of the Electronic Banking Rules (SAMA 2010) clearly states that

> *…banks are responsible for providing secure and safe systems and services for their customers unless the customer fails to safeguard their account user number or password and divulges it to a third party.* (p. 14).

Similarly, the Consumer Protection Principles (SAMA 2013) forbid customers to reveal their online credentials to anyone, including bankers:

> *Customers must not share their online credentials with anyone. In addition, customers must not reveal online credentials (username or password) to bankers.* (p.11)

7.3.4 Bank cards

In addition to making banks responsible for educating customers about what to do if a bank card or cheque book is lost or stolen, sections 13.1 and 13.2 of the SAMA regulations state that bank cards must be issued and delivered only to the account holder or to a delegated person assigned formally by the account holder. It is standard practice for the bank to issue an ATM card to the holder of a newly opened account, but a credit card must be issued only upon the request of the account holder, as stated in section 13.5 (SAMA 2013).

7.3.5 SMS notification service

Section 14 of the SAMA regulations, Bank Services via Internet and ATM (SAMA 2013) contains guidelines for banks on using all possible means to protect customers using online banking and ATM services. One of these means is to send SMS notifications to inform account holders of all transactions.

7.3.6 Section summary

This section has reviewed the Saudi banking policies and infrastructure related to household banking. As policies guide the process of using a system, this review is essential to the building of a framework to evaluate the security of household customers in the KSA. The problem of proving the identity of female customers who have no national ID card is addressed by the customer presenting her family ID card, supported by the national ID card of a relative or a female friend; but as discussed in Section 6.3.2.1, the data show that this solution is prone to the threat of impersonation. However, since November 2016, there has been a legal requirement in Saudi Arabia for all females aged 15 years and over to be issued with national ID cards (Thakefni 2016). The application of this new law is expected to improve the security of female bank customers by countering the impersonation threat.

Despite the requirement under SAMA regulations for banks to educate their customers about bank services, set out above, the majority of the household customers participating in this study expressed ignorance of the regulations concerning bank credentials and most were not familiar with the procedures for using services such as online banking. Many household customers were also not aware of bank services that have been available for some time, such as mobile banking. More surprisingly, some bankers were not even aware of services such as contactless payments and urgent cash offered by the banks for which they worked. It is essential for banks to educate their own employees comprehensively about the services they provide if there is to be any possibility of keeping their customers fully informed.

The majority of household customers were found to make use of the SMS notification facility to inform them of every transaction and this proved to be a useful and reliable security measure in many cases. However, there is a need for improvement, in that there

is no procedure for informing the account holder if the saved mobile number is changed, as demonstrated by Case 12, where a son perpetrated an insider attack against his mother's account (see Appendix 13).

However, the review of the banking policies issued by SAMA reveals no evidence of policy related to telephone banking or mobile banking, nor any guidance on the use of these services. In addition, the review failed to find any procedure for bankers to follow in case of insider threats such as those discussed in Chapter 6, Section 6.3.1.3.

The third and final block of the framework is that of banking technologies and processes, which are discussed next.

7.4 Banking Technologies and Processes

The banking policies and infrastructure discussed above drive what bank technologies are available and how they operate. As mentioned in Section 2.3.3.2, Saudi banks offer a wide range of technologies: cheques, bank cards, telephone, mobile and online banking. This section discusses the security analysis of bank technologies, using threat modelling, which is a structured approach enabling the identification of security risks relating to a system. The discussion takes the form of a review of work published by banking experts. Specifically, the technologies discussed here are online banking, telephone banking and bank cards, i.e. the three technologies which household customers participating in this study reported using, as detailed in Chapter 4, Section 4.5. The two analytical tools used here are those introduced in Chapter 2, Section 2.2.1: STRIDE and DREAD, used respectively to identify objectives and vulnerabilities in bank technologies regarding specific security threats and to quantify the risk from these threats to banking technologies. It was considered important to use these tools in order to focus on the security of the bank system and that by integrating them with the

findings of the household context of use, the resultant framework would cover both security and cultural aspects of the system.

The following subsections use STRIDE and DREAD to analyse the security threats associated with the use of online banking, telephone banking and bank cards.

7.4.1 Spoofing

7.4.1.1 Online banking

According to Möckel and Abdallah (2010) and to Xin and Xiaofang (2014), there is a significant risk from spoofing threats to online banking, often using social engineering methods such as phishing to acquire personal or authentication details. Password security is threatened when password strength is insufficient or the default password is insecure and fraudsters often use complex malware such as spoofing or replay attacks to defeat banks' security systems. Analysis of the data presented in this thesis shows that insiders can carry out spoofing attacks against household online banking customers in two ways: firstly, the widespread practice of sharing credentials poses the threat of spoofing by the misuse of the shared credentials; secondly, an insider attacker can activate the account of a household member via the online banking service without permission, as no physical verification of identity is required to activate this service, as explained in Section 5.3.4.1.

Table 4: DREAD analysis for spoofing of online banking quantifies the risk posed by the threat of spoofing to online banking, this assessment being based on the understanding of the DREAD classification set out in Table 1: DREAD classification and explained in Section 2.2.1.2. It shows that spoofing poses a high risk to online banking. The damage potential is 3, because by spoofing the online credentials of a legitimate bank customer the attacker will obtain full trust authorization; reproducibility

is 3, because the attack can be reproduced at any time and does not require a timing window; exploitability is 3, because a novice programmer could make such an attack in a short time; affected users is 1, because spoofing the online credentials of a particular customer would only affect that customer; discoverability is 3, because there is a great deal of published information on the use of social engineering methods such as phishing to acquire personal or authentication details.

Table 4: DREAD analysis for spoofing of online banking

	Damage potential	Reproducibility	Exploitability	Affected users	Discoverability	Total
Spoofing of online banking	3	3	3	1	3	13

The spoofing threat to online banking can be mitigated in various ways. The first form of mitigation is the banks' policy, explained in Section 7.3.3, on keeping online credentials secure and confidential, and not sharing them. By sharing their credentials, household customers undermine this mitigation. The second form of mitigation is the introduction by the banks of a one-time authentication code or basic tokens and in order to strengthen the security of their online systems, several banks have now introduced offline card readers based on the MasterCard Chip Authentication Programme (CAP). Barclays UK, for example, claims to have been very successful in defending against fraud with PINsentry, their version of CAP (Barclays 2017), and numerous specialist suppliers including Reiner SCT in Germany and Cryptomathic in the UK now offer CAP-based authentication solutions to banks. In the KSA, banks protect online banking by sending a one-time authentication code to account holders by SMS (Section 4.5.2.2). The third form of mitigation is the use of SMS notifications. As the data in Section 4.5.2.2 show, this technique is widely used to inform the account holder instantly about new transactions, thus mitigating the threat of spoofing even if the account holder has shared online credentials. A fourth form of mitigation is to add a physical verification of

the identity of the account holder to the process of activating the online banking service for new customers. Finally, spoofing threats against the customer element can be mitigated by avoiding attack surfaces for social engineering, e.g. through the use of random password generators rather than simple passwords, and offering customers awareness programmes and training (Möckel and Abdallah 2010).

7.4.1.2 Telephone banking

Telebanking is a competitive and time-saving banking environment, but has been criticised as highly susceptible to identity theft (Sathye 1999). One of the main shortcomings hindering its robust operation in an open environment is its vulnerability to security threats. Its security generally relies on the use of telephone pins (TPINs) and passcodes, which customers are required to enter using either the telephone keypad or a voice recognition system, depending on the service design (Gunson, Marshall et al. 2011). However, these are the weakest credentials for providing security to any remote-access system. In cases of loss, theft, misuse or any other compromise to security, it is the user who is most likely to suffer. The security of typical knowledge-based applications is very easy to circumvent. TPINs, passcodes and the typical security questions posed by the banks to secure telephone banking are often shared and can be compromised by brute force attacks; answers are also predictable and a simple internet search can often yield the required information.

An additional weakness of telephone banking that compromises its security and makes it even more challenging is that neither party can be sure who is speaking at the other end. Just as with online banking, as discussed in Section 7.4.1.1, insiders can carry out spoofing attacks on telephone banking against household customers in two ways: through the misuse of shared credentials or by exploiting the lack of physical

verification of identity to activate this service without the account holder's knowledge or permission.

Where voice print technology is used to strengthen the security of telephone banking, one of the possible threats is a replay attack, which as Villalba and Lleida (2010) explain, is where an impostor impersonates the account holder using a recording of his voice. Among the possible ways of obtaining such a recording would be surreptitiously making a far-field recording of the victim using the microphone of a smartphone or laptop.

Table 5 uses the DREAD classification to quantify the risk that spoofing poses to telephone banking, showing that the risk is a high one.

Table 5: DREAD analysis for spoofing of telephone banking

	Damage potential	**Reproducibility**	**Exploitability**	**Affected users**	**Discoverability**	**Total**
Spoofing of telephone banking	3	3	3	1	3	13

As in the case of online banking, one mitigation of the spoofing of telephone banking is the bank policy against the sharing of credentials. Again, this would be undermined by household customers sharing credentials, although it should be noted that none of those participating in this research reported sharing their telephone banking credentials. Voice authentication -where a female voice is expected if the account holder is female, and a male voice for a male account holder- has the potential to improve security to some extent but the service would remain vulnerable to impersonation by an attacker of the same gender as the account holder. Another way of mitigating the risk of identity spoofing in telephone banking is to increasing the security level by requiring two-factor authentication. In a study of telephone banking security, Gunson, Marshall et al. (2011) compared single-factor and two-factor authentication. The single-factor approach

involves a what-you-know technique, usually requiring the user to recall two digits, selected at random from a six-digit secret number previously registered by the user and known only to him or her. The system or operator will ask the user to enter the x^{th} digit of the secret number and then to enter the y^{th} digit. The two-factor approach will similarly require the user to respond with two secret digits, but with the addition of a what-you-have component, involving the use of a hardware authentication token such as a portable key fob, a smartcard reader or an SMS sent to a mobile phone. Gunson, Marshall et al. (2011) conclude that single-factor authentication is easier to use and more convenient than two-factor authentication, but less secure. Thus, a gain in security is obtained at a cost to the usability of the service. This result corroborates the findings of earlier research on two-factor authentication for internet banking by Weir, Douglas et al. (2009), which found that usability and convenience were sacrificed when further layers of security were added to the system.

7.4.1.3 Bank cards

A bank card can be spoofed if the PIN is revealed to an unauthorised person (Braeuer, Gmeiner et al. 2015); according to Diebold (1999, cited by (Oruh 2014), this threat arises frequently when customers are careless with their cards and PINs, and may be exacerbated when ATM cards are issued without regard to the customer's literacy level. Adeoti (2011) cites a more recent source, a Report on Global ATM Frauds (2007), as identifying various types of ATM threats, including the use of a stolen card in an ATM by a fake presenter. Diebold (1999, cited by (Oruh 2014) states that the main ATM threat is fraud depending on PIN theft, which is mostly a result of congestion at ATM points; alternatively, it can be carried out using methods such as skimming, where the attacker captures card data from the magnetic stripe on the back of the card. Skimming can also be used to intercept card data from an EFTPOS system (Whitteker 2014).

The DREAD classification of the risk factors for the spoofing of bank cards is shown in Table 6, indicating that spoofing poses a high risk to bank card users.

Table 6: DREAD analysis for spoofing of bank cards

	Damage potential	Reproducibility	Exploitability	Affected users	Discoverability	Total
Spoofing of bank cards	3	3	3	1	3	13

As in the cases of online and telephone banking, the first form of mitigation is the policy of non-sharing of bank credentials, which is undermined by the practice of sharing that this study has identified among household customers. Again, the risk can be mitigated by the sending of SMS notifications to account holders' mobile phones. The data show this technique as being widely used to update the holder instantly about transactions on the account, thus mitigating the threat of spoofing, even if the account holder has shared the use of the card and its PIN. In the case of a stolen card, the threat of its fraudulent ATM or EFTPOS use is mitigated by the short time which often elapses before the cardholder discovers and reports the theft, followed by the bank deactivating the card. A final mitigation of this kind of threat is the fact that the attacker has only three attempts to discover the PIN for a stolen credit or ATM card (Schneier and Shostack 1999).

7.4.2 Tampering

7.4.2.1 Online banking

According to Möckel and Abdallah (2010) and Xin and Xiaofang (2014), online banking may face the threat of tampering, where an attacker gains direct access to the authentication database by employing an unsupported configuration or execution code, then viewing or tampering with the database content such as account names and passwords. A tampering attack may be perpetrated on online banking when a customer

activates an embedded malicious program which tampers with the user input (Xin and Xiaofang 2014). Another scenario is where an insider attacker activates the online banking service for the account of a household member without permission, made possible by the absence of physical verification of identity discussed with reference to spoofing, then tampers with the information related to the account. Alternatively, this threat can result from credential sharing, when an insider misuses the shared credentials by changing the password; in this case the account holder will be denied online access to the account until he or she has contacted the bank and reset the online credentials.

Table 7 sets out the DREAD classification of the risks of tampering with online banking, revealing an overall medium risk level.

Table 7: DREAD analysis for tampering with online banking

	Damage potential	Reproducibility	Exploitability	Affected users	Discoverability	Total
Tampering with online banking	3	2	1	3	2	11

As with the threats previously discussed, the banks' policy against credential sharing offers a mitigation of the risk of tampering with online banking, but this is undermined by the fact that sharing appears to be widespread. A second mitigation mechanism is to add the physical verification of identity to the process of activating the online banking service for new customers. Möckel and Abdallah (2010) recommend that in addition to physical security measures, the risk of tampering with the online banking authentication database can be mitigated by protecting the data storage from direct access through the use of a firewall, a private network connection between the web server and the database, and sophisticated rights management for viewing, accessing, altering and deleting data.

7.4.2.2 Telephone banking

Telephone banking can be exposed to the risk of tampering by insecure account holder practices, particularly where the account credentials are not kept secret and an attacker makes use of them, exploiting the weak security of telephone banking, which as noted in Section 7.4.1.2, is made even more challenging by the fact that neither party to the call can be sure of the identity of the other speaker. The attacker then can tamper with data, such as by changing the telephone banking password. A related risk, discussed in Section 7.4.5.2, is that of denial of service, as the account holder would not be able to access the telephone service without proving his/her identity to the bank and changing the password. Another scenario is where an insider attacker accesses the account of a household member by activating the telephone banking service without permission, since there is no physical verification of identity when the service is activated, as explained in Section 5.3.4.1. The attacker can then tamper with the information related to the account.

Table 8 presents the DREAD analysis of the risk of tampering with telephone banking, which is shown to be high.

Table 8: DREAD analysis for tampering with online banking

	Damage potential	**Reproducibility**	**Exploitability**	**Affected users**	**Discoverability**	**Total**
Tampering with telephone banking	3	3	3	1	3	13

Once again, the banks' non-sharing policy on account credentials should mitigate the threat of tampering with telephone banking, but this mitigation is undermined by the widespread practice of sharing. As with other risks to telephone banking security, voice authentication would offer some degree of mitigation, if only to the extent of eliminating the risk of impersonation by an attacker of the opposite gender to the account holder.

7.4.2.3 Bank cards

Bank cards are exposed to the threat of tampering in the form of changing the configuration files of ATM and/or EFTPOS platforms by injecting the platform by a malicious software such as Trojan horses (Braeuer, Gmeiner et al. 2015). In addition, bank cards can be exposed to the threat of tampering as a result of the widespread practice of sharing cards and their credentials, allowing an insider to tamper with account information such as a PIN or registered mobile number by using an ATM.

The risk of tampering with bank cards is calculated to be of medium severity, as shown by the DREAD analysis in Table 9 and supported by the findings of Breauer, Gmeiner et al. (2015).

Table 9: DREAD analysis for tampering with bank cards

	Damage potential	**Reproducibility**	**Exploitability**	**Affected users**	**Discoverability**	**Total**
Tampering with bank cards	3	2	3	1	2	11

Apart from the policy excluding the sharing of credentials, widely undermined by the actual practice of sharing, the risk of tampering with cards can be mitigated by the use of SMS notifications. The data gathered for this study show this technique to be widely used to update the account holder instantly about any transactions, so that even if he or she has shared a card PIN, the risk of successful tampering is mitigated.

7.4.3 Repudiation

7.4.3.1 Online banking

The threat to online banking of repudiation, whereby users are able to falsely deny carrying out transactions, may arise in case of conflicts with customers due to problems with the documentation and log file system of the transaction database, such as where there is no log record or where it is not perfect (Möckel and Abdallah 2010, Xin and

Xiaofang 2014). This threat can also arise from insecure account holder practices, particularly where the online banking credentials are not kept secret and another person who knows the credentials makes use of them to perform what will then appear to be a genuine transaction, according to the log record of the online activities of the account. Another scenario leading to repudiation of online banking transactions is where an insider attacker activates the online banking service for the account of a household member without his or her permission or knowledge, given the lack of a requirement of physical verification of identity, as explained in Section 5.3.4.1. Any transactions later performed by the attacker using this account will then appear to be genuine, but may be repudiated in good faith by the account holder.

Table 10 categorises the risk of repudiation for online banking using DREAD and shows that it appears to pose a medium level of risk.

Table 10: DREAD analysis for repudiation of online banking

	Damage potential	Reproducibility	Exploitability	Affected users	Discoverability	Total
Repudiation of online banking	3	1	1	1	2	8

Möckel and Abdallah (2010) state that to mitigate repudiation threats against databases and other elements of the online banking system, banks should establish comprehensive logging facilities, providing adequate levels of evidence in case of fraud or conflict. Another mitigating measure would be to require the physical verification of identity when the online banking service is initially activated by a customer. The SAMA warnings against credential sharing cited in Section 7.3.3 again represent a potential mitigation, largely nullified by the insecure sharing practices reported in this thesis.

7.4.3.2 Telephone banking

As noted above with regard to spoofing and to tampering, telephone banking faces the risk of repudiation as a result of insecure account holder practices, particularly where credentials are not kept secret. In the absence of any other means of identifying a caller, an attacker can conduct a transaction which appears to be genuine and can be proved to have happened by the recording of the call. Again, an insider attacker may activate the telephone banking service for the account of a household member without permission, in the absence of physical verification, then use the account to perform what appear to be genuine transactions.

The DREAD analysis of the risk of repudiation associated with telephone banking is shown in Table 11, revealing it to be at a medium level.

Table 11: DREAD analysis for repudiation of telephone banking

	Damage potential	Reproducibility	Exploitability	Affected users	Discoverability	Total
Repudiation of telephone banking	3	1	1	1	2	8

The repudiation threat to telephone banking is, in common with the threats of spoofing and tampering, potentially mitigated by keeping credentials secret and by the use of voice authentication, but these mitigations are subject to the limitations already noted in Sections 7.4.1.2 and 7.4.2.2.

7.4.3.3 Bank cards

Although the vast majority of chip-card payments are processed without a hitch, there are occasions when a cardholder later repudiates a payment. The cardholder may be adamant that he or she was not present to authorise the transaction, while the issuing bank considers the transaction data and certificate to provide evidence to the contrary, because they show that a chip-and-PIN mechanism was used to authenticate the

cardholder's identity. The card issuer trusts its chip-card environment and considers the transaction authentic, whereas the cardholder believes it to be fraudulent; these are the ingredients of a dispute (Boyd 2009). In June 2009, a UK court ruled in favour of a high street bank in a dispute with a customer over phantom withdrawals, although the only available evidence lay in the bank's log files, as the payment card and the authorisation request cryptogram that were once held by the bank had been destroyed (Finextra 2009).

Boyd (2009) notes that an account can be subject to a repudiation threat when a new card and PIN are sent through the post and both are intercepted, exploited and then forwarded to the intended recipient. Particularly where there is no obvious evidence of attack, the presence of the on-card receipt or footprint could cause a wrong conclusion to be drawn. As with all other threats analysed in this chapter, the threat of repudiation can arise from insecure cardholder practices such as failure to keep the PIN secret; if another person who knows the PIN makes use of the card and returns it before its absence is noticed, then the transaction appears to be genuine, with a matching on-card receipt (Boyd 2009).

The final scenario where a card transaction risks being repudiated was mentioned by some participants in this study (such as P30 in Section 7.5.1.1) and is also reported in a study by Abdulmuhmin (1998), some of whose participants recounted negative experiences with EFTPOS terminals failing to connect properly to the server, resulting in double payment. In this case, the two payments will appear in the bank's log file, one of them having been made intentionally by the customer, while the other was made because of the poor connection to the server.

The DREAD analysis for the repudiation of bank card transactions shown in Table 12 indicates that there is a medium risk associated with this.

Table 12: DREAD analysis for repudiation of bank cards

	Damage potential	Reproducibility	Exploitability	Affected users	Discoverability	Total
Repudiation of bank cards	3	1	1	1	2	8

Once again, the mitigation of the repudiation risk to bank card transactions inherent in the SAMA non-sharing rules was found to be undermined by the widespread sharing of card credentials. Another mitigation mechanism is the use of instant SMS notifications, which the data show to be widely used to inform account holders of transactions. This represents a more successful mitigation of the threat, since it works even if the account holder has shared the card PIN. Finally, to mitigate the risk of double payment, the customer must contact the bank, complete a refund form and provide the payment receipt.

7.4.4 Information disclosure

7.4.4.1 Online banking

Information disclosure is particularly harmful for data flows transferring valued assets such as the amount of credit in an account or a customer's banking activity. Where the information disclosed is in the form of bank credentials, attackers may be able to intercept the transferred information, gain access to the credentials element and use it fraudulently (Möckel and Abdallah 2010, Xin and Xiaofang 2014) for the purposes of spoofing or the disclosure of further information. An example of information disclosure applicable to online banking is when attackers use malware to steal credentials and other sensitive information via the keyboard record or when a user is phished by means of a fake site to obtain user input (Xin and Xiaofang 2014). Another scenario for this threat is where an insider attacker fraudulently activates the online banking service for the account of a household member, as discussed in Sections 7.4.1.1, 7.4.2.1 and 7.4.3.1, enabling the attacker to access all of the information related to the account. The

threat of information disclosure can also result directly from shared credentials being used to access account information online.

Table 13 uses DREAD to quantify the risk to online banking of information disclosure, showing it to be at a high level.

Table 13: DREAD analysis for disclosure of online banking information

	Damage potential	Reproducibility	Exploitability	Affected users	Discoverability	Total
Disclosure of online banking information	2	3	3	1	3	12

Möckel and Abdallah (2010) state that the disclosure of information transferred via data flows can be mitigated by employing standard protocols such as SSL/TLS and extended validation SSL certificates provided by specific certification authorities for correct identification of the bank's website. For example, most banks in Europe use HTTPS measures either for their entire web platform (e.g. Sparkasse and Santander), or partially for online banking facilities (e.g. Barclays and Lloyds). As with the other categories of threat discussed earlier in this chapter, the risk of disclosure would be mitigated by adherence to the policy of forbidding credential sharing, but this is undermined by the practice of sharing that this study has found to be widespread in the KSA. Another mitigation would again be to require the physical verification of the account holder's identity for the initial activation of online banking.

7.4.4.2 Telephone banking

The compromise to the security of telephone banking noted several times above, that neither party to a call can identify the other with certainty, can be exploited by attackers who take a social engineering approach by calling bank customers and deceiving them into disclosing sensitive information regarding their accounts and activities. Another weakness applicable to this threat and to all of those discussed above, affecting both

telephone and online banking, is the lack of a requirement for physical verification of identity to activate the service and so gain access to all account information. Finally, the sharing of credentials poses a strong threat of information disclosure where such credentials are misused to access account information.

The DREAD analysis for information disclosure in telephone banking shows that there is a high risk of this (Table 14).

Table 14: DREAD analysis for disclosure of telephone banking information

	Damage potential	Reproducibility	Exploitability	Affected users	Discoverability	Total
Disclosure of telephone banking information	2	3	3	1	3	12

The comments repeatedly made above regarding mitigation via identity verification for activation apply here, as do those on the way that the mitigation inherent in the SAMA non-sharing rules is undermined by actual practices that ignore this requirement. Information disclosure threats against the customer element can be mitigated by avoiding attack surfaces for social engineering, e.g. through the use of random password generators rather than simple passwords, and offering customers awareness programmes and training (Möckel and Abdallah 2010). As with the other threats to telephone banking, some level of increased level of security would be provided by voice authentication, at least where the would-be impersonator was not of the same gender as the intended victim.

7.4.4.3 Bank cards

The threat of disclosure arises when unprotected card data such as card numbers are obtained by an attacker (Braeuer, Gmeiner et al. 2015). The card information can be disclosed by using skimmers on ATMs where this would allow an attacker to capture and record cards' information (Adeoti 2011).

If the disclosed information is the associated PIN, the possible consequences include both spoofing and further information disclosure. As with many other threats, cardholder practices are significant, particularly if the PIN is not kept secret and another person who knows the PIN makes use of the card to obtain information related to the account and returns the card before the cardholder notices its absence.

The DREAD analysis for the disclosure of bank card information is shown in Table 15, which quantifies this as a high-level risk. This is contradict with the findings of Braeuer, Gmeiner et al. (2015) where they stated the risk level would be medium.

Table 15: DREAD analysis for disclosure of bank card information

	Damage potential	Reproducibility	Exploitability	Affected users	Discoverability	Total
Disclosure of bank card information	2	3	3	1	3	12

The mitigation of the threat of information disclosure represented by the bank policy on the confidentiality of credentials is again undermined by the widespread practice of sharing credentials, whereas the use of SMS notifications will mitigate the information disclosure threat in the case of bank cards, as with other threats discussed above, even where the cardholder has shared the PIN.

7.4.5 Denial of service

7.4.5.1 Online banking

Denial of service can affect online banking when a channel is overloaded, causing log processing to hang or crash (Xin and Xiaofang 2014). This threat may make the website element unstable and ultimately unavailable to users, damaging the reputation of the bank and overall trust in its security (Möckel and Abdallah 2010, Xin and Xiaofang 2014). Another scenario for this threat, in common with those outlined above in respect of telephone and online banking, is where an insider attacker activates the service

without the permission of the household member whose account it is. In this case, the genuine account holder will be denied access to the service until she has contacted the bank and arranged for the online credentials to be reset. Similarly, this threat can arise as a result of sharing credentials, which can be used by the insider to change the password and so deny access to the account holder until the credentials are reset.

Table 16 shows that the DREAD analysis for denial of service in online banking rates this as a high risk.

Table 16: DREAD analysis for denial of service in online banking

	Damage potential	Reproducibility	Exploitability	Affected users	Discoverability	Total
Denial of service in online banking	3	2	1	3	3	12

Möckel and Abdallah (2010) state that denial of service threats can be mitigated through performance testing for accordant system capacity, input limitation and validation, consistent coding, backup facilities and the existence of an emergency plan and a business continuity plan. The remarks repeated above on the undermining of the mitigating effect of credential confidentiality rules and policies by household users' sharing practices apply to the denial of service in online banking, as do those concerning the value of requiring the physical verification of identity for the initial activation of the service.

7.4.5.2 Telephone banking

A denial of service attack on telephone banking might take the form of flooding the bank's system with telephone traffic to prevent legitimate network traffic from flowing. This would disrupt connections between customers and the telephone banking centre, thus preventing access to the service. As with online banking, if an insider attacker activates telephone banking for the account of a household member without permission,

the account holder will be denied access to the service until the online credentials have been reset. Similarly, shared credentials may be misused to change the telephone banking password, again denying access for the account holder until he has arranged for the resetting of the credentials.

The DREAD analysis of the risk of denial of service in telephone banking (Table 17) indicates that the overall risk level is high.

Table 17: DREAD analysis for denial of service in telephone banking

	Damage potential	Reproducibility	Exploitability	Affected users	Discoverability	Total
Denial of service in telephone banking	3	2	1	3	3	12

As noted repeatedly above in respect of other threats, the widespread sharing of credentials undermines the mitigation of the threat of denial of service in telephone banking represented by the official confidentiality policy. Again, physical verification of identity would mitigate the risk of the misuse of service activation. Finally, as for all threats to telephone banking, voice authentication would mitigate the impersonation risk to some extent.

7.4.5.3 Bank cards

The denial of service threat to bank cards can take the form of making ATMs and/or EFTPOS platforms unavailable to all customers by dominating some of their resources (Braeuer, Gmeiner et al. 2015). At the individual level, if the cardholder divulges the PIN to another person, who then makes use of the card and changes the PIN at an ATM, the genuine account holder will then need to contact the bank to reset the PIN before regaining access to ATM or EFTPOS services.

Table 18 shows the DREAD analysis of the risk of denial of service for bank cards, indicating that there is only a low risk of this, consistent with the findings of Braeuer, Gmeiner et al. (2015).

Table 18: DREAD analysis for denial of service for bank cards

	Damage potential	Reproducibility	Exploitability	Affected users	Discoverability	Total
Denial of service for bank cards	1	1	2	1	2	7

Once more, the non-sharing policy on credentials represents a potential mitigation of this threat, which is undermined by the insecure practices that this study has found to be widespread. Another mitigation is the use of SMS notifications, which as noted in Sections 7.4.1.3, 7.4.2.3 and 7.4.3.3, will provide additional security to card users even if they have shared credentials.

7.4.6 Elevation of privilege

7.4.6.1 Online banking

According to Möckel and Abdallah (2010) and Xin and Xiaofang (2014), elevation of privilege threats may affect the administrator account, for example, if an unauthorised user manages to exercise certain privileges such as taking control over accounts or accessing confidential data. Possible consequences of such an elevation of privilege scenario are the related threats of spoofing and information disclosure. Another scenario which applies here as with other threats discussed above is where an insider attacker activates the online banking service for an account without permission, giving the attacker the privileges of accessing and using the account online. Once more, the widespread practice of sharing credentials elevates this threat.

Table 19 depicts the DREAD categorisation of the risk of elevation of privilege for online banking, which reveals that this is a high risk.

Table 19: DREAD analysis for elevation of privilege for online banking

	Damage potential	Reproducibility	Exploitability	Affected users	Discoverability	Total
Elevation of privilege for online banking	3	3	3	3	3	15

Möckel and Abdallah (2010) state that protection against elevation of privilege threats can be achieved through sophisticated two-factor authentication systems. In common with all of the other threats considered in this chapter, elevation of privilege threats would be mitigated by the policy against the sharing of credentials, but this is undermined by the practice of sharing identified in this study. As to the unauthorised activation of the online banking service, this threat would again be mitigated by the addition of a physical verification of identity requirement.

7.4.6.2 Telephone banking

Since elevation of privilege is typically quite a technical form of attack, it is not applicable directly to telephone banking, but can occur as a consequence of a spoofing attack. For example, an attacker using the credentials of a legitimate customer, obtained for example by credential sharing, might exploit the weakness of telephone banking whereby neither party to a call can be sure of the other's identity to gain the privileges associated with using the account. Alternatively, in the absence of physical verification of identity, an insider attacker might activate the telephone banking service for the account of a household member without permission, thus obtaining the privileges of accessing and using the account.

The risk of elevation of privilege for telephone banking, according to the DREAD analysis shown in Table 20, is at a high level.

Table 20: DREAD analysis for elevation of privilege for telephone banking

	Damage potential	Reproducibility	Exploitability	Affected users	Discoverability	Total

Elevation of privilege for telephone banking	3	3	3	1	3	13

The remarks repeated several times above regarding threat mitigation by the policy of not sharing credentials, as well as those on its undermining by widespread practice, apply equally to elevation of privilege in the context of telephone banking. The same is true for the value of requiring physical verification of identity in order to activate the telephone banking service and for the partial mitigation offered by voice authentication.

7.4.6.3 Bank cards

A elevation of privilege attack can affect bank cards by modifying the configuration files of an ATM and/or EFTPOS platform and making changes to the user access control module to gain more privileges (Braeuer, Gmeiner et al. 2015); in this case, elevation of privilege and tampering are synonyms in the context of bank cards. A related issue is insecure cardholder practices, in particular the failure to keep one's PIN secret, since another person who knows the PIN could gain privileges and make use of the card.

The DREAD analysis for elevation of privilege for bank cards in Table 21 shows that there is a high risk, which is contradict the findings of Braeuer, Gmeiner et al. (2015) where they stated that the risk level is medium.

Table 21: DREAD analysis for elevation of privilege for bank cards

	Damage potential	**Reproducibility**	**Exploitability**	**Affected users**	**Discoverability**	**Total**
Elevation of privilege for bank cards	3	3	3	1	2	13

As has been stated for all other threats, the threat of elevation of privilege is potentially mitigated by the banks' policy against credential sharing, a mitigation which is undermined by the actual practice of sharing identified in this study.

7.4.7 Section summary

Table 22: Summary of DREAD analyses

	Risk of spoofing	**Risk of tampering**	**Risk of repudiation**	**Risk of information disclosure**	**Risk of denial of service**	**Risk of elevation of privilege**
Online banking	**13 high**	11 medium	8 medium	**12 high**	**12 high**	**15 high**
Telephone banking	**13 high**	**13 high**	8 medium	**12 high**	**12 high**	**13 high**
Bank cards	**13 high**	11 medium	8 medium	**12 high**	7 *low*	**13 high**

Table 22 summarises the 18 specific DREAD analyses detailed above. It is worth mentioning here that the sharing of credentials practised by most participating household customers enables all of the STRIDE threats. In addition, this sharing practice makes some threats easier for the attacker to enact and raises the DREAD level.

Sections 7.2, 7.3 and 7.4 have detailed in turn the three essential elements of the security evaluation framework, i.e. household context of use, banking policies and infrastructure, and banking technologies and processes. The following sections discuss the application of the framework to two cases: the evaluation of using of fingerprints as a new security mechanism applied to an existing technology, i.e. the authentication of banks cards, and the evaluation of the security of a new banking technology, i.e. mobile banking.

7.5 Using the Framework to Evaluate the Security of Banking Practices of Household Customers in the KSA

As mentioned before, the security evaluation framework consists of three elements detailed in Sections 7.2, 7.3 and 7.4, i.e. household context of use, banking policies and infrastructure, and banking technologies and processes. This framework can be used by bank system developers and security analysts (as shown in Figure 21) to evaluate proposed countermeasures and to select one that is both culturally sensitive and secure.

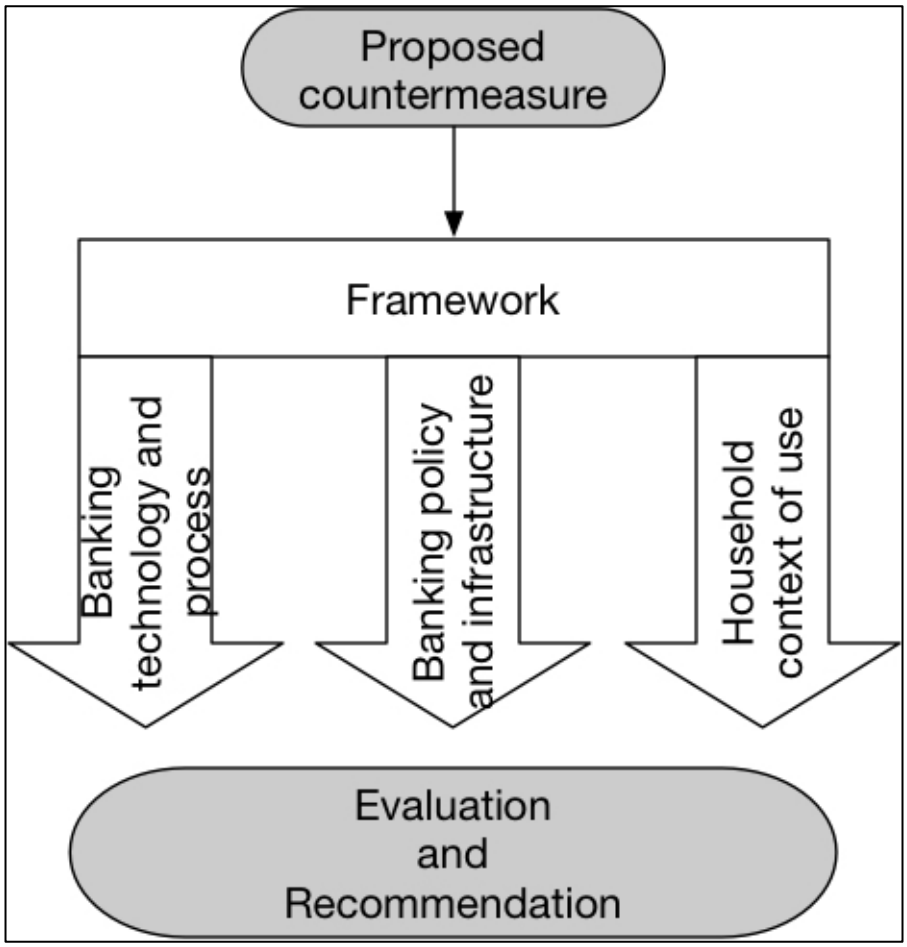


Figure 21: Applying the framework to a countermeasure.

The following sections discuss the application of the framework to two cases: the evaluation of the use of fingerprints as a new security mechanism applied to an existing technology, i.e. the authentication of banks cards, and the evaluation of the security of a new banking technology, i.e. mobile banking.

7.5.1 Using biometrics in authentication

This section is concerned with applying the framework developed above to evaluate the security of the use of fingerprints in the authentication of banks cards, which represents the use of the framework to evaluate a new security mechanism applied to an existing technology. Fingerprint authentication is a kind of biometric authentication that refers to the use of physiological and behavioural biometrics to authenticate users (Renaud

2004). Biometric authentication relies on matching patterns of user characteristics or practices that are distinctive and distinguishable (Kent and Millett 2003); thus it assumes that there are no similarities of these characteristics or practices among different users. By applying the conceptual framework proposed in 7.1 and depicted in Figure 18, this case will now be presented using the three building blocks of the conceptual framework: household context of use, banking policies and infrastructure, and banking technologies and processes.

7.5.1.1 Household context of use

By exploring the household context of use of bank cards and consulting the three models of customer, banking and gender perspectives, it is possible to identify a number of factors strongly motivating the sharing of bank cards and PINs among household members, leading to the practice of sharing credentials being adopted by the majority of household customers, which in turn threatens the security of both customers and bank systems. For example, the case study below shows how participant P30 regarded the sharing of his bank card and its PIN.

As part of the third round of data collection from bank customers, P30 reported in his diary that his wife used the ATM card to one of his accounts to buy groceries for the household, which consisted of P30, his wife, two sons and one daughter. As explained in 4.5.2.7 and the gendered practice **Control** `(men are guardians of women)` in 6.3.1.1, in response to religious obligations and cultural expectations, P30 as the head of the household was considered responsible for the family finances. In order to control family expenditure while maintaining his financial independence, he held two bank accounts, one of which he kept private, related to the `secret bank account` gendered practice mentioned in Section 6.3.4.2. The second account was used specifically for family expenditure; P30 would transfer money monthly to this account and share its

information, ATM card and PIN with other family members. As noted in Section 7.2, the practice adopted by P30 of sharing his account credentials is widespread among household customers in the KSA. P30 partially shared his account credentials (card and PIN without online credentials) and account control (knowledge of the account, withdrawal of cash). His motivations and justifications for doing so included the need to manage the family finances, trusting his wife and being able to rely on receiving SMS notifications to monitor the use of the account. Meanwhile, P30 used his private account differently; his family knew about the existence of the account but they had no other information related to it, so P30 only partially shared one form of account control, i.e. `knowledge of the account`. The family had operated the account in this way for the past four years. His wife would buy groceries for the household twice a week using the shared ATM card that had been issued to P30. As a female, P30's wife was prohibited from driving in Saudi Arabia and relied on a chauffeur to drive her to a grocery store. The Western alternative of online shopping for groceries remains unavailable in the KSA and in any case, ATM cards cannot be used for online shopping (Section 2.3.3.2). Local grocery stores are unlikely to have EFTPOS terminals, leaving customers no option but to withdraw cash from an ATM. Larger supermarkets would offer the option of EFTPOS, but P30 expressed his concern about two attendant risks, consistent with other participants in this study and the findings of (Abdulmuhmin 1998), which had led him to advise his wife to use cash in preference to EFTPOS as much as possible. The first risk was of the loss of control over expenditure when using EFTPOS; P30 explained that his wife would withdraw a certain amount of cash from an ATM to use for expenditure and not exceed this amount of money, whereas when using EFTPOS there was a strong chance that she would use all of the available credit in the account. The second concern about using EFTPOS was the safety and reliability of the system;

P30 recounted negative experiences of a terminal failing to connect to the server, causing a double payment to occur.

As mentioned before in the model of the banking perspective, the sharing practice adapted by P30 is widespread by household customers and `bankers are aware of credential sharing` and according to participating bankers, the need to keep credentials secure was "*general knowledge*" and they were sure that their customers already knew this; therefore there was no need to worry them by discussing the risks. Some bankers declared that they would not report these incidents of sharing to managers or any bank committees, because, as one put it, "*everyone knows this is common practice among customers and it happens regularly*". When maintaining the confidentiality of credentials was raised, all of the participating bankers assigned full responsibility for this to the customer, thus `shifting responsibility`.

Given the current design of banking systems, the only way in which customers can delegate authority over their banking activities is by sharing credentials. A possible solutions would be to include biometric fingerprints with the card and PIN or to use fingerprints instead of the card PIN. The adoption of unshareable authentication mechanisms such as fingerprints would help to stop the sharing practice; in the present case, P30 would not be able to share his card with his wife, as he could not share his fingerprints. Consequently, such a new security mechanism would increase the security of using bank cards and provide more protection to both customers and bank system. However, the household context of use clearly indicates that this solution would not be likely to work as intended, as it strongly conflicts with a number of existing cultural norms; for instance, it would make the situation of female customers even worse for accessing cash: because of their movement limitations, they frequently rely on getting others to access cash on their behalf, and would be prevented from doing so with a

biometric form of authentication. In the case of P30 he needs to transfer money for groceries to the account of his wife but this would mix the groceries' money with the wife's money that might cause problems. Instead P30 can make a joint account with his wife used for family expenditure where in this case the fingerprint for both P30 and his wife would be used for the authentication process for the card of the joint account. The final point in the household context of using fingerprints in the authentication process of bank cards is the cultural aspects around using the same fingerprint scanner in ATM/EFTPOS by both men and women. As such scanners are already used in the KSA by both men and women for other purposes such as issuing national ID cards and issuing of mobile SIM cards, it is anticipated that applying this new security mechanism would not create a cultural problem.

7.5.1.2 Banking policies and infrastructure

As stated above, P30 shared the card and the PIN of one of his accounts with his wife. Clearly such a practice is against official regulations of protecting banking credentials (SAMA 2010, SAMA 2013), which state clearly, for instance, that "banks are responsible for providing secure and safe systems and services for their customers unless the customer fails to safeguard their account user number or password and divulges it to a third party" (SAMA 2010)p. 14). This implies that banks are free to disclaim any responsibility for cases of fraudulent access to the accounts of people who have shared their credentials, even if the fraud did not happen because of this practice. Based on this, P30 is at risk of not being protected by the bank. As explained in Chapter 6, the cultural, social and religious norms regarding gender roles put greater pressure on women than on men to share their credentials, which combined with the banks' policies regarding sharing, results in women being more exposed and less protected by the banks. Although P30's practice of sharing credentials clearly contravenes bank policy

(Section 7.3.3), he claimed, in common with the majority of participants in this study, not to be aware of this policy, which suggests that banks may be failing to meet their responsibility to educate customers about bank cards and their importance (Section 7.3.2).

In the case of using fingerprints in the authentication process of bank cards, such a mechanism would stop the sharing practice completely and sharing credentials would not be an available option to household customers which is compatible with the SAMA policed mentioned above. For female household bank customers, using fingerprints would stop the pressure to share their credentials and make them more protected and less exposed to security threats such as insider thereat. However, as mentioned before the using of fingerprints would make the situation of female customers even worse for accessing cash because of their movement limitations.

As explained when discussing the infrastructure of Saudi banks, branches are segregated by gender, so that in most locations there will be a men's branch and a separate women's branch. Thus, if P30 used a joint account with his wife to solve the problem of controlling family expenditure, then he would scan his fingerprint in the men's branch and his wife would do the same in the women's branch. However, it is anticipated that applying this new security mechanism would not create a culture/gender problem regarding the use of the same fingerprint scanners at ATMs and EFTPOS terminals by both men and women, as this already happens in the KSA for other purposes, such as issuing national ID cards and mobile SIM cards.

7.5.1.3 Banking technologies and processes

Given the current design of banking systems, the only way in which customers can delegate authority over their banking activities is by sharing credentials. Consequently,

the auditability and non-repudiation of banking activities are seriously compromised, because it is no longer possible to assert that properly authenticated credentials uniquely identify a single individual. In addition, P30 is exposed to the bank card's risks discussed in Section 7.4. Moreover, when P30 shared his credentials with his wife he exposed himself to all of the STRIDE threats, spoofing: the wife is not the account holder but by sharing the card and its PIN with her, she is masquerades as a legitimate user, tampering: the wife can use the shared credentials to change the PIN using the ATM, repudiation: P30 can repudiate a transaction as a result of lack of auditability and using credentials by someone else, information disclosure: the wife can use the shared credentials and ATM to disclose more information such as the credit in the account, denial of service: the wife can use the shared credentials to change the PIN using the ATM and then P30 would not be able to use the card, elevation of privilege: the shared credentials elevate the privilege for the wife by giving her the right to access and use the account.

The use of fingerprints in the authentication process of bank cards would help to stop the sharing practice; consequently, such a new security mechanism would protect the auditability and non-repudiation of the bank system. In addition, this mechanism would strengthen the security of P30 and all household customers in respect of all STRIDE threats against their bank cards, thus reducing the risk level for each threat.

However, researchers who have examined this suggested solution (Jain and Nandakumar 2012, Oruh 2014) warn of two types of authentication error to which biometric systems are prone: false nonmatch and false match. False nonmatch occurs when two samples from the same individual have such low similarity that the system cannot correctly match them, while false match occurs when samples from two different individuals have such high similarity that the system incorrectly declares them to be a

match. The former results in a denial of service to a legitimate user, while the latter can allow intrusion into the system by an unauthorised user. Denial of service to a legitimate bank customer in this case means that the customer would not be able use ATM/EFTPOS unless fixing the problem by visiting the bank branch which is not a problem for men but cause a new burden for women because of movement limitation.

7.5.1.4 Evaluation and recommendations

Given the current design of banking systems, the only way in which customers can delegate authority over their banking activities is by sharing credentials. Possible mitigations to prevent the sharing of credentials would be to include biometric fingerprints with the card and PIN or to use fingerprints instead of the card PIN. The adoption of unshareable authentication mechanisms such as fingerprints would help to stop the sharing practice and such a new security mechanism would thus make the use of bank cards more secure and provide more protection to both customers and the bank system. However, the household context of use clearly indicates that this solution would not be likely to work as intended, as it strongly conflicts with a number of existing cultural norms; for instance, it would make the situation of female customers wishing to access cash even worse: because of their movement limitations, they frequently rely on others to access cash on their behalf, but the imposition of a biometric form of authentication would prevent them from doing this. The use of fingerprints to stop the practice of sharing credentials however is compatible with the SAMA policy mentioned previously. In addition, such a new security mechanism would protect the auditability and non-repudiation of the bank system, as well as strengthening the security of household customers in respect of all STRIDE threats against their bank cards, thus reducing the risk level for each threat.

7.5.2 Using mobile banking

Banks offer different technologies to customers and encourage them to use these technologies to save money, time and effort for themselves and for the banks. One such technology is mobile banking, which may be distinguished from online banking by the use of a smartphone application, rather than a personal computer and web browser (Brown, Cajee et al. 2003). As mentioned before, Saudi banks offer mobile banking technology to household customers, however, none of the household customers who participated in this study is using this technology. By applying the conceptual framework proposed in 7.1 and depicted in Figure 18, the case of using mobile banking will be presented using the three building blocks of the conceptual framework: household context of use, banking policies and infrastructure, and banking technologies and processes as following:

7.5.2.1 Household context of use

Mobile banking services allow customers to use a mobile device for transactions such as balance enquiries, ordering cheque books and completing funds transfers. A study by Sohail and Al-Jabri (2014) shows that mobile banking users in the KSA tend to be young, educated males, not necessarily with high incomes; the authors argue that banks should target these groups of customers. Bank customers need to use the same account credentials as for online banking to access the mobile banking services (Al-Jabri and S. 2012). As stated in Section 4.5, online banking was not widely used by participants in the present research; this may be one of the factors explaining the fact that none of the 47 participating household customers reported using mobile banking. The limited use of mobile banking cannot be related to the general level of smartphone use, since in 2016 there were 22.2 million smartphone users among Saudi Arabia's population of around 30 million (Statista 2016). Al-Husein and Sadi (2015) found that the quality of internet

connections, the degree of awareness among customers, trust in mobile banking and resistance to change were among factors having a significant impact on customers' attitudes towards adopting mobile banking in the KSA.

Comparing to other banking technologies, the advantages of mobile banking are its convenience, offering access to banking services no matter what the location or time, and its efficiency (Jarvenpaa, Lang et al. 2003, Laukkanen 2007, Tiwari, Buse et al. 2007, Kanniainen 2010) which means that this technology would offer greater freedom to customers to manage their bank accounts. Mobile banking is potentially more available than online banking since it does not require a computer, and as mentioned above smartphones are used extensively in the KSA where around 75% of the population is already have smartphones. By using the model of gender perspective on the using of mobile banking it found that this technology would also affected by the gender role. For female household customers, the using of mobile banking would facilitate banking activities that currently done in person by visiting bank branch or using ATM and making burden with the movement limitations for Saudi females. For male household customers, the using of this technology might make it even easier to maintain secret bank accounts, since they can be managed directly from a personal device such as smartphone where the using of online banking needs to be performed on a computer that can be a shared device. In addition, if the computer is shared in the household that would increase the chance for monitoring banking activities by family members when using online banking while monitoring banking activities would not be easy when using personal smartphone for mobile banking.

Mobile banking offering the same services as online and telephone banking; moreover, it would facilitate the use of an urgent cash service, which in turn would allow customers, especially females, to withdraw cash without sharing their cards and PIN. As

mentioned in Section 5.3.3, three Saudi banks introduced in 2014 an urgent cash service which allows customers to withdraw up to 1000 SAR from an ATM without a card, using their bank's app on a smartphone and validating the transaction by means of a passcode, an activation code sent by SMS and their national ID number (AlRiyadh newspaper December 2014). The model of banking perspective notably revealed that most bankers participating in this research, even some employed by the three banks in question, had no information about this service. This lack of awareness among bankers would significantly weaken their ability to educate new customers about the service; the banks must first develop a serious training programme for bankers, then advertise the service prominently. KPMG report for 2011 mentioned by Alkhaldi (2016) revealed that 38% of bank customers in the Middle East were unaware that their banks offered mobile banking. Banks in Saudi Arabia should raise customers' awareness of the usefulness of using mobile banking through advertising and banks should highlight the full functionality of their systems to response efficiently to the different banking needs of users.

7.5.2.2 Banking policies and infrastructure

As mentioned before SAMA was established in 1952 for supervising Saudi banks and managing and operating all bank technologies. SAMA has issued various laws to manage different internet banking technologies such as the "Electronic Transactions Law" issued in 2007, with the aim of providing a legal framework, and controlling and regulating internet banking. Meanwhile, to employ the SAMA strategies in this regard, SAMA has launched a special department which is responsible for the development and improvement of the internet banking technologies amongst Saudi banks. The department is named Banking Technology Department (BTD), under the guidance of the Directorate of Banking Control (DBC) (BIS 2012). Furthermore, SAMA requires

Saudi banks to hold an SAMA license to provide internet banking technologies and banks that own a valid SAMA license are required to obtain a prior statement from SAMA allowing the addition of any new internet banking technology or to modify an existing one (Basel Committee 2003, Alkhaldi 2016). In addition, the review of the banking policies issued by SAMA reveals different policies regarding the using of banking technologies in general presented and discussed in Section 7.3 but no evidence of policy related specifically to mobile banking services or of guidance on their use.

7.5.2.3 Banking technologies and processes

The security analysis of mobile banking would be similar to that of online banking; in particular, STRIDE threats arising from the sharing of credentials practised by most of the participating household customers would be likely to apply in the same way to mobile banking. Social engineering methods such as phishing to acquire personal or authentication details would also be likely to occur. Similarly, an insider attacker who fraudulently activated the online banking service for the account of a household member, as discussed repeatedly in Section 7.4, could then use the same online credentials for mobile banking. A simple mitigation of this threat would be to offer awareness programmes and training to educate customers about these threats and the consequences of the sharing practice; by doing so, the banks would be following SAMA policy regarding customer education mentioned in Section 7.3.2.

By exploring more the security of the technology of mobile banking it found that the overall statistics for 2015 provided by Kaspersky Security Bulletin (Garnaeva, van der Wiel et al. 2015) revealed that two families of mobile banking Trojans – Faketoken and Marcher – were included in the Top 10 banking Trojans most commonly used in 2015. The processes of the Trojan-Banker.AndroidOS.Faketoken family work with computer Trojans. To distribute this malware, attackers use social engineering techniques. When a

bank customer visiting his/her online banking account, the Trojan modifies the page, asking the customer to download an Android application which is supposedly required to securely confirm the transaction. In fact the link leads to the Faketoken application. Once Faketoken is on the customer's smartphone, attackers gain access to the customer's banking account via the computer infected with the banking Trojan and the compromised mobile smartphone allows them to intercept the one-time authentication code.

The second family of mobile banking Trojans is Trojan-Banker.AndroidOS.Marcher. After infecting a smartphone, the malware tracks the launch of just two applications: the mobile banking customer of a European bank and Google Play. If the user starts Google Play, Marcher displays a false window requesting credit card details which then go to the attackers. The same method is used by the Trojan if the user starts the banking application.

7.5.2.4 Evaluation and recommendations

Mobile banking services allow customers to use a mobile device for transactions such as balance enquiries, ordering cheque books and completing funds transfers, which means that this technology would offer greater freedom to customers to manage their bank accounts. Mobile banking is potentially more readily available than online banking, since mobile phones are widely used compared to more traditional computers. For female household customers, the use of mobile banking would facilitate banking activities that they currently perform in person by visiting a bank branch or using an ATM, both of which are made burdensome by the movement limitations on Saudi females. For male household customers, the use of this technology might make it even easier to maintain secret bank accounts, since they can be managed directly from a personal device such as a smartphone, whereas the use of online banking requires a

computer, which is more likely than a smartphone to be a shared device. In addition, if a computer is shared by a household, there will be increased opportunities for its members to monitor banking activities when using online banking, while this would not be as easy when using a personal smartphone for mobile banking. However, studies show that many Saudis are unaware that their banks offer mobile banking. Banks in Saudi Arabia should advertise to raise customers' awareness of the usefulness of mobile banking and should highlight the full functionality of their systems to respond efficiently to users' different banking needs. For its part, SAMA should improve its policies regarding the use of banking technologies and should adopt specific policy and guidance on the use of mobile banking services. Finally, banks should take the lead by offering awareness programmes and training to educate customers about mobile banking threats and the consequences of sharing practices; by doing so, the banks would be following SAMA policy regarding customer education mentioned in Section 7.3.2.

7.6 Chapter Summary

This chapter has covered the three essential elements of the framework for evaluating the security of household bank customers in the KSA: It first presented the household context of use of bank system in the KSA, then discussed the policies and infrastructure of Saudi banks, before analysing in detail the security of the three bank technologies and processes used by household customers in this research. As reported in Section 2.5, Dourish and Anderson (2006) found that in order to give an adequate account of computer users' practices, it is necessary to have a deep understanding of these practices and of their social and cultural context; the practices must also be related to the concepts of risk, danger, trust, secrecy, identity, morality and power from which they derive their meaning. The framework presented here satisfies these requirements. The roles of

STRIDE and DREAD are important in focusing on the security of the bank system, and integrating this with the findings of the household context of use means that the resultant framework would cover both security and cultural aspects of the bank system. The chapter ended by evaluating the security of household banking, by applying the framework to two case studies. The first evaluated the use of fingerprint as a new security mechanism with an existing technology, in the authentication of bank cards. The second case study discussed the application of the framework to evaluate the security of mobile banking, a technology not used by the household customers who participated in this research.

8 CONCLUSION

8.1 Overview

The aim of this research has been to evaluate the security of household banking in the KSA by investigating the fit between the bank system and the banking practices of household customers. Saudi banks operate as part of a worldwide banking system; to evaluate the security of the Saudi banking system within this global framework, the present study has sought to identify the banking practices of household customers, to explore the motivations and other factors influencing them and to interrogate the relevant technical banking requirements and regulations. This research responds to the need to identify the banking practices of household customers and to assess the significance of their effects on the security of the banking system, in order to inform future research efforts into making that system more secure. Based on the identification of these practices, a framework is proposed which provides a means of addressing both technical and human factors and evaluating them, as a contribution towards a secure and effective banking system. Without a framework describing customers' practices and the related requirements, it would be difficult to evaluate the current system or to propose improvements that would make it more effective, more secure and more responsive to the actual banking practices of Saudi Arabian household customers. The framework that

is proposed here therefore has important public policy implications for efforts to achieve a more competitive and efficient financial system. The study could help the regulatory authorities to determine what future courses of action should be pursued to further strengthen the Saudi Arabian banking sector, particularly the domestically incorporated banks.

Therefore, the overall research question addressed by this work is: How can the security of Saudi bank systems be evaluated by considering household customers' banking practices?

More specifically, it has sought answers to these two sub-questions, reproduced here from the introduction to Chapter 1:

RQ1: What are the banking practices of household customers of Saudi banks that affect the security of the banks' systems?

RQ2: How can technical security mechanisms be augmented in Saudi banks' systems to improve the fit between the banking practices of their household customers and the banks' technical systems?

To find answers to these questions, the study has elicited data from household customers on their banking practices, analysed the applicable policies and infrastructure, and investigated the banking technologies used and processes followed. An empirically based framework has thus been created for the evaluation of household banking practices and the security of the system currently operating in the KSA. It is worth mentioning here that the focus of this thesis is not on changing Saudi Arabian cultural norms or legislation on allowing women to drive, or otherwise reducing or minimising the influence of gender in Saudi culture; rather, its focus is on evaluating the banking system with a view to making it more compatible with existing legal and sociocultural

realities, in order to ensure the equal provision of secure banking for both male and female customers.

The remaining sections of this concluding chapter lay out the contributions of the study (Section 8.2), offer a critical review of the study (Section 8.3) and consider suggestions for future work (Section 8.4).

8.2 Contributions

8.2.1 Substantive contributions

8.2.1.1 Identifying practices

The investigation of customers' practices in Chapter 4 has shown that household bank customers in the KSA regularly violated bank regulations by sharing bank credentials, consistent with the findings of several published studies (Singh 1997, Singh and Cassar-Bartolo 2004, Singh, Cabraal et al. 2006, Singh, Jackson et al. 2006, Singh, Cabraal et al. 2007a, Singh, Cabraal et al. 2007b, Singh 2008).

In addition, Chapter 5 has revealed that bankers are aware of credential sharing among household customers and the banking perspective of shifting the responsibility of household banking security entirely onto the customers. Moreover, bankers pointed out that this sharing practice would have the effect of damaging the reputation of banks and banking; the banking authorities should respond to this point by paying more attention to this practice and its consequences.

This is the first study of its kind in its identification of the specific insecure practices that participants adopted in KSA and of the household contexts of use in which they did so. It makes it possible for banks to target these specific practices in the measures they undertake to improve banking security among their household customers.

8.2.1.2 Household context of use.

At the heart of the research reported in this thesis lies a model of household context of use and of the factors which motivate their adoption, as depicted in Figure 6 (for a detailed model, see Appendix 11). It includes a number of factors such as the influence of the head of the household, the role of gender and the lack of customer education. Knowledge of these causative and motivating factors and of their interplay provides a fuller understanding of the ways in which customer practices are determined in specific situations. Moreover, the model was consciously created without resorting to the findings that had been generated by the limited amount of previous research in this field.

8.2.1.3 A conceptual framework for evaluating banking security

Chapter 7 has shown how the findings presented in this thesis can be used by banks to evaluate household banking. The framework makes the findings easily accessible and applicable to bank developers and security analysts on whom the banks rely to ensure the effectiveness of their security. Without such a conceptual framework, it would be unclear which elements of the existing Saudi banking system are responsible for positive outcomes and which can be improved on; we are unaware of any conceptual framework which integrates details of the systems of Saudi banks with the banking practices of their household customers.

8.2.2 A practical guide to the methodology

Chapter 3 has presented a detailed discussion of the efforts to explore the available and previously used qualitative methods, of the selection of the appropriate one to collect data from participants, of the challenges faced and of the amendments made to adjust each method to the context of a conservative culture such as that of the KSA. This would constitute a useful guide for researchers intending to use qualitative methods

with both male and female informants in such cultures, preparing them for the challenges that might occur and suggesting possible solutions.

8.2.2.1 Reflections on building rapport with participants

As mentioned in Section 3.6.3, I built rapport with participants by sharing my status as a married woman and mother, studying at the well-known and prestigious University of Oxford. I noticed that the fact that I am a Saudi, which is obvious from my surname, increased this rapport, as illustrated by this comment from a participant concerning the ban on women driving in the KSA:

Women can't drive here… You know this… You are from the Alghamdi tribe, so you're one of us and you already know this. [P45, F]

The building of this rapport with participants was reflected in the level of trust and understanding that it helped to create between them and me, making it more likely that they would take my study seriously. Meanwhile, my status as a Saudi helped to make participants feel relaxed and comfortable, since they would expect me to be able to understand them and their practices and motivations without judging them or requiring them to provide lengthy explanations.

8.2.2.2 Reflections on the sensitivity of the research topic

My rapport with the participants, as noted above, helped to build understanding and trust, allowing them to feel relaxed and comfortable. However, discussing threats within the household context raised the possibility of insider threats and of family members acting against one another, topics which required very sensitive handling. Interestingly, one of the participants in the current research raised this point when he gave an example of an insider threat, relating how his female cousin had asked him to help her retrieve her bank card from her husband (full details are given in Section 6.3.4.1). When the

researcher asked this participant whether it would be possible to interview his cousin (the victim) to obtain more information about this incident, the participant refused, citing the sensitivity of this topic:

I don't think she will really accept sharing this information with you because you are a stranger and being a victim is rather embarrassing… She shared this information with me because I'm a relative and she asked me to get involved and talk to her husband to try to get her card back. ... I think you may have met people in your study who are victims or offenders but they did not admit this to you ... because this topic is quite sensitive. It's embarrassing to discuss this with strangers if you are a victim or an offender. [P34, M]

8.2.2.3 Reflections on the methods of collecting data

Telephone interviews were well chosen as offering a straightforward method of collecting data from participants. Although I was unable to observe and record participants' physical responses, using this method did allow me as researcher to collect sufficient and deep data from participants of both genders and to identify and discuss customers' practices related to the use of bank systems.

As to the use of the focus group technique to collect data from household customers, despite all of the challenges detailed in Section 3.6.4, this method facilitated an exploration of participants' thoughts and opinions regarding real-world situations. Focus groups are useful, but researchers must be aware that some members may not express their opinions freely if they believe that to do so would conflict with religious obligations or cultural norms, or that other group members might not accept or respect their opinions. This shortcoming was illustrated when a member of the daughters' focus group said that she would not share her credentials with her father, at which the other

members glared at her and made it clear that they considered her remark to be unacceptably disrespectful to her father.

The use of diaries to collect data from customers in the third round provided a log of factual data regarding the daily banking practices of household customers. Compared to the methods used in the first two rounds, considerable investment of time, resources and effort was required by participants and the researcher to ensure that the diaries prepared were fit for purpose and met the aims of the research. This method required participants to be given both training prior to keeping their diaries and ongoing support while doing so. The researcher was very sensitive to the diversity of participants and to the type of information that needed to be elicited. As explained in Section 3.6.5, it became clear that it would not be possible for the diaries to be audio recorded on smartphones, because of the relatively low level of IT skills of some of the participants, especially the older ones, and because of the religious objections of some of participants; therefore, it was decided to revert to the use of written diaries. As the interviews followed the writing of the diary, the researcher took the opportunity to ask each participant at the end of the interview about writing the diary. The questions were about the diary period, the method and the use of WhatsApp to remind and support the participants. Analysis of the responses (see Appendix 12, shaded codes) reveals that although none of the participants had kept a diary before, either in their personal lives or for research purposes, they did not find it difficult or inconvenient to do so, especially because they found that a month was an acceptable duration for the exercise. In addition, most participants kept pen and paper in a drawer near their bed and recorded each night all of the banking transactions that they had carried out that day. Participants also reported that the WhatsApp messages reminding them to keep recording led them to feel that they were in touch with the researcher and not isolated.

It is worth mentioning here that the benefits of using multiple methods of data collection are to increase the trustworthiness and validity of the data and to obtain multiple perspectives, so that the limitations of any particular method or the conditions of any of the rounds of collection would not confound the final results.

8.3 Critical Review

8.3.1 Research scope

The research documented in this thesis has provided a grounded theory model of the banking practices of household customers and of the factors influencing their choices. This research relies on an exclusively qualitative analysis because quantitative research questions would have restricted and predefined from the outset the phenomena under investigation, whereas no model of these phenomena had previously existed. A consequence of using qualitative methods was to limit access to participants in two senses. Firstly, a much smaller number of participants than would typically have been recruited for quantitative research could be employed here, because of the very time-consuming nature of qualitative analysis. It should also be emphasised that this study is qualitative and that one of its purposes has been to provide a detailed account of household customers' banking practices, not a statistical record; the sample size would have been inadequate for the latter purpose but satisfied the former. Secondly, volunteers had to be willing to spend an hour or more participating in an interview or focus group, or keeping a diary for a whole month, which reduced the number of recruits. In addition, recruiting participants for this research required the use of the mail system of Umm Al-Qura University, access to which is limited to Saudi nationals only. This led in turn to a restriction on the backgrounds from which participants could realistically be recruited. For example, while acknowledging that the practices and opinions of foreigners living in the KSA would also have been worthy of investigation,

the study was limited in practice to the households of Saudi nationals. This exclusive focus on those of Saudi nationality can be seen as allowing the study to retain a relatively consistent cultural perspective. However, the scope of such research could beneficially be extended in future to cover non-Saudis living in the KSA.

8.3.2 Thesis complexity

There is a dual complexity to the grounded theory model that this research has adopted, arising from the fact that many factors are incorporated and from their multiple interactions. This is a necessary consequence of the complexity of the phenomenon itself, valuable information about which would be lost by oversimplification. The model is structured hierarchically, however, with a storyline at the highest level which its users must be able to access. The difficulty in using it properly lies in the fact that this requires some understanding of more complex aspects at lower levels of the model. However, Chapter 7 is aimed strongly at actual beneficiaries of the findings presented here, who want to employ them to evaluate the security of household banking in the KSA. It is hoped that the application of the framework presented and discussed in Sections 7.5 and 7.5.2 will make it possible for bank developers and security analysts to use the findings in precisely this way.

8.3.3 Framework validation and evaluation

It is important to validate and evaluate the framework emerging from this research, but it proved difficult to recruit, for this purpose, one or more security analysts who had a sound background in Saudi culture. Great efforts were made to contact members of the security committees of various Saudi banks, these efforts being complicated by the fact that such committees would be exclusively male in their membership and would operate only at the banks' provincial head offices. In the event, there was no response from any

of them. However, it should be borne in mind that the framework was built using grounded theory, meaning that it is grounded in the data elicited from both household bank customers and bankers, so that its validity can be seen to derive from the validity of grounded theory itself and from the meticulous application of its methods to the building of the framework.

The trustworthiness and validity of the data are also augmented by the triangulation achieved through the use of multiple techniques to collect them from participants. The benefit of the data being triangulated in this way is that the limitations of any particular methodology or of the conditions of any of the rounds of collection would not confound the final theory.

8.4 Future work

8.4.1 Testing the model's theory

The model of household context of use has revealed that the sharing of credentials is a common banking practice among household customers. The analysis of the data has shown that this sharing practice is widely adopted in the controlling and protective environment of male guardianship; however, this theory and its potential implications are open to future investigation and should be tested in a larger scale study.

8.4.2 Testing the model's predictions

This research into the banking practices of household customers has taken grounded theory as its primary methodology because this has enabled the modelling of a complex phenomenon which not much was known about before the work began. An experimental methodology would not have been certain to examine all of the significant influential factors, because it would have been necessary to make assumptions as to their existence and identity at the outset. It follows from this distinction between the two

investigative approaches that experiments could now be designed on the basis of the grounded theory model which this research has developed, testing its predictions, with the potential to augment confidence in the results of the present analysis. Such experiments would also allow the quantification of the relative importance of the factors included in the model to begin. In addition, such experiments will make it possible to improve the security of household banking by revealing new ways of influencing the factors proposed by the model, hence influencing in turn the banking practices of household customers.

8.4.3 Comparative studies

Section 8.3.1 has pointed out that the scope of the research findings is currently limited because a side effect of using qualitative methods was to limit access to potential participants. The study was also limited in practice to the households of Saudi nationals in order to retain a relatively consistent cultural perspective. However, the scope of such research could beneficially be extended in future to cover non-Saudis living in the KSA. It would also be important for future research to investigate other populations so that the findings could be generalised. While the methodology used here could be replicated, thus creating models of other populations which could then be compared to the one presented in this thesis, a more practical approach would be form focus groups from among other populations, asking them questions whose aim would be to validate or disconfirm the identity and interactions of the factors comprising the present model, without excluding the possibility that alternative factors would emerge. Alternatively, an experimental approach, as suggested in section 8.4.1, would make it possible to more rapidly validate the model for larger populations.

8.4.4 Non-banking familial practices

The scope of the current study focuses on the practices of household customers when using Saudi bank systems. The results reveal the strong influence of family relationships on banking practices and the close commitment of bank customers to their families, extended families or extended relationships. Such influences arise because in a collectivist culture like that of Saudi Arabia, loyalty is critically important and overrides almost all social rules, which means that it is pointless to adopt an information security standard without customising it to the culture concerned. Understanding and exploring this factor would benefit the HCI literature on the familial practices influencing both the security and privacy of non-banking systems. Further research is needed into the influence of familial practices on social networks, for instance, and the findings of the current research can be seen as making a good start.

9 APPENDICES

APPENDIX 1: PILOT STUDY QUESTIONS 227

APPENDIX 2: FOCUS GROUP QUESTIONS 229

APPENDIX 3: SAMPLE DIARY 231

APPENDIX 4: INTERVIEW QUESTIONS WITH CUSTOMERS IN THE 3RD ROUND OF DATA COLLECTION 232

APPENDIX 5: INTERVIEW QUESTIONS FOR BANKERS 234

APPENDIX 6: INVITATION LETTER 236

APPENDIX 7: CONSENT FORM 239

APPENDIX 8: SAMPLE OF DATA CODING 242

APPENDIX 9: MODEL OF HOUSEHOLD CUSTOMERS' PERSPECTIVE 243

APPENDIX 10: MODEL OF BANKING PERSPECTIVE 244

APPENDIX 11: HOUSEHOLD CONTEXT OF USE OF BANK SYSTEM 245

APPENDIX 12: CODES AND MEMOS 247

APPENDIX 13: INSIDER ATTACK CASES 258

APPENDIX 1: PILOT STUDY QUESTIONS

Bank account
Do you use a credit card? Tell me about it.
PROMPT: e.g. Is it for a personal or joint account?
How long have you had this account?
How many times per week do you use this card?
What do you use the card for?

Do you use online banking? Tell me more about this.
PROMPT: e.g. Is it for a personal or joint account?
How long have you had this account?
How many times per week do you use this card?
What do you use the card for?

Does your partner use a credit card? Tell me more about it.
PROMPT: e.g. Is it for a personal or joint account?
How long have you had this account?
How many times per week do you use this card?
What do you use the card for?

Does your partner use online banking? Tell me more about it.
PROMPT: e.g. Is it for a personal or joint account?
How long have you had this account?
How many times per week do you use this card?
What do you use the card for?

Are you involved with the banking arrangements of your wider family?
Children, parents/grandparents, brothers/sisters?

How frequently do they (your family) use online banking and ATM cards?

How do you access your online banking?
PROMPT: e.g. smartphone, personal computer, shared personal computer or work computer?
If you use a shared computer, do you share the credentials for that computer? Or do you have you own account on that one computer?

Can you tell me how your online banking is protected?
PROMPT: e.g. password, token, one-time authentication code, etc?

Have you ever been in the situation of "online banking credential sharing" with...?
Partner, family, others?
If yes, then why?

Have you ever shared your ATM card's PIN with...?
Partner, family, others?
If yes, then why?

Are you aware of your bank's policy regarding the protection of your banking authentication?
This would cover both ATM card and online banking authentication?
Has your bank warned you not to tell anyone your password?
Have you ever thought about what would happen to your banking security if you got separated from your partner?
This issue of "sharing password and then separating" has come up in discussions with people. What do you think about it?

Demographic questions
Tell me about yourself.
Age
Education level
Employment status
Salary range

Tell me about your partner.
Age
Education level
Employment status
Salary range
How long they have been together

Tell me about your family.
Children, Parents/Grandparents, Brothers/Sisters
Living arrangements
Do people live together?
Are they geographically close?
Do they meet frequently?

APPENDIX 2: FOCUS GROUP QUESTIONS

The following are common methods of using bank accounts. Please arrange them from the most often used to the least (How frequently you use each of them):
Online banking.
ATM.
Visiting a bank branch.
Online shopping.
PayPal.
Sales points.
Others (please name them).

The following are common reasons to use bank accounts. Please arrange them from the most often used to the least:
Checking credit/transactions
Checking salary
Paying bills, rent, etc
Drawing cash
Making money transfers
Others (please name them)

In what situations would someone else have access to your account?
Who?
Why?
How does he/she access your account?

In what situations would you have access to someone's account?
Whose account is it?
Why do you have access?
How do you access it?

Ahmad shared his bank authentication with his wife and after a big problem with her, he found that she had accessed his account online and transferred money to her account without his permission.
Do you think Ahmad made a mistake when he shared his account authentication with his wife? Why?
What if he did not share his authentication with her? Do you think this is acceptable? Why?
Can you list the reasons why it is (not) acceptable? Can you rank them in order of importance?
Do you think sharing authentication is a common practice between couples in the KSA? Why?
What if the opposite happened (*he* accessed and transferred *her* money without her permission)? Is that acceptable? Why?
Can you list the reasons why it is (not) acceptable? Can you rank them in order of importance?

When Eman opened a bank account, her father signed the papers so as to have access to her account even without her permission (full procuration).
Can Eman refuse this? Why?
In what situations would this be acceptable?
Do you think this situation would be different if Eman was a son, not a daughter?
Do you think this is common in father/daughter relationships? What about mother/daughter? Why?
Do you think this is common between father and son? What about mother/son? Why?

Ali is the eldest son in his family and therefore he manages the family's affairs, which involves accessing the bank accounts of his father, mother and sisters.
Do you think this is common in the KSA? Why?
What if one of the sisters refused this arrangement? Can she? Why? What can she do to stop this?
Do you think Ali would have access to his brothers' accounts?
Why is there a difference in brother/brother and brother/sister relationships?
Do the siblings' ages make any difference?

Why would a mother, wife, husband, father, son or daughter share his/her account authentication with someone?
To make life easier?
Because they have to? Why?
Can the account holder stop this sharing? How? What are the consequences?
Is there any difference between a wife and a mother?

APPENDIX 3: SAMPLE DIARY

Dear Participant,

Thank you for participating in my study. The following are examples of diaries that might help you in keeping a diary about your banking practices. If you have any questions, please contact the researcher (deena.alghamdi@cs.ox.ac.uk).

Tuesday, 27/12/1435 H.

I used my account by using ATM machine to make bank account inquiry and withdraw cash.

Wednesday, 28/12/1435 H.

I used my account by using ATM machine to make a transfer to my wife's account.

Thursday, 29/12/1435 H.

I used online banking to check my credit and to transfer money to my brother's account.

Saturday, 1/1/1436 H.

I used online banking to check my credit and transferred money for charity.

Monday, 2/1/1436 H.

I used my wife card to withdraw money for her from her bank account.

Tuesday, 3/1/1436 H.

I used the phone banking service to check my credit and transfer money to my son's account.

Friday, 6/1/1436 H.

I used my husband's card in point-of-sale to pay for shopping.

Saturday, 7/1/1436 H.

I used online banking to pay the electricity bill for my house.

Best regards

Deena Alghamdi

APPENDIX 4: INTERVIEW QUESTIONS WITH CUSTOMERS IN THE 3RD ROUND OF DATA COLLECTION

Introduction to the domain
Could you give me an overview of your bank accounts?
How many accounts? Why do you have more than one bank account?
In which bank? Why?
Joint or personal? Why?
How long have you had your account(s)?
Questions based on the participant's diary
In your diary, you mentioned that on the 25th you used online banking to check your salary and pay your electricity bill... Can you tell me more about using online banking to *check your salary*, *pay bills*?
Do you often use online banking for …?
Do you use other methods for …?
Can anyone else access your account via online banking? Who? Why? Since when? How did that start?
What if you wanted him/her to stop accessing your account?
Could you ask him/her to stop?
What are you going to do?
How does this sharing affect your life? **PROMPT:** e.g. make it easier, more difficult, having a backup of your bank authentication.
Do you use online banking to access someone else's account? Partner? Son? Daughter? Mother? Father? Sibling? Other? Why? Since when? How did that start?
What if he/she asked you to stop accessing his/her account?
What would happen if you suddenly found that he/she had changed the account password?
Do you access his/her account using other methods such as ATM?
How do you access your online banking? **PROMPT:** e.g. smart phone, personal computer, shared personal computer or work computer?
If you use a shared computer, do you share the credentials for that computer, or do you have your own account on that one computer?
Sharing questions
Have there been any conflicting perspectives arising from sharing or not sharing security details (or is there always agreement)?
If there is no conflict: Is sharing (or not sharing) such information considered an **expected thing**? Why?
If there is conflict: Who raises objections? Why?
What are the situations where these objections become apparent? Do you **accept** this conflict? Why?
Is it considered a **privacy**, **security** or **trust** issue?
Have you ever thought about what would happen to your banking security if any members of your family were to become estranged?

Permission questions
This issue of sharing security details and then using them to access an account without permission has come up in discussions with people. What you think about it?
Has this happened to you before (or have you done it before)?

To what extent is it acceptable to have access to your (wife's, mother's, father's, …) account without permission?
When does it become unacceptable?
What counts as "permission"? **PROMPT:** e.g. variable permission? You tried once and he didn't say anything so you continued accessing his account? You are expected to have permission because …?
Has it ever happened that you gave someone broader permission to access your account than before? **PROMPT**: e.g. before, he only had access, but now he can also transfer money?
Why? What happened? How did you express to him that he now had broader permission?
Has someone else given you broader permission to access his/her account than before?
Why? What happened? How did he/she express that to you?
Do you know anyone who has been in a similar situation?

Demographic questions
Can you tell me about yourself?
Age
Education level
Employment status
Salary range

Can you tell me about your partner?
Age
Education level
Employment status
Salary range
How long have you been together?

Can you tell me about your family?
Children, parents/grandparents, brothers/sisters
Living arrangements
Do these people live together?
Are they geographically close?
Do they meet frequently?

APPENDIX 5: INTERVIEW QUESTIONS FOR BANKERS

How can a customer open a bank account? Do you explain to him his rights and obligations especially regarding card PIN?
Online banking:
How can a customer use online banking? Do you help the customer set up this service? Does the customer expect you to help him set this service up for him? Do you explain to him his rights and obligations especially regarding username/password?
Customers:
Have you ever noticed any of the customers sharing bank information (PIN, card, online banking username/password) with others?
If yes, How and what you did then with the customer? Have you reported this to your supervisor, if yes what happened then, if no why?
If no, did you ever asked any of the customers about this? What if you noticed this, what is the procedure that you have to follow?
Although you have noticed customers share bank information, why is the bank not focusing on educating customers about the rules around this to reduce this practice?
What are the risks from sharing as far as you know/have heard/expect?
Has it ever happened that a male/female customer came to you and say "I did not do this transaction" or "There is money missing from my account"? What did you do? What is the procedure if that happened?
What is the bank offering to educate customers about their rights and responsibilities?
Is there anything the bank offers especially for female customers? (To protect them/educate them/ help with mobility)
Some of the bank procedures are not as easy for women as for men because of mobility limitation differences (such as using ATM to activate a user for online money transfer) which may cause more trouble for women than men. Did the bank consider that?
Have you known a case of a man identifying a woman as his wife/sister/mother then you found that she was not?
Bankers:
Why are there men-only branches and women-only branches? How it did this start?
What is the difference between them? Why?
Why are women-only branches just tokens and not fully independent branches?
Can a male banker serve a female customer?
Can a female banker serve a male customer?
Can a woman banker contact a man banker? What about the opposite?
Can a woman banker have access to a men's branch? What about the opposite?
Are there any gender differences between male and female bankers?
Do women branch managers have the same authority/responsibility/training as men branch managers?
Future of banking:
Do you know if the bank is planning in the future to move to things like contactless payments or smartphone payments?

APPENDIX 6: INVITATION LETTER

Department of Computer Science
University of Oxford
Wolfson Building
Parks Road
OXFORD
OX1 3QD UK

دعوة للمشاركة في الدراسة

السلام عليكم ورحمة الله وبركاته

عزيزي المشارك

أنا دينا الغامدي و أنا طالبة دكتوراه في السنة الثالثة بجامعة اكسفورد ،قسم الحاسب الالي. بحثي بعنوان "اطار نظري لتمركز أنظمة البنوك البنكية في المملكة العربية السعودية حول المجتمع و الثقافة"

"Conceptual Framework for the Socially and Culturally Centred Design of Saudi Bank Systems".

هذه الدراسة تركز علي دراسة ممارسات العوائل السعودية و بالخصوص ممارسات التحقق من الهوية. تدور هذه الدراسة حول أنظمة البنوك (بطائق الصراف والبنك الالكتروني). يتم اختيار مشاركين في هذه الدراسة لانهم مواطنين سعوديين. و كمشارك لديك الحق بطرح أي سؤال عن البحث. وكون مشاركتك تطوعية فلك الحق بالانسحاب متي تشاء ودون الحاجة لتقديم أي مبررات ومن دون أي عواقب علي حقوقك القانونية. أذا كان المشارك طالب فلن تكون هناك عقوبات اكاديمية في حال عدم المشاركة في الدراسة. سيتم تنظيم المشاركة في الدراسة كالتالي:

- سيكون هناك ٤ مجموعات منفصلة للمشاركة فيها: مجموعة الاباء، الابناء، الأمهات، البنات.
- مجاميع الذكور ستكون بقيادة د.جهاد العمري، ومجاميع النساء بقيادتي.
- سيتم الاعلان لاحقا عن مكان المجاميع ولكن سيكون في مكان عام.
- سيتم تسجيل المشاركة صوتا وصورة ثم تفريغها علي الورق بعد ذلك.

هذا المشروع تمت مراجعته واعتماده من أخلاقيا من اللجنة الاخلاقية للأبحاث في جامعة أكسفورد. وهذ البحث سيتم كتابته كرسالة دكتوراه للطالبة ويسلم لجامعة أكسفورد وسيتم نشرة الكترونيا. تلتزم جامعة اكسفورد بنشر ابحاث منسوبيها ليستفيد منها المجتمع والاقتصاد و كدعم لهذا الالتزام فقد تأسس ارشيف الكتروني لتخزين الابحاث. هذا الارشيف يتضمن نسخ الكترونية لرسائل الدكتوراه الخاصة بطلاب الدراسات العليا. وهذا الارشيف يوفر سرعة الوصول للأبحاث مجانا مما يزي من احتمالية تنفيذها.

في حال موافقتك علي المشاركة في الدراسة سيتم كتابة هذه الدراسة كرسالة دكتوراه وتسليمها كنسخه ورقيه مطبوعة واخري الكترونيه لتخزينها في ارشيف الجامعة الالكتروني. سيتم نشر هذه الرسالة الكترونيا لتكون متوفرة لجميع مستخدمي الانترنت.





Department of Computer Science

University of Oxford

Wolfson Building

OXFORD

OX1 3QD UK

Invitation to Participate in a Study

Hello everyone,

My name is Deena Alghamdi, and I am a second year DPhil student in the Computer Science Department at Oxford University. My research title is "Conceptual Framework for Socially and Culturally Centred Design". This study focuses on the security practices of Saudi families, in particular authentication practices. The broad scope of this research will cover user authentication for bank accounts, credit card and online banking passwords.

The people who are invited to take part in this study are all nationals of the Kingdom of Saudi Arabia. As a participant, you have the opportunity to ask questions about the research. Your participation is voluntary, and you are free to withdraw at any time without giving any reason and without any consequence. This study requires the participation of you and members your family, such as your father, mother, sisters, brothers and children (above 18). You will first participate in a focus group to discuss practices and concerns about bank accounts and bank usage. The focus group session, lasting two hours, will be gender segregated and will be audio recorded. The recording will be transcribed and used as part of the study. There will be a follow-up telephone interview, lasting up to an hour, which also be audio recorded, transcribed and used as part of the study. Please note that anonymised quotes may be used in presentations or publications stemming from the research, but not in any way that might allow for identification of individual participants. In addition, the data will be kept confidential at all times.

This project has been reviewed by, and received ethical clearance through, the University of Oxford Central University Research Ethics Committee. The project will be written up as a

student's thesis that will be submitted to Oxford University, published and stored online. The University of Oxford is committed to the dissemination of its research for the benefit of society and the economy and, in support of this commitment, has established an online archive of research materials. This archive includes digital copies of student theses successfully submitted as part of a University of Oxford postgraduate degree programme. Holding the archive online gives easy access for researchers to full text of freely available theses, thereby increasing the likely impact and use of that research.

This research aims to understand the social and cultural practice of household bank customers in Saudi Arabia. As a result of these research findings, it is hoped that new guidelines will emerge for the design and development of bank systems in the Kingdom.

If you are willing to participate in this study (or have any questions or concerns about any aspect of the research) please contact the researcher (deena.alghamdi@cs.ox.ac.uk).

Best regards

Deena Alghamdi

Department of Computer Science

University of Oxford

Wolfson Building, Parks Road

OX1 3QD, UK

+44 (0) 1865610801

e-mail: deena.alghamdi@cs.ox.ac.uk

APPENDIX 7: CONSENT FORM

UNIVERSITY OF OXFORD
DEPARTMENT OF COMPUTER SCIENCE

Department of Computer Science
University of Oxford
Wolfson Building
Parks Road
OXFORD
OX1 3QD UK

موافقه بالمشاركة في الدراسة

Conceptual Framework for the Socially and Culturally Centred Design of Saudi Bank Systems

أطار نظري لتصميم أنظمة بنوك في السعودية متوافقة حضاريا واجتماعيا

Please read and confirm your consent to participate in this interview by signing and dating this form.

الرجاء قرأه ما يلي و التأكيد علي الموافقة بالتوقيع:

1. I confirm that the purpose of the study has been explained to me and that I have had the opportunity to ask questions about the research and have had these answered satisfactorily.

   ١- أأكد أنه تم شرح لي الغرض من هذه الدراسة و أني حصلت علي الفرصة لأسأل للحصول علي المزيد من الإيضاحات و أنه تم الإجابة علي أسئلتي وبوضوح.

2. I understand that my participation is voluntary, and that I am free to withdraw at any time without giving any reason and without any implications for my legal rights.

   ٢- أنا علي علم أن مشاركتي في هذه الدراسة هي مشاركة تطوعية بحتة وأنه يمكنني التوقف والانسحاب متي ما رغبت دون الحاجة للإعطاء توضيحات ودون ترتب أي نتائج علي حقوقي القانونية.

اذا كان لديك اي سوال بخصوص هذا البحث فيمكنك الاتصال بالمشرفين والذين سيقومان بما في وسعهما للاجابة علي استفساراتك.

Ivan Flechais, Department of Computer Science, University of Oxford, Wolfson Building, Parks Road,OX1 3QD, UK, e-mail at ivan.flechais@cs.ox.ac.uk and **Marina Jirotka**, Oxford e-Research Centre, 7 Keble Road, Oxford, OX1 3QG, UK, +44 (0) 1865 601613, or by e-mail at marina.jirotka@oerc.ox.ac.uk

أذا ما زلت غير راضي و تريد التقدم بشكوي خطية فيمكنك الاتصال بـ:

If you remain unhappy and wish to make a formal complaint, please contact the Research Ethics Committee at the University of Oxford at ethics@socsci.ox.ac.uk; +44 (0)1865 614871; Social Sciences & Humanities Inter-Divisional

3. I am allowing the researcher to audio record me as part of the study. The recordings will be transcribed. I understand that anonymised quotes may be used in presentations or publications stemming from the research but not in any way that might allow for identification of individual participants.

٣- أنا أسمح للباحثة بتسجيل المقابلة صوتيا كجزء مهم لعمل الدراسة، ويترتب عليه قيامها بتفريغ المقابلة بعد ذلك علي الورق. كما أنني أعلم أنه و بالمحافظة علي سرية معلوماتي الخاصة قد يتم الإشارة لجزء من مقابلتي و استعمالها في أبحاث منشوره متعلقة بالبحث ولكن مع المحافظة على سرية معلوماتي.

4. I understand the data will be kept confidential at all times.

٤- أنا علي علم أنه سيتم المحافظة علي سرية المعلومات دائما.

5. I agree to take part in this study.

٥- أنا اوافق علي المشاركة في هذه الدراسة.

Name of participant: **أسم المشارك:**

Signature: **التوقيع:**

Date: **التاريخ:**

اذا كان لديك اي سؤال بخصوص هذا البحث فيمكنك الاتصال بالمشرفين والذين سيقومان بما في وسعهما للإجابة علي استفساراتك.

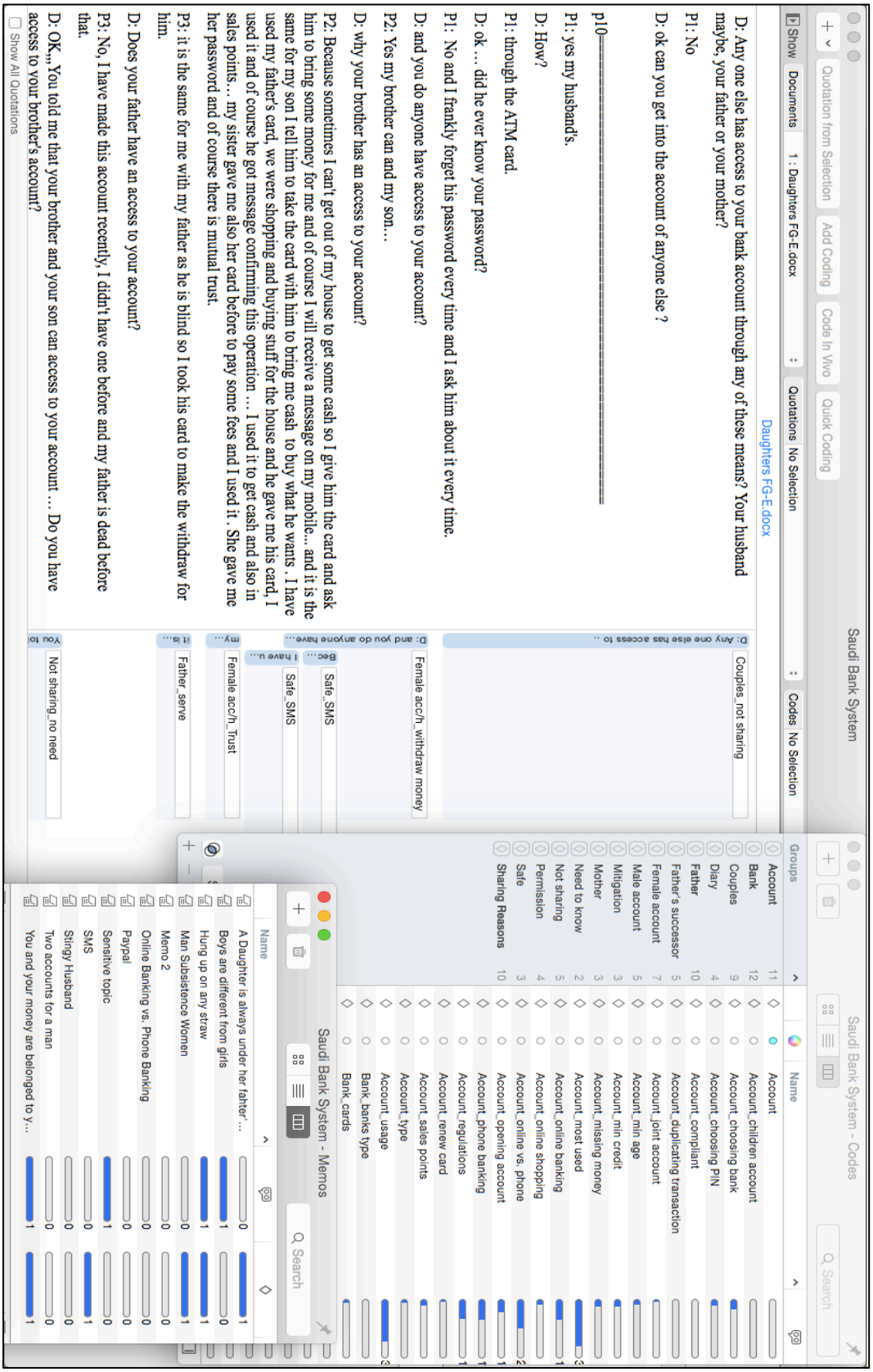
Ivan Flechais, Department of Computer Science, University of Oxford, Wolfson Building, Parks Road,OX1 3QD, UK, e-mail at ivan.flechais@cs.ox.ac.uk and **Marina Jirotka**, Oxford e-Research Centre, 7 Keble Road, Oxford, OX1 3QG, UK, +44 (0) 1865 601613, or by e-mail at marina.jirotka@oerc.ox.ac.uk

أذا ما زلت غير راضي و تريد التقدم بشكوي خطية فيمكنك الاتصال بـ:

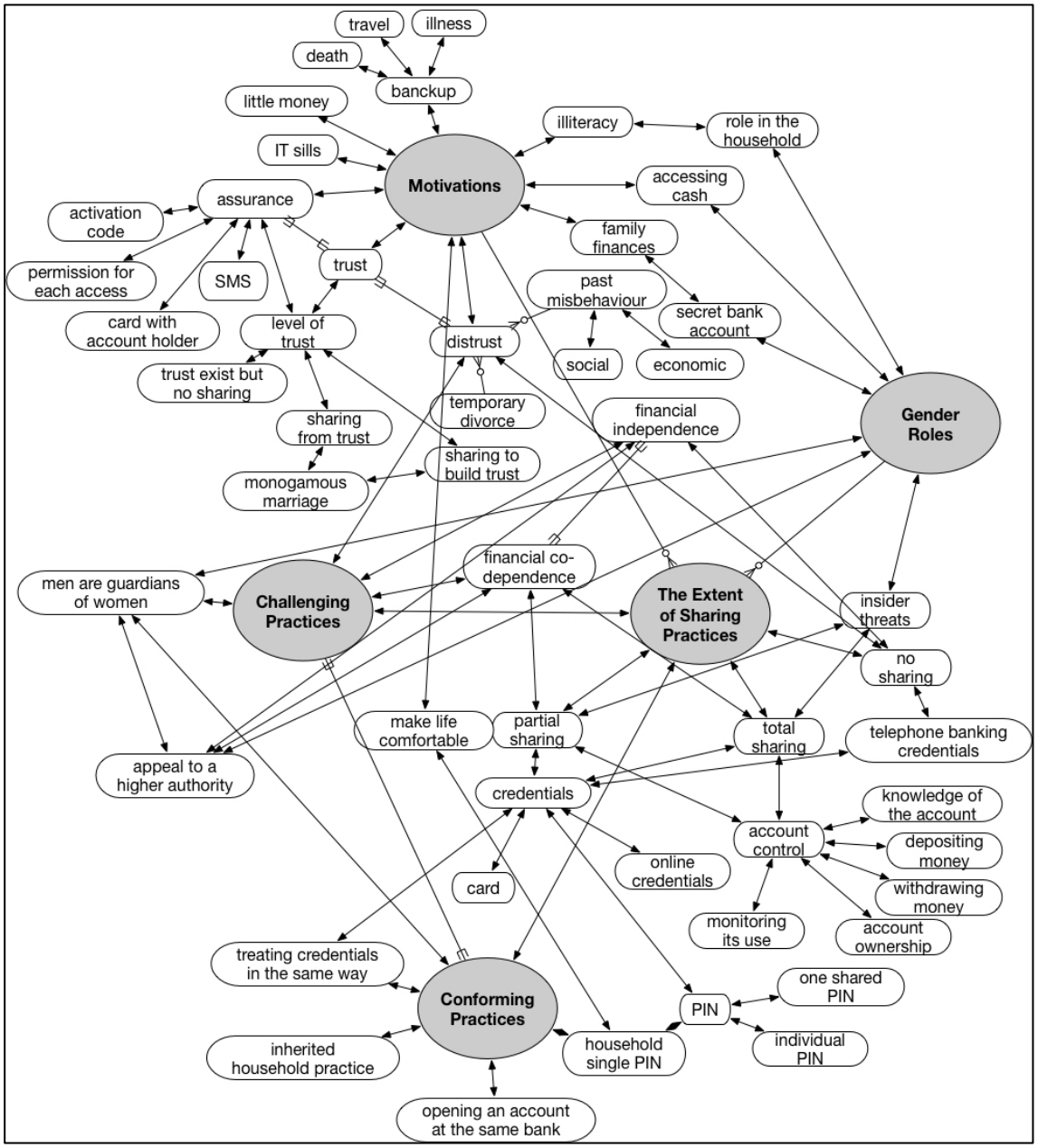
If you remain unhappy and wish to make a formal complaint, please contact the Research Ethics Committee at the University of Oxford at ethics@socsci.ox.ac.uk; +44 (0)1865 614871; Social Sciences & Humanities Inter-Divisional

APPENDIX 8: SAMPLE OF DATA CODING

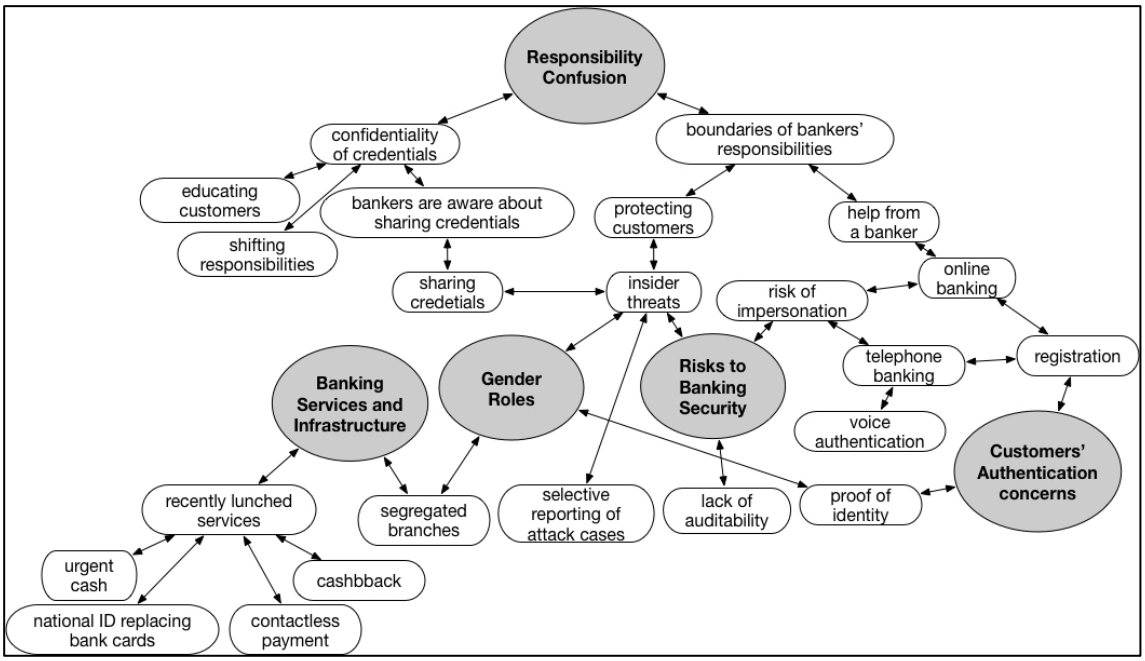
The following screenshot presents part of the coding process, codes and memos using ATLAS.ti.



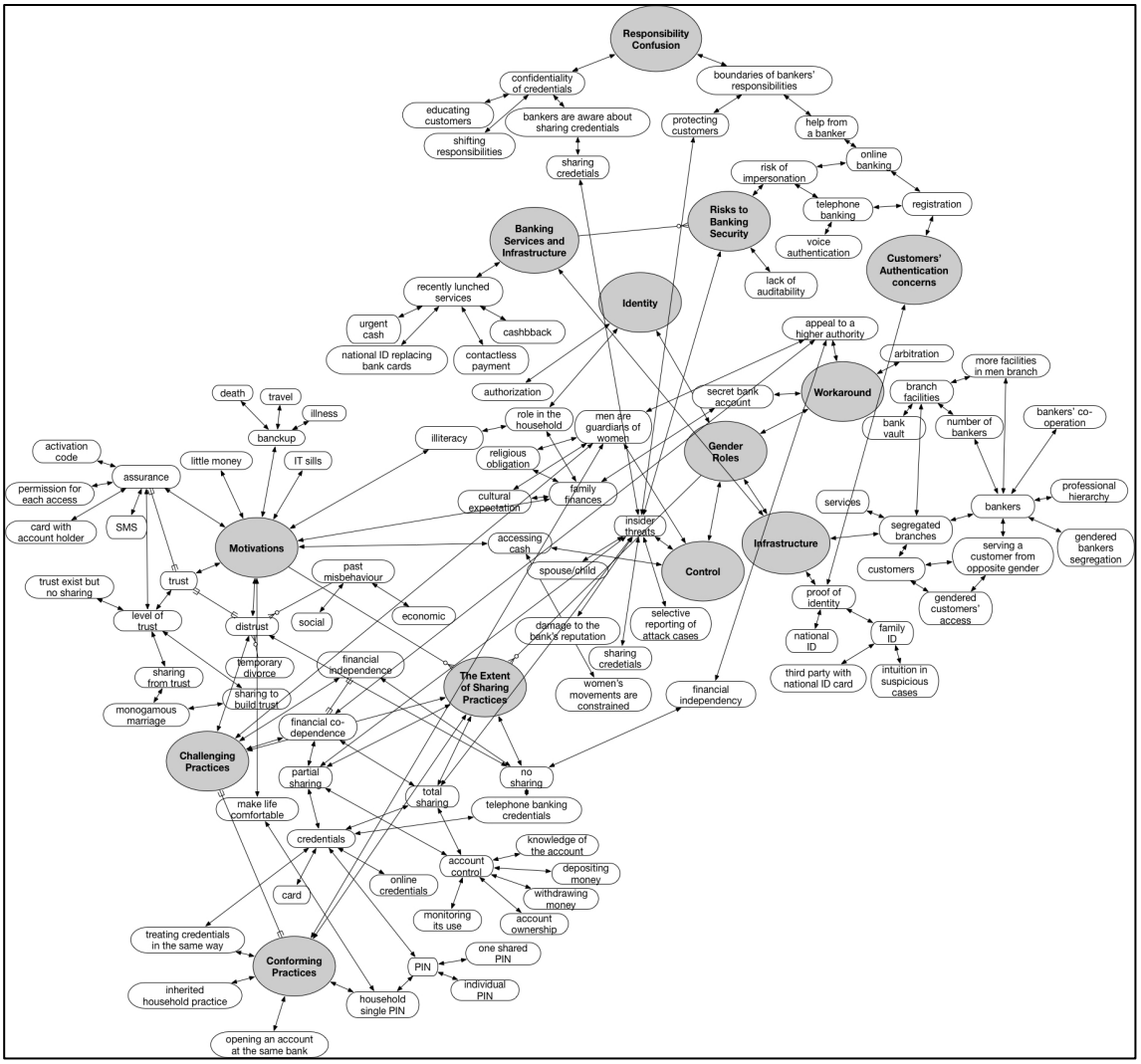
APPENDIX 9: MODEL OF HOUSEHOLD CUSTOMERS' PERSPECTIVE



APPENDIX 10: MODEL OF BANKING PERSPECTIVE



APPENDIX 11: HOUSEHOLD CONTEXT OF USE OF BANK SYSTEM



APPENDIX 12: CODES AND MEMOS

Codes

Overall 108 codes generated from analysing the data. In the table below groundedness (Grd) is a code quality shows how many the code repeated in the analysis. In other words it shows how many quotations linked to this code.

Code	Description	Grd	Sample quotation
accessing cash	Because of the driving law in KSA prevent women from driving; adopting sharing practice among females is common to access cash from their accounts.	17	P18: getting cash from my account is the reason for me to share my card and PIN with my husband and my brothers when I can't get out.
account control	The different forms of sharing control over an account	4	P3: I always deposit money for my mother to her account.
account ownership	A form of controlling an account is by sharing its ownership.	2	P1: I and my wife have a joint account. The idea was to save some money for our daughter.
activation code	One of the ways to assure not misusing the shared credentials and monitor the account.	6	P14: I will receive the activation code on my mobile for every access to online account.
appeal to a higher authority	Mostly women would use this option to stop insider threats.	2	See case 1 in Appendix 13 in Appendices.
arbitration	Arbitration is found to gendered because it seems successful for men but not women.	2	See case 5 in Appendix 13 in Appendices.
assurance	This subcategory presents the using of four ways to protect and monitor the account while adopting sharing practice.	18	P3: There is the SMSs which confirm for me every single time how much money has been taken from my account and when, that made my husband more responsible.
authorization	Gender of customers was found to influence the authorization process.	5	P37: I visited the bank branch to renew the card of my mother's account without the need for her to come with me.
Backup	This reason is given by participants for sharing practice.	20	P29: Sometimes we have to share credentials so if someone is sick, tired or old.
bank vault	This subcategory is discussing the issues of bank vault in the segregated branches.	8	P69: The bank vault is always in men branch.
bankers	This subcategory is related to bankers' issues in the segregated branches.	16	P57: To serve my uncle, he went to the men branch next door, and a male banker helped him filling the form then I preceded the application in the bank system in the womn branch.
bankers are aware about sharing credentials	This subcategory is about bankers being aware of sharing credentials among household members.	5	P56: Yes, I do see customers sharing their credentials with their family members and this happens too much.
bankers' co-operation	This subcategory discussing the co-operation between bankers.	3	P57: To serve my uncle, he went to the men branch next door, and a male banker helped him filling the form then I proceeded the application in the bank system in the womn branch.
Boundaries of bankers' responsibilities	This subcategory is about defining the responsibilities boundaries of bankers	20	P52: No, I don't warn customers about SAMA policy regarding sharing credentials, the customer will read them in the form anyway.
branch facilities	This subcategory is comparing branch facilities in the segregated branches.	16	P65: men branch would have more facilities, such as safe boxes. Only big women branchs will have this facility.
card	Card is one form of credentials.	21	P18: getting cash from my account is the reason for me to share my card and PIN with my husband and my brothers when I can't get out.

Code	Description	Grd	Sample quotation
card with account holder	One of the ways to assure not misusing the shared credentials and monitor the account.	12	P4: I am sharing with my brother becasue he can't reach the card. It is with all the time.
cashback	This subcategory is related to the service of cashback that is one of the services released recently.	8	P58: cashback has lunch last year I think.
Confidentiality of credentials	This subcategory is about the responsibility for keeping credentials secure	62	P52: No, I don't warn customers about SAMA policy regarding sharing credentials, the customer will read them in the form anyway.
contactless payment	This subcategory is related to the releasing of the service of contactless payment and the issues around this service.	11	P57: No I never heared of this service.
Credentials	The different forms of account's credentials that shared between household members.	11	P18: getting cash from my account is the reason for me to share my card and PIN with my husband and my brothers when I can't get out.
cultural expectation	This expectation is one of the reasons for men guardianship.	12	P23: I have the right of expenses so it is my right to get my expenses from my husbnad. That what Shareaa said and that is our customs.
customers	This subcategory is related to customers' issues in the segregated branches.	13	P64: the bank prohibited women access to men branch.
damage to the bank's reputation	This subcategory is related to the impact of insider threat cases by damaging the bank's reputation.	3	P55: threats would it is not good to bank's reputation,, the customer would not trust the bank security by witnessing such cases.
death	The account holder death is identified as one of the reasons to share credentials as backup.	17	P29: Sometimes we have to share credentials so if someone is sick, tired or old.
depositing money	A form of controlling an account is by depositing money in the account.	2	P3: I always deposit money for my mother to her account.
Diary_period	Here are the anawers from the participants regarding the diary period of one month.	15	P34: I didn't find it too long. It was fine. It was neither long nor short.
Diary_way	Here are the anawers from the participants regarding the way used to record the diary.	18	P37: I keept a pen and paper in a drawer near my bed and every night I record all my banking transactions once before sleep.
Diary_WhatsApp	Here are the anawers from the participants regarding using WhatsApp by the researcher to remined the participants.	9	P41: It was useful contacting and sending me messages via WhatsApp to remained me about writing the diary that was really good idea.
distrust	Two reasons for distrust identified which cause of adopting not sharing practice between household members.	46	P4: I used to trust my husband but now I am not trusting him because of temporary divorce,,, I become afraid.
economic	Past misbehaviour can be economically.	7	P11: I don't share with my sister as she is the kind of person who misuses money.
educating customer	This subcategory related procedures taken by bankers to educate customers regarding SAMA policies.	39	P52: No, I don't warn customers about SAMA policy regarding sharing credentials, the customer will read them in the form anyway.

Code	Description	Grd	Sample quotation
Family finances	By religion and culture, men are responsible for family finances. This motivated most men to adopt a pattern of practice of having two accounts one of them is secret.	52	P23: I have the right of expenses so it is my right to get my expenses from my husbnad. That what Shareaa said and that is our customs.
family ID	This subcategory is related the using of family ID as proof of identity for household customers.	14	P63: if a female customer does not have a national ID then she can use family ID and someone else with national ID must accompined herto confirm her claim.
Financial co-dependen	This is demonstrated when people rely on each other.	51	P5: I use my father's and my mother 'saccount to withdraw cash for them to serve them and to make life comfortable.
Financial independence	This subcategory related to when a customer seeks a high degree of control over his/her own finances.	68	P16: bank credentials are supposed to be confidential and not share them with anyone.
gendered bankers segragation	This subcategory is related to the segregation among bankers based on gender.	14	P54: the difference between men and women branches is that only male can work in men branches and only women can work in womn branches.
gendered customers' access	This subcategory is discussing the difference in customers' access to the segregated branches.	9	P64: the bank prohibited women access to men branch.
help from a banker	This subcategory related to the help from bankers into registering customers in online banking	4	P59: No I would not register the customer in online banking and instead I will give her a leaflet to follow the instructions of registeration.
Household single PIN	A single PIN would be a signed for all the accounts belonged to household members.	3	P33: My son assigned the same PIN for my card, his cards, and his wife card.
Illiteracy	Illiteracy found to be one of the reasons for mothers to share credentials with their children.	10	P3: I know all my mother's passwords, for she doesn't know how to use the ATM machine.
illness	The account holder illness is identified as one of the reasons to share credentials as backup.	5	P29: Sometimes we have to share credentials so if someone is sick, tired or old.
individual PIN	This describing when the PIN is unique to one account and not used for other accounts.	21	P30: The PIN for my card is different than the one for my wife card.
Inherit household practices	The new bank customers in a household would follow the banking practice for old bank customers in the household.	9	P3: I used to see my father and his wife exchanging their passwords... and there was no problem. So I am doing the same thing.
Insider threats	This risk arises because customers share credentials with family members.	41	See cases 2 and 3 in Appendix 13 in Appendices.
intuition in suspicious cases	Bankers referred to the intuition in suspicious cases as a way to suspect an insider threat case.	4	P64: He said she is his wife but I noticed from her appearance and age that she can't be his wife because she seems older than the age in the family ID card.
IT skills	This reason motivates sharing of online banking credentials among family members.	6	P5: I access my wife online banking account because she is not that experienced in technical things.

Code	Description	Grd	Sample quotation
knowledge of the account	A form of controlling an account is by knowing its existence.	8	P22: Some men have two accounts one is known and used by his family and another account which is secret.
Lack of auditability	Sharing credentials makes it difficult to identify a customer uniquely.	2	P49: one of the risks is that we don't know who did what.
level of Trust	This subcategory discusses the trust level.	67	P25: It is ok if they have mutual trust.
Little money	This reason is given by participants for sharing practice.	7	P2: in addition to trust, I share my card and its PIN with my husband because the amount of money in my account is not that much.
Make life comfortable	This reason is given by participants for sharing practice.	55	P5: I use my father's and my mother 'saccount to withdraw cash for them to serve them and to make life comfortable.
men are guardians of women	This subcategory is related to the guardianship of men over women and the issues around this subject.	13	P28: in our society we look to women as helpless and that I have to control my sister.
monitoring its use	A form of controlling an account is by monitoring its use.	13	P12: The father might be afraid becaseu his daghuter is extravagant and he needs to monitor her account.
more facilities in men branch	This subcategory is related to the more facilities in men branches.	12	P65: men branch would have more facilities, such as safe boxes. Only big women branchs will have this facility.
most used technology		68	P20: I rather the selling points it is easier than the ATM machine… I am that kind of persons who don't like to let cash with so I prefer to use the selling points.
national ID	This subcategory is related the using of national ID as proof of identity for household customers.	8	P63: a customer would use her/his national ID to proof identity.
national ID replacing bank cards	This subcategory is related to the idea of using National ID as a replacement of bank cards.	2	P59: I heared about this service from newspapers but I am not sure when it will lunched by banks.
No sharing	Not sharing account control or its credentials.	72	P16: bank credentials are supposed to be confidential and not share them with anyone.
number of bankers	This subcategory is related to the number of bankers in the segregated branches.	8	P63: men branches would be bigger and having more bankers than men branches as men braches would servie more customers.
one shared PIN	This describing the case of a single PIN shared between the husband and his wife in the household.	1	P3: The PIN for my card and my husband's card is the same.
online banking	This subcategory is related to online banking service.	69	P2: I use online banking but I don't share its credetnials with my husband.
online credentials	Online credentials are one form of credentials.	4	P2: I use online banking but I don't share its credetnials with my husband.
online shopping	This code is related to the use of online shopping	3	P21: in the online shopping we fear not to know the source, if something is withdrew or anything went wrong, you don't know where to go to fix the mistake.

Code	Description	Grd	Sample quotation
Opening an account at the same bank	New bank customers in a household would open their accounts in the same bank as old bank customers in the household.	10	P35: I opened my account in the same bank as my family members.
Partial sharing	The partial sharing for either credentials or account control or both of them.	49	P18: getting cash from my account is the reason for me to share my card and PIN with my husband and my brothers when I can't get out.
past misbehaviour	One of the reasons of distrust.	12	P27: If the father has previous history in exploiting family's individual money then his daughter can refuse sharing her credetnials with him.
permission for each access	One of the ways to assure not misusing the shared credentials and monitor the account.	57	P3: My husband never uses my card without my permission.
PIN	PIN is one form of credentials.	21	P18: getting cash from my account is the reason for me to share my card and PIN with my husband and my brothers when I can't get out.
professional hiraricy	This subcategory discussing the bankers' hierarchy.	12	P66: There is no difference between man and women bankers in the same position,, all of them have similar authorities.
proof of identity	This subcategory is related to the different proof of identity used by household customers.	18	P63: a customer would use her/his national ID to proof identity.
protecting customers	This subcategory is related to procedures to protect customers from insider threats.	16	P62: For me, I can't do anything for the customer to protect her/him. How can I interfere?
recently lunched services	New services recently launched by banks in the KSA	29	P58: cashback has lunch last year I think.
Registeration	Registering customers for online and telephone banking	7	P59: No I would not register the customer in online banking and instead I will give her a leaflet to follow the instructions of registeration.
religious obligation	This obligation is one of the reasons for men guardianship	2	P23: I have the right of expenses so it is my right to get my expenses from my husbnad. That what Shareaa said and that is our customs.
risk of impersonation	This risk applies to online and telephone banking.	7	See cases 10 and 14 in Appendix 13 in Appendices.
role in the household	This subcategory related to the different influence of role in the household.	83	P19: the father consider the son a responsible that will open a house and have a family, he is even responsible of his sisters.
secret bank account	This banking practice would normally be adopted by men and difficult to be adapted by women.	8	P22: Some men have two accounts one is known and used by his family and another account which is secret.
segregated branches	Similarities and differences between men and women branches	42	P70: both men branch and women branch are offering the same services to customers.
Selective reporting of attack cases	The reporting of insider attack cases would be in the case only	10	P60: I don't report this because the branch manager has too many things other than a

Code	Description	Grd	Sample quotation
	if the attacker is unknown to the customer and not a member to the household.		customer who shares his card with his wife.
services	This subcategory is discussed the services provided by men and women branches.	5	P70: both men branch and women branch are offering the same services to customers.
Serving a customer from opposite gender	This subcategory is related to serving a customer form opposite gender in the segregated branches.	21	P57: To serve my uncle, he went to the men branch next door, and a male banker helped him filling the form then I preceded the application in the bank system in the womn branch.
sharing credentials	Sharing credentials has been identified by bankers as the reason for insider threats cases.	5	P56: Yes, I do see customers sharing their credentials with their family members and this happens too much.
sharing from trust	One of trust levels is when sharing credentials occur based on existed trust.	61	P25: It is ok if they have mutual trust.
sharing to build trust	One of trust levels is when sharing credentials occur to build trust.	6	P31: I want them to trust me, especially because I am not their mother. I am their stepmother… I did not force any of them to call me Mum, but they did so by themselves. They didn't call me Mum until they trusted me.
shifting responsiblilities	This subcategory is related to banker's practice to shift responsibility of keeping credentials secure to customers only.	11	P61: I don't do anything; this is the customer's responsibility to protect her credentials
sms	One of the ways to assure not misusing the shared credentials and monitor the account.	23	P3: There is the SMSs which confirm for me every single time how much money has been taken from my account and when, that made my husband more responsible.
social	Past misbehaviour can be socially.	8	P9: A daughter might refuse to share her credentials with her father if she used to see him treating her mother and family members badly.
spouse/child	Comprising all cases of insider threats reported where the insider is a husband or a child who normally would be a son.	4	P67: In most insider attack cases I witnessed the insider is either the husband or the son.
telephone banking	This subcategory is related the telephone banking service.	29	P15: I prefer to use telephone banking because for me it's easier than online banking.
telephone banking credentials	Telephone banking credentials is one form of credentials.	23	P17: I use telepnone banking but I don't share its credentials with my family as my card and it's PIN.
tempporary divorce	One of the reasons of distrust.	2	P4: I used to trust my husband but now I am not trusting him because of temporary divorce,,, I become afraid.
third party with national ID card	This subcategory is related the using of family ID as proof of identity for household customers supported by third party.	14	P63: if a female customer does not have a national ID then she can use family ID and someone else with national ID must accompined herto confirm her claim.
Total sharing	The total sharing for either credentials or account control or both of them.	2	P1: I and my wife have a joint account. The idea was to save some money for our daughter.
travel	The account holder travel is	5	P29: Sometimes we have to share credentials

Code	Description	Grd	Sample quotation
	identified as one of the reasons to share credentials as backup.		so if someone is sick, tired or old.
Treating credetnials in the same way	New bank customers in a household would treat their credentials in the same way as old bank customers in the household by either share it or keep it private.	4	P43: I do trust my family but I prefer to keep my credetnials secure,, and that what I teach my children to do as well.
Trust	One of the main motivations for adopting sharing practice between family members is trust.	62	P25: It is ok if they have mutual trust.
trust exist but no sharing	One of trust levels is when trust is exist but without sharing credentials.	2	P43: I do trust my family but I prefer to keep my credetnials secure,, and that what I teach my children to do as well.
urgent cash	This subcategory is related to the service of urgent cash that is one of the services released recently.	9	P51: urgent cash is usefull to access cash in cases of losing or forgetting cards.
voice authentication	Voice authentication is a mitigation to risk of impersonation in telephone banking.	29	P53: in telephone banking, customer's voice must match the gender of the account holder.
withdrawing money	A form of controlling an account is by withdrawing money from the account.	26	P5: I use my father's and my mother 'saccount to withdraw cash for them to serve them and to make life comfortable.
Women's movments are constrained	Mobility of Saudi women is restricted as they cannot drive or walk.	42	P18: getting cash from my account is the reason for me to share my card and PIN with my husband and my brothers when I can't get out.

Memos

Presented here are the details of the memos generated during the analysis. Memos serve as a means of documenting the thoughts of the researcher throughout the analysis, and thereby serve as a means of documenting reflexivity.

Memo 1:

Two accounts for a man:
Two accounts for the head of the household if he is a man:
one known by his family members and they can use its card for family expenditure. The other account is unknown for anyone even his wife.
If the head of the household is women as in the case of widows:
She would be the head of the household if her eldest son is still young only, if the son is old enough then he would be the head of the household.
The son can be his father's successor if the father is old and/or sick.

Memo 2:

SMS

Most of the participants rely on SMS from the bank notifying them about any operation done. However, it happened before in the mother-son story Case 12 [The son changed the saved mobile number to his mobile number]. So this way is reliable some extent but it needs some improvement such as:
Sending SMS at the beginning of each month to confirm the saved number.
or
Send SMS to the old number notifying that the saved number has been changed to a new number.

Memo 3:

Online banking vs. telephone banking
The using of online banking is rare between females, however, the using of telephone banking is more than the using of online banking although both online banking and telephone banking share the advantage that a female can have access to her account without the need to use a car.
The activation for both services does not require physical verification of the account holder which open these services to risk of impersonation.

Memo 4:

Insider attack
Why banks do not keep record for insider attack cases? Is it because not to be liable in front of legal agency such as SAMA?
When banker faced a case such as Case 14, the banker responded immediately by calling police. Meanwhile in other cases of insider attacks bankers do not get involve or even if they want to, there is no clear procedure for them to follow.
After analysing SAMA banking policies and regulations, no policy found regarding this subject although of the widespread adaption of sharing practice among household customers.

Memo 5:

Online banking
Why bankers do not activate online baking for new customers immediate after opening the new account for them? such service would save a lot of money to the bank
In Daughters focus group none is using online banking (all 6 participants). They even don't know what is it or how to do it. In Mothers focus group, only one from 6 participants knows and use online banking. The using of online banking is rare between females although online banking can offer good services and the female can use her bank account anytime/anywhere she want without the need to use a car which can be a good solution to solve the problem of movement limitation for females in KSA. The participants said the bank employees did not cooperate with them to teach them how to use it.

Memo 6:

Insider attack 2
How it occurs?

P48 argued that insider attacks occur because customers share account information with their family member to make their lives easier. They do not expect an insider attack to happen to them, even when they know that it has happened to others.

To support this assumption, we examine the case of P3. She mentioned that she had only one bank account and that her husband had three accounts at different banks. Because they had four cards for each account – and to make their lives easier and to remember the PIN for each account's card – they decided to use the same PIN for all four cards. However, P3 was not the only user of her card. She mentioned that three of her brothers also used her card to withdraw money for her. Therefore, her brothers also knew the PIN for her husband's cards, because it was the same PIN as for her cards. She made her husband's accounts vulnerable and when the researcher pointed this out during the interview, it became clear that she had not thought about this. She replied, *"My brothers will never know that we are using the same PIN for all of my and my husband's cards . . . this idea will never come to their minds!"*

Memo 7:

Man guardianship over women

Is there any difference between religion and culture definition of guardianship?

what is the limit, or is it unlimited?

A debate on Twitter to differentiate between a protective guardianship and controlling guardianship on 8 September 2016 Sheikh Dr. Abdullah Almanee supported this distinction in Okaz, a major Saudi newspaper, claiming that Islam maintained full freedom for women and that the notion of guardianship applied only in marriage. However many Saudis appear not to accept the validity of Almanee conclusions.

Memo 8:

Sensitive topic

The sensitivity of the topic because it is about financial and banking matters and because it discuss the household practice.

Although of all the effort from the researcher to build rapport with participants in different ways, some participants mentioned that because of the sensitivity of the topic people especially victims of insider attacks would not prefer to admit and discuss this with the researcher.

Participant P34 confirmed this point.

Memo 9:

Boys are different from girls

Participants invoke the different between boys and girls as it is culturally more than religion. The two concepts of culture and religion are intertwined in the Saudi cultural norms where it become difficult to differentiate between them.

Memo 10:

Authorisation

Gender was found to play a role in customer authorisation. This can be seen different response by bankers in case of P37 and case of P39.

However, one implication of the case of P37 that it shows the bank colluding in some cases in the 'illegal' sharing practices of household customers, however, the data is insufficient to know what is the consequences of this colluding and if the bank would be liable and share the responsibility with the customer or as stated before in Section 5.3.1.2 the responsibility will be shifted completely to the customers.

Memo 11:

Auditability

Although auditability, accountability, and non-repudiation of banking activity are seriously compromised by the widespread practice of household customers sharing credentials with family members, only one banker mentioned it.

If the practice of sharing credentials among household customers is know by bankers, why bank do not take serious steps to stop it or at least to minimize it?

Why bank turn a blind eye to this practice and its consequences.

APPENDIX 13: INSIDER ATTACK CASES

Cases Reported by Household Customers:

Case 1:

A participant in the daughters' focus group recounted that her friend had shared control of her account with her widowed mother in order to protect her (paternal) inheritance from her husband. The husband had repeatedly tried to convince his wife to give him part of her inheritance so that he could use it to expand his business. To avoid direct conflict with him and to protect her money, the wife made her mother a joint account holder. The husband now recognised that his mother-in-law was supervising her daughter's account and monitoring every transaction, which stopped him from attempting to persuade his wife. The daughter thus challenged her husband as head of the household and to keep her financial independence from him she appealed to her mother.

Case 2:

A female customer, P3, reported that her husband had twice misused her credentials, despite that she still shared her card PIN with him. When asked why, she replied that the misuse had happened four years ago and she did not think it would happen again.

Case 3:

A female customer in the daughters' focus group, P10, reported the case of her sister who had assigned her husband as a joint account holder; he misused his authority by taking out a loan of half a million SAR (£102,900), which the wife now had to repay.

Case 4:

P45 stated that her sister was illiterate and counted on her son to withdraw money; he withdrew more than his mother had asked for and kept the excess. The mother had kept her card with her at all times to protect and monitor her account, but this seems not to have been effective in this case.

Case 5:

A case mentioned by P45 involved an illiterate father-in-law who shared his credentials with his son-in-law, whom he later found to be misusing his credentials by withdrawing money without permission. The victim asked his daughter to support him by divorcing her husband (the misuser); when she refused, her father disowned her. He then sought help from his tribe and family, was successful in recovering his money, then stopped sharing his credentials with anyone.

Case 6:

This case was recounted by P34, who was asked by one of his female relatives to help her retrieve her bank card from her husband. The husband had kept his

wife's card with him at all times and used her account without her permission. She was unwilling to confront her husband directly because she was afraid that he would divorce her,[8] so she sought the help of her tribe and her family while keeping this appeal secret from her husband.

When my cousin asked me to talk with her husband about this matter, she asked me not to reveal that I knew about what he was doing… because she thought this would make the situation worse by revealing a secret of their house… Instead, she asked me to approach him indirectly by saying that this practice by a husband is forbidden in Islam and would be a mistake. But this did not work, and he is still using her salary as if it was his own money… My poor cousin … she could not even ask for money for herself from her account, but to get some money from him now and then, she says that she needs money for charity purposes and of course she uses the money for herself. [P34, M]

Case 7:

P41 the mother in household 4 had a husband who kept her card and used the account without permission for a long time and without any objection from her. However, after discussing this situation with female colleagues and under social pressure from them, the wife sought to change this situation and to keep the card with her. After a long and heated discussion with her husband, the wife managed to retrieve her card and keep it with her at all times, but still shared her credentials with her husband.

Cases Reported by Bankers:

Case 8:

A female banker gave this example:

A customer came to the bank to apply for a loan of 50.000 SAR (£9150). After filling the application and while we waiting for the final approval she told me that she was forced by her husband to take the loan. He was waiting for her at the door of the women's branch and she was obliged to give him the money. In this case, I couldn't do anything to help her. I could only advise her. I didn't know what to say to her. Should I say "These are personal problems, it's not my business", or should I call the police? Or advise the customer to call her brothers to protect her? All the other employees said this was not my business. Don't get involved, because the customer might say that the banker has told her to do so and so, and I would get into trouble. I was unable to do anything, but I advised her to call one of her brothers. When the loan application approved and the customer received the money she decided to call her brother and asked him to come and protect her, then she filled an envelope with brochures to make it look like it was filled with money and sealed it. The customer had a physical disability and she couldn't walk properly, but she went out, gave her husband the fake envelope, then ran barely to her brother's car with the money. [P51,F]

---

[8] Culturally, Saudi society accepts a divorced man more than a divorced woman. A man can usually divorce his wife without bringing shame on his family, but the converse is not generally true.

Case 9:

A male banker mentioned that a man came to the branch with his three daughters to open accounts for each of them so that they could receive the monthly allowance from the government. From the banker long experience of over 20 years working in banking sector and from the way of the father treating his daughters, the banker believes that the father intended to keep the bankcards in order to divert the money for his own use but the banker could do nothing to help the daughters.

Case 10:

A female banker, P67, reported a case of two sisters: S1 and S2. S1 came to the branch to open a new account for herself, saying that she was expecting a money transfer from her sister, S2. After a few days, she received the transfer from S2's account. Some time later, S2 came to the bank claiming that she had lost 26,300 SAR (£5,400) from her account. The detailed record of her account revealed that the money had been transferred to S1's account online. S2 was sure that she had not done this, because she had not registered for online banking. Since S1 and S2 shared bank credentials, as do most household customers, S1 had all the information she required to register her sister without her knowledge, then use online banking to transfer the money. Upon further investigation, it was discovered that S1 had registered for S2's online banking with her own mobile number and misused this access to transfer the money. However, because S1 did not later change the mobile number, S2 and the banker were able to discover what had happened.

Case 11:

In another example, P58 a female banker described the case of a widowed mother who suffered from repeated insider threats from her son. He repeatedly took his mother's card without permission and withdrew the retirement salary of his deceased father. Because this money was the household's only income and the mother could not stop her son, the banker advised the mother to cancel the card and withdraw the money by visiting the branch. Although this solution stopped the son, it caused another problem for the mother, who had to travel to the bank to withdraw the money.

Case 12:

A case was recounted by a female banker, P50:

A customer came to us two days ago. She was very angry and said that she would sue the bank because it had stolen money from her account … A detailed record of her account showed that money had been withdrawn from her account using her card in an ATM in Cairo. The customer became angry and said that she had not visited Egypt in two years …When the bank's representative suggested that her card might have been used by someone else "… your husband or your son… Has anyone from your family recently been to Egypt?", it was very clear that she had not thought about that possibility. Then, by comparing the date of the transactions that occurred in Egypt, she found that it was in the same period that her son was in Egypt with his friends … She admitted that she kept her card in her bedroom drawer with a piece of paper containing the PIN, online username and password. … She and the banker

became more sure that her son was the one who used her card when they checked the electronic services for her account. They found that he had changed his mother's mobile number to his, by using the information that he had found with the card. Once the mobile number had been changed, his mother would not receive SMSs for every transaction, so he could guarantee that she would not know what he had done.

Case 13:

A female banker, P61, recounts the anecdote of a female customer who came to a branch to open a new account, saying that she was going to start studying at university and needed this account to receive the monthly allowance from the university. She did not have a national ID card and instead provided the family card, with her father supporting her claim by showing his ID in the men's branch. The banker noticed that the customer was claiming to be 18 years old, although from her face she appeared at least 40. After the customer left the branch the banker reviewed the papers and found that the customer was claiming to be her own younger sister, who was registered on the family card and was aged 18.

Case 14:

A case recounted by a female banker, P55:

This case happened to my friend … a customer service officer in bank [X]. … A female customer came to the women's branch to apply for a loan, claiming that her name was Sara and that she held an account at the bank. Sara did not have a national ID card, so she used the family card and her husband [Ahmad] was in the men's branch to support her claim. The banker did not suspect anything and Sara signed all the appropriate forms. The banker then told her that it would take two working days to process her loan application. Two days later, another woman came to the branch claiming to be Sara and asking about an SMS from the bank saying that the loan requested had been granted and inviting her to visit the branch, which surprised her because she had not applied for a loan. While the banker was discussing this problem with the second customer, the first woman came into the branch. Both claimed to be Sara, so the banker closed the main door of the bank branch to prevent either of them leaving and called the police. It turned out that both women were married to Ahmad, who was planning to steal money from his wife Sara with help from his other wife.

Case 15:

A female banker, P48, said:

An interesting case happened long time ago, a customer let's called him Adil married two women: Nora and Nada. He opened only one personal account for both of them to use. The account was not a joint account so the bank did not know that two customers were using it. Both Nora and Nada had been using very similar signatures for the account. One day, Nada went to the bank to withdraw money, but she found that there was no money in the account. After a discussion, the banker discovered that there were two different women using the same account, and that the last transaction showed that one of them came and withdrew all the money from the account. The difference between the two women's signatures was very small and was not noticed by any of the bank's employees, so the bank hired an expert in signatures to prove this.

Case 16:

A female banker, P51, said:

A customer came and complained that in the 26th of every month (25th is the day of salary payment for most of the employees in KSA), a 1000 SAR (£210) is withdrawn from her account by using ATM. After discussing this with the

customer and the bank statement for her account, the customer suspected that her husband takes her card from her wallet while she is sleeping and withdraws the sum, she doesn't know what he does with this money, but the customer disappeared after that, and she never came to the branch again.

Case 17*:*

A female banker, P67, said:

A customer came to the branch to withdraw a check. The check is issued by charity agency to help widows and divorced women. The customer provided her national ID but the bank cashier noticed that date of birth in the ID is for a woman over 70 and the customer who provided the check is young and around 25 years but in the same time the photo in the ID is similar to the customer. After investigating this and asking the customer it turns out that the check and the ID is for the customer's mother who is old and cannot come the branch every time to withdraw the check. Interestingly, both the customer and her mother are almost identical and the customer used to withdraw checks for her mother every 6moths by using the mother's national ID and the previous branch manager allowed her to do so.

Case 18:

A male banker, P69, said:

A female customer came to women branch and her brother came to men branch, the customer used family ID and her brother used his national ID to support her claim. The customer failed to sign the same signature she tried to make similar signature but not the same and it turns out that she is not the account holder but her sister. When female bankers discussed this with the customer, she confessed saying that this is her sister's account.

Case 19:

A male banker, P64, mentioned a case of a male customer complained of missing 15,000 SAR (£3200) from his account. The customer said that he had not lost his card and had not shared it with anyone. An investigation revealed that the money had been withdrawn from the account using the card at three different ATMs. The authorities checked the CCTV connected to the ATM and it was found that the customer's son had withdrawn the money using his father's card without his permission, having taken the card while his father was sleeping. The father said, *"I am an old man … every time I accompanied my son to withdraw cash for me from my account. Every time this happens in my presence"*. When the customer found that it was his son who had taken his money, he withdrew his complaint. P64 said that he did not know what happened after this. He also stated that the bank was not responsible for what had happened and that it was the customer's fault for having shared his credentials with his son. Moreover, because the father had shared his credentials, it had not been possible to determine whether he or his son had withdrawn the sums in question until the investigation was extended to checking the CCTV footage.

Case 20:

A male banker, P60, mentioned a case of a male customer came to men branch trying to open a new bank account for his wife. The customer was unaccompanied by his wife so the banker refuses to open the account without the wife, however, the customer insisted as the wife guardian to open the account to his wife. When the banker refused to do so, the customer left the branch for a while then he came with a female claiming to be his wife and provide the family card as proof of identity to the wife. The banker noticed from the wife appearance, her hands, age, and handwriting that she is not cannot be his wife

because her age is evident on the family card so the banker suspected in the case and refused to open the account.

Case 21:

A male banker, P56, a wife was about to open a bank account to receive the monthly stipend from the government but she found that there is already a bank account registered with her name and information. When she discussed this in the bank branch with a banker it turned out that she did not open that account and because there is a problem with her husband she think that he opened that account with help of any female relative to him. So the wife closed the account and reopened a new account for her.

Case 22:

A male banker, P56, mentioned a case of a customer who shared his card and PIN with his wife. One day the wife took the card secretly and by using ATM she transferred a huge amount of money 250,000 SAR (£52,600) to her account. The banker said the bank is not responsible for what happened and it is the customer fault to share this information with his wife.

10 REFERENCES

Abdulmuhmin, A. and I. A. Alzamel (2001). "Retailers' experiences with and attitudes toward the Saudi Arabian EFTPoS system." International Journal of Retail & Distribution Management **29**(4): 188-199.

Abdulmuhmin, A. G. (1998). "Demographic differences in usage and attitudes toward the saudi arabian EFTPoS system." International Journal of Bank Marketing **16**(3): 117-128.

Abdulmuhmin, A. G. and O. Al-Abdali (2004). Adoption of Online Purchase by Consumers in Saudi Arabia: An Exploratory Study. Second Conference on Administrative Sciences (King Fahd University of Petroleum & Minerals, Dhahran, Saudi Arabia.

Abdulmuhmin, A. G. and Y. Umar (2007). "Credit card ownership and usage behaviour in Saudi Arabia: The impact of demographics and attitudes toward debt." Journal of Financial Services Marketing **12**(3): 219 – 234.

Adams, A. and M. A. Sasse (1999). "Users are not the enemy." Communication. ACM **42**(12): 40-46.

Adeoti, J. (2011). "Automated Teller Machine (ATM) Frauds in Nigeria: The Way Out." Journal of Soc Sci **27**(1): 53-58.

Agre, P. (1998). Introduction. Technology and Privacy: The New Landscape. P. Agre and M. Rotenberg. Cambridge, Mass, The MIT Press**:** 1-28.

Ahmed, S., S. Jackson, N. Ahmed, H. Ferdous, M. Rifat, A. Rizvi, S. Ahmed and R. Mansur (2014, April). Protibadi: a platform for fighting sexual harassment in urban Bangladesh. 32nd annual ACM conference on Human factors in computing systems, ACM.

Al Dabis, F. (2016). No Women's Guardianship in Islam Except in Marriage. Okaz. KSA. **5562**.

Al Rajhi Bank. (2014). "About Us." 22/2/2015, from http://www.alrajhibank.com.sa/en/about-us/pages/default.aspx.

Al-Garni, M. (2000). The Impact of Family Structure and Family Function Factors on the Deviant Behaviors of High School Students in Makkah City, Saudi Arabia. PhD, The Ohio State Univesity.

Al-Hamar, M., R. Dawson and L. Guan (2010). A culture of trust threatens security and privacy in Qatar. IEEE 10th International Conference on Computer and Information Technology (CIT), IEEE.

Al-Husein, M. and M. Sadi (2015). "Preference on the Perception of Mobile Banking: A Saudi Arabian Perspective." European Online Journal of Natural and Social Sciences **4**(1): 161-172.

Al-Jabri, I. M. and S. M. S. (2012). "Mobile banking adoption: Application of diffusion of innovation theory." Journal of Electronic Commerce Research **13**(4): 379-391.

Al-Munajjid, M. "Islam Question and Answer." Retrieved Accessed: 25/2/2016, from http://islamqa.info/en/1497.

Al-Qaradawi, Y. "The Voice of a Woman in Islam." Retrieved Accessed: 25/2/2016, from http://www.islam101.com/women/qaradawi.html.

Al-Rasheed, M. (2007). Contesting the Saudi state : Islamic voices from a new generation, Cambridge University Press.

Al-Somali, S., B. Ghlami and B. Clegg (2009). "An investigation into the acceptance of online banking in Saudi Arabia." Technovation **29**: 130–141.

Al-Subaihi, A. (2008). "Comparison of Web and Telephone Survey Response Rates in Saudi Arabia." The Electronic Journal of Business Research Methods **6**(2): 123 - 132.

Al-Suhaimi, J. (2001). Consolidation, competition, foreign presence and systemic stability in the Saudi banking industry. The banking industry in the emerging market economies: competition, consolidation and systemic stability. Basel, Switzerland.

Al-Turki, S. (1987). Al-Mar'ah fi al-Saudiyah The woman in Saudi Arabia, London: Highlight Publications.

Alahli Bank. ""Contactless Payment"." from https://www.alahli.com/en-us/personal-banking/credit-cards/Pages/Overview.aspx.

Alahli Bank. ""Urgent Cash"." from http://www.alahli.com/en-us/personal-banking/banking-and-e-services/Pages/AlahliMobile.aspx -EmergencyCashWithdrawal.

Alam, A., O. Malik, N. Hadi and K. Gaadar (2016). "Barriers of Online Shopping in Developing Countries: Case Study of Saudi Arabia." EUROPEAN ACADEMIC RESEARCH **III**(12).

Alamri, J. (2012). An analysis of the influence of cultural backgrounds of individuals upon their perspective towards privacy within internet activities. Doctor of Philosophy, De Montfort University.

Alarabiya News. ""National ID Card as Bank Card"." from Thesis- Corrections 1 f.docx.

Alashban, A. and M. Burney (2001). "Customer adoption of tele-banking technology: the case of Saudi Arabia." International Journal of Bank Marketing **19**(5): 191-200.

Alaszewski, A. (2006). Using Diaries for Social Research. London, Sage Publications.

AlBawaba (2010). Shrinking family size to help Saudi housing sector, Al Bawaba (Middle East) Ltd., Saudi Economic Survey.

Algarni, A. (2013). "Policing internet fraud in saudi arabia: expressive gestures or adaptive strategies?" Policing and Society: An International Journal of Research and Policy **23**(4): 498–515.

Alhossaini, K. (2011). Procedural protection of the check in the Saudi Criminal Procedure Law. Master, Naif Arab University for Security Sciences.

Alinma Bank. "Urgent Cash." from https://www.alinma.com/wps/portal/alinma/Alinma/MenuPages/RetailServices/SelfServiceBanking/AlinmaAppForSmartDevices/!ut/p/z1/04_Sj9CPykssy0xPLMnMz0vMAfIjo8ziff0tTTy8TQy9DYItHA0cHd0DzHwtjYwN3Az0w1EVWLiaGRs4ega6mzgGhhm4h5jpR1Gi34AI_VGoStzNnFyAJvgZGJj6-Rm6mxiiK8DiRLwKDDAV-HuBrDD3DQ7wdzTyNzSFKjDAARwN9AtyQyMMMj0zAWAMMwE!/dz/d5/L0lDUmlTUSEhL3dHa0FKRnNBLzROV3FpQSEhL2Vu/.

AlKaabi, A. (2014). STRATEGIC FRAMEWORK TO MINIMISE INFORMATION SECURITY RISKS IN THE UAE. PhD, University of Bedfordshire.

AlKaabi, A. and C. Maple (2012). Cultural Impact on Information Security: The Case of Arab Culture. IADIS International Conference e-Society.

Alkaabi, A. and C. Maple (2013). "Cultural impact on user authentication systems." Int. J. Business Continuity and Risk Management **4**(4): 323-343.

Alkhaldi, A. (2016). "ADOPTION OF MOBILE BANKING IN SAUDI ARABIA: AN EMPIRICAL EVALUATION STUDY." International Journal of Managing Information Technology (IJMIT) **8**(2).

AlLily, A. (2011). "On line and under veil: Technology-facilitated communication and Saudi female experience within academia." Technology in Society **33**(1--2): 119 - 127.

Almogbil, A. (2005). Security, Perceptions, and Practices: challenges facing Adoption of Online Banking in Saudi Unpublished Ph.D.Thesis, George Washington University.

Almunajjed, M. (1997). Women in Saudi Arabia Today, London: Macmillan.

Alosaimi, F. (2009). "The Islamic plan to ensure the basic needs of each individual (Arabic resource)." King Saudi University.

AlRiyadh newspaper. (December 2014). ""Urgent Cash"." from http://www.alriyadh.com/999710.

Alsharif, F., F. Siewe, C. Fidler and G. Bella (2013). "The On-line Shopping Consumption Patterns of Saudi Shoppers." International Journal of Computer and Communication Engineering **2**(4).

Anthony, B. (2005). "Tribes and Tribulations: Bedouin Losses in the Saudi and Iraqi Struggles over Kuwait's Frontiers." {British Journal of Middle Eastern Studies **32**(2).

Anthony, B. (2006). Last Battles of the Bedouin and the Rise of Modem States in Northern Arabia, 1850- 1950. Nomadic Societies in the Middle East and North Africa: Entering the 21st Century. D. Chatty, Brill**:** 49--77.

Arab Monetary Fund (1991). Al-Taqrir al-Iqtisadi al-Arabi al-Muwahhad 1990 (Unified Arab Economic Report). Abu Dhabi**:** 223.

Arab News. (2014). "Transgender surgery procedure set forth." from http://www.arabnews.com/news/564451.

Arebi, S. (1994). Women and words in Saudi Arabia: the politics of literary discourse, New York: Columbia University Press.

Baki, R. (2004). "Gender-segregated Education in Saudi Arabia: Its Impact on Social Norms the Saudi Labor Market." Education Policy Analysis Archives **12**.

Barclays. (2017). "About the PINsentry card reader." Retrieved 15/1/2017, from http://www.bank.barclays.co.uk/Helpsupport/AboutthePINsentrycardreader/P1242560253440.

Barr, T., A. Knowles and S. Moore (2004). Taking users up the value chain: Australian Internet research. Melbourne, Smart Internet Technology Cooperative Research Centre**:** 89.

Barrett, M. (1997). "Playing the right paradigm." Bank Marketing **29**(9): 32.

Basel Committee (2003). Basel committee on banking supervision.

Bearak, M. and D. Cameron. (2016). "Here are the 10 countries where homosexuality may be punished by death." The Washington Post, , from https://www.washingtonpost.com/news/worldviews/wp/2016/06/13/here-are-the-10-countries-where-homosexuality-may-be-punished-by-death-2/.

Bender, D. (1967). "A Refinement of the Concept of Household: Families, Co-Residence, and Domestic Functions." American Anthropologist **69**: 493--504.

Bender, D. (1971). "De Facto Families and De Jure Households in Ondo." American Anthropologist **73**(1): 223--241.

BIS (2012). Payment, clearing and settlement systems in Saudi Arabia, Bank for International Settlements.

Bishop, M. (2005). Psychological acceptability revisited. Security and Usability: Designing Secure Systems that People Can Use. L. F. Cranor and S. Garfinkel, O'Reilly**:** 1--11.

Bloor, M., J. Frankland, M. Thomas and K. Robson (2001). Focus groups in social research. London, SAGE.

Bogdanovic, D., M. Dowd, E. Wattam and A. Adam (2010). "Contesting Methodologies: evaluating focus group and privacy diary methods in a study of on-line privacy." Journal of Information, Communication and Ethics in Society **10**(4): 208-221.

Bohannan, P. (1963). Social Anthropology, Holt, Rinehart & Winston.

Bollier, D. (1996). The future of electronic commerce: A report of the Fourth Annual Aspen Institute Roundtable on Information Technology. Aspen, Colorado, Aspen Institute.

Bonne, K., I. Vermeir, F. Bergeaud-Blackler and W. Verbeke (2007). "Determinants of halal meat consumption in France." British Food Journal **109**(5): 367-386.

Boyd, D. (2009). E-Payments: Cardholder Privacy and Non-Repudiation. PhD, Royal Holloway, University of London.

Braeuer, J., B. Gmeiner and J. Sametinger (2015). ATM Security A Case Study of a Logical Risk Assessment. ICSEA 2015 : The Tenth International Conference on Software Engineering Advances**:** 355-362.

Brown, I., Z. Cajee, D. Davies and S. Stroebel (2003). "Cell phone banking: predictors of adoption in South Africa—an exploratory study." International Journal of Information Management **23**: 381–394.

Buchler, I. and H. Selby (1968). Kinship and social organization: an introduction to theory and method, Macmillan.

Butler, J. (2011). Gender trouble: Feminism and the subversion of identity, routledge.

Calisir, F. and C. Gumussoy (2008). "Internet banking versus other banking channels: Young consumers' view." International Journal of Information Management **28**: 215–221.

Carroll, J. M. and R. Campbell (1989). "Artifacts as Psychological Theories: the Case of Human-Computer Interaction." Behaviour and Information Technology in Society **8**(4): 247-256.

Champion, D. (2003). The Paradoxical Kingdom: Saudi Arabia and the Momentum of Reform, New York: Columbia University Press.

Chan, R. (1997). "Demographic and attitudinal differences between active and inactive cardholders - the case of Hong Kong." International Journal of Bank Marketing **15**(4): 117-125.

Charmaz, K. (2006). Constructing grounded theory : a practical guide through qualitative analysis, Sage Publications.

Cherns, A. (1987). "Principles of Sociotechnical Design Revisited. ." Human Relations **40**(3).

Cohen, J. (2011). "Migration, Remittances, and Household Strategies." Annual Review of Anthropology **40**: 103--114.

Cohen, M. (1976). House United, House Divided: The Chinese Family in Taiwan, Columbia University Press.

Cole, D. (1975). Nomad of the Nomads: The Al Murrah Bedouin of the Empty Quarte, Chicago: Aldine Publishing Co.

Cole, D. (2010). Bedouins of the Empty Quarter, New Jersey: Aldine Transaction.

Cole, D. and S. Altorki (1989). Arabian oasis city : the transformation of 'Unayzah, University of Texas Press.

Coles-Kemp, L., A. Angus and F. Stang (2013). Letting go: working with the rhythm of participants. CHI '13 Extended Abstracts on Human Factors in Computing Systems. Paris, France, ACM 373-378.

Coles-Kemp, L. and D. Ashenden (2012). Community-centric engagement: lessons learned from privacy awareness intervention design. Proceedings of BCS HCI 2012 Workshops: Designing Interactive Secure Systems.

Coles-Kemp, L. and A. Kotova (2014). Sticking And Making: Technology As Glue For Families Separated By Prison. UK Academy for Information Systems Conference Proceedings 2014.

Corbin, J. M. and A. Strauss (2008). Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory. Los Angeles, [Calif.] ; London, SAGE.

Cotula, L. (2002). Gender and Law: Women's Rights in Agriculture, FAO Legislative Study No. 76, (revised 2007),. Rome, FAO (Food and Agriculture Organization) Legal Office (2002 [2007]).

Cranor, L. F. and S. Garfinkel (2005). Preface. Security and Usability: Designing Secure Systems that People Can Use. L. F. Cranor and S. Garfinkel. Sebastopol, CA, O'Reilly**:** ix-xviii.

D'Hertefelt, S. (2000). Trust and the perception of security.

Dallos, C. (2003). Identity and opportunity: asymmetrical household integration among the Lanoh, newly sedentary hunter-gatherers and forest collectors of Peninsular Malaysia. PhD, McGill University.

Deave, S. (1980). The contemporary Saudi women. A world of women: anthropological studies of women in the societies of the world. Bourguignon (and contributors) E, New York: Praeger.

Deif, F. (2008). "Perpetual minors: human rights abuses stemming from male guardianship and sex segregation in Saudi Arabia. London: Human Rights Watch.", from http://www.hrw.org/sites/default/files/reports/saudiarabia0408webwcover.pdf.

Del Castillo, D. (2003). "Teaching through an electronic veil." The Chronicle of Higher Education **49**(29).

Denscombe, M. (2007). The Good Research Guide, McGraw-Hill Education.

Devlin, J. (1995). "Technology and innovation in retail banking distribution." International Journal of Bank Marketing **13**(4): 19-25.

Dhamija, R. and A. Perrig (2000). Déjà Vu: A User Study Using Images for Authentication. 9th USENIX Security Symposium, Denver, Colorado, USA.

Dialsingh, I. (2008). Face-to-Face Interviewing. Encyclopedia of Survey Research Methods. P. Lavrakas, SAGE.

Dix, A. J., J. E. Finlay, G. D. Abowd and R. Beale (1998). Human-Computer Interaction, Hemel Hempstead: Prentice Hall Europe.

Dorst, K. (2015). Frame Innovation : Create New Thinking by Design, MIT Press, Cambridge, Mass.

Dourish, P., E. Grinter, J. Delgado de la Flor and M. Joseph (2004). "Security in the Wild: User Strategies for Managing Security As an Everyday, Practical Problem." Personal Ubiquitous Computer **8**(6): 391-401.

Dourish, P. and D. Redmiles (2002). An Approach to Usability Security Based on Event Monitoring and Visualization. New Security Paradigms Workshop, Virginia Beach, VA.

Dunne, D. and R. Martin (2006). "Design Thinking and How It Will Change Management Education: An Interview and Discussion." Academy of Management Learning & Education **5**(4): 512 - 523.

Eid, M. (2011). "Determinants of E-Commerce Customer Satisfaction, Trust, and Loyalty in Saudi Arabia." Journal of Electronic Commerce Research **12**(1).

Entendahod, I. (2015). "How woman can use her money." Al-Madinah Hadith Studies|.

Equaldex. (2016). "1932 in LGBT Rights." from http://www.equaldex.com/timeline/1932.

Eunus Ali, M., S. Rishta, L. Ansari, T. Hashem and A. Khan (2015). SafeStreet: empowering women against street harassment using a privacy-aware location based application. Seventh International Conference on Information and Communication Technologies and Development, Singapore.

Filotto, U., P. Tanzi and F. Saita (1997). "Customer needs and front-office technology adoption." International Journal of Bank Marketing **15**(1): 13-21.

Finextra. (2009). "Court sides with Halifax in chip card clone case." Retrieved 24/4/2017, from https://www.finextra.com/newsarticle/20102/court-sides-with-halifax-in-chip-card-clone-case.

Fornell, C. and B. Wernerfelt (1987). "Defensive marketing strategy by customer complaint management: a theoretical analysis." Journal of Marketing Research **24**: 337-346.

Friedman, B. and E. Felten (2002). Informed Consent in the Mozilla Browser: Implementing Value-Sensitive Design Thirty-Fifth Annual Hawaii International Conference on System Sciences.

Friedman, B. and J. Grudin (1998). Trust and Accountability: Preserving Human Values in Interactional Experience. CHI '98, ACM.

Gallagher, E. and C. Searle (1985). "Health services and the political culture of Saudi Arabia." Social Science & Medicine **21**(3).

Garnaeva, M., J. van der Wiel, D. Makrushin, A. Ivanov and Y. Namestnikov (2015). Kaspersky Security Bulletin: overall statistics for 2015.

Gaw S and F. EW. (2006). Password management strategies for online accounts. Symposium on Usable Privacy and Security (SOUPS'06). Pennsylvania, USA**:** 44-45.

General Authority of Statistics (2015). Statistics of Students by Sex and level of Education.

General Authority of Statistics (2016). Gross Domestic Product Per Capita.

Gillham, B. (2005). Research interviewing: the range of techniques. Maidenhead ; New York, Open University Press.

Glaser, B. (1978a). Advances in The Methodology of Grounded Theory. Mill Valley, CA, Sociology Press.

Glaser, B. (1978b). Theoretical sensitivity : advances in the methodology of grounded theory. Mill Valley, Calif Sociology Press.

Glaser, B. (1992). Basics Of Grounded Theory Analysis, Emergence vs. Forcing. Mill Valley, CA, Sociology Press.

Glaser, B. (1998). Doing Grounded Theory: Issues and Discussions. Mill Valley, CA, Sociology Press.

Glaser, B. and A. Strauss (1967). The Discovery of Grounded Theory: Strategies for Qualitative Research, Aldine.

Glesne, C. and A. Peshkin (1992). Becoming qualitative researchers: an introduction, Longman.

Goldberg, J. (2011). "Two thirds of web users re-use the same passwords." AgileBits Blog.

Gunson, N., D. Marshall, H. Morton and M. Jack (2011). "User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking." Computers & Security **30**(4): 208-220.

Hamdan, A. (2005). "Women and education in saudi arabia: Challenges and achievements." International Education Journal **6**(1).

Hammel, E. A. and P. Laslett (1974). Comparing Household Structure Over Time and Between Cultures.

Haron, S. (1997). Islamic banking : rules and regulations. Petaling Jaya, Selangor Pelanduk Publications.

Hilden, J. T. (2011). Bedouin weaving : of Saudi Arabia & its neighbours, London : Arabian.

Hofstede, G. (2003). Geert Hofstede Culture Dimensions.

Holt, A. (2010). "Using the telephone for narrative interviewing: a research note." Qualitative Research **10**(1): 113-121.

Howcroft, B., R. Hamilton and P. Hewer (2002). "Consumer attitude and the usage and adoption of home-based banking in the United Kingdom." The International Journal of Bank Marketing **20**(3): 111–121.

Hsiao, R.-L. (2003). "Technology fears: distrust and cultural persistence in electronic marketplace adoption." The Journal of Strategic Information Systems **12**(3): 169-199.

Hunt, T. (2012). "What do Sony and Yahoo! have in common? Passwords?" Troy Hunt Blog.

Huyette, S. (1985). Political Adaptation in Saudi Arabia: A Study of the Council of Ministry., Colorado: Westview Press.

Inglesant, P. and M. A. Sasse (2010a). The true cost of unusable password policies: password use in the wild. CHI '10, Atlanta, Georgia, USA, ACM.

Inglesant, P. and M. A. Sasse (2010b). Studying Password Use in the Wild: Practical Problems and Possible Solutions. SOUPS '10, Redmond, WA, USA.

International Constitutional Law. (2005). "Article 1: Saudi Arabian constitution." Retrieved 05/02/2015, from http://www.servat.unibe.ch/icl/sa00000_.html.

International Monetary Fund (2013). Saudi Arabia: Financial Sector Assessment Program Update, Detailed Assessment of Observance of the CPSS Core Principles for Systemically Important Payment Systems.

Irvine, A. (2010). "Using phone interviews." from http://www.socialsciences.manchester.ac.uk/morgancentre/realities/toolkits/phone-interviews/14-toolkit-phone-interviews.pdf.

Jagatic, T., N. Johnson, M. Jakobsson and F. Menczer (2007). "Social Phishing." Commun. ACM **50**(10): 94–100.

Jain, A. K. and K. Nandakumar (2012). "Biometric Authentication: System Security and User Privacy." Computer **45**(11): 87-92.

Jamjoom, M. (2009). "Female Islamic studies teachers in Saudi Arabia: a phenomenological study." Teaching and Teacher Education **26**(3): 547-558.

Jarvenpaa, S., K. R. Lang, Y. Takeda and V. K. Tuunainen (2003). "Mobile commerce at crossroads: an international focus group study of users of mobile handheld devices and services." Communications, ACM **46**(12): 41-44.

Jerichow, A. (1998). The Saudi File, New York: St. Martin's Press.

Johnston, R. and S. Mehra (2002). "Best-practice complaint management." Academy of Management Journal **16**(4): 145-154.

Ka-Ping, Y. (2002). User Interaction Design for Secure Systems. 4th International Conference on Information and Communications Security, Springer-Verlag.

Kamali, M. (1999). Law and society: The interplay of revelation and reason in the shari'ah. The Oxford history of Islam. e. Esposito, Oxford University Press.

Kanniainen, L. (2010). "Alternatives for banks to offer secure mobile payments." International Journal of Bank Marketing **28**(5): 433-444.

Karat, C.-M., J. Karat and C. Brodie (2005). "Why HCI research in privacy and security is critical now." International Journal of Human-Computer Studies **63**(1-2): 1-4.

Karat, J. (1988). Software evaluation Methodologies. Handbook of human computer interaction. Helander M. Amsterdam, North-Holland**:** 891-903.

Kaye, J. J. (2011). Self-reported Password Sharing Strategies. the SIGCHI Conference on Human Factors in Computing Systems, CHI '11. Vancouver, BC, Canada, ACM, New York, NY, USA**:** 2619--2622.

Kelly, M. J. (2008). The SAGE Encyclopedia of Qualitative Research Methods. Thousand Oaks Thousand Oaks, California, SAGE Publications, Inc.

Kent, S. T. and L. I. Millett (2003). Who Goes There?: Authentication Technologies Through the Lens of Privacy, National Academies Press.

Khraim, H. (2010). "Measuring religiosity in consumer research from Islamic perspective." International Journal of Marketing Studies **2**(2): 166-179.

Kieckhaefer, J. M., J. P. Vallano and N. Schreiber Compo (2014). "Examining the positive effects of rapport building: When and why does rapport building benefit adult eyewitness memory?" Memory **22**(8): 1010-1023.

Kitzinger, J. (1995). "Qualitative Research: Introducing focus groups." BMJ **311**(7000): 299-302.

Kitzinger, J. and R. Barbour (1998). Developing Focus Group Research: Politics, Theory and Practice, SAGE Publications.

Koocher, G. P. (2009). " Ethics and the Invisible Psychologist." Psychological Services **6**(2): 97–107.

Krimly, R. (1999). "The Political Economy of Adjusted Priorities: Declining Oil Revenues and Saudi Fiscal Policies." Middle East Journal **53**(2): 254-267.

KSA Transition to Knowledge Society (2014). KSA Transition to Knowledge Society.

Kumaraguru, P., S. Sheng, A. Acquisti, L. Cranor and J. Hong (2010). "Teaching Johnny Not to Fall for Phish." ACM Trans. Internet Technol. **10**(2): 7-31.

Lapidus, I. M. (1973). "The Evolution of the Muslim Urban Society." CONTEMPORARY STUDIES IN SOCIAL HISTORY: 21-50.

Lassar, W., C. Manolis and S. Lassar (2005). "The relationship between consumer innovativeness, personal characteristics, and online banking adoption." International Journal of Bank Marketing **23**(2): 176 – 199.

Laukkanen, T. (2007). "Internet vs mobile banking: comparing customer value perceptions." Business Process Management Journal **13**(6): 788-797.

Lee, F. (2011). "Modeling the Economy as a Whole: An Integrative Approach." American Journal of Economics and Sociology **70**(5): 103--114.

Lee, J. and A. Allaway (2002). "Effects of personal control on adoption of self-service technology innovations." Journal of Services Marketing **16**(6): 553-572.

Leeuwen, J., D. Rijken, L. Bloothoofd, E. Cobussen, B. Reurings and R. Ruts (2016). Thematic Research in the Frame Creation Process. Fifth Service Design and Innovation conference.

Lipsky, G. (1959). Saudi Arabia: its people, its society, its culture, New Haven: Hraf Press.

Liu, C., J. T. Marchewka, J. Lu and C.-S. Yu (2005). "Beyond concern: a privacy-trust-behavioral intention model of electronic commerce." Information & Management **42**(1): 127-142.

Long, S. (2013). Socioanalytic Methods: Discovering the Hidden in Organisations and Social Systems, Karnac Books.

Luhmann, N. (1988). Familiarity, confidence, trust: problems and alternatives. Trust: Making and Breaking Cooperative Relations. D. Gambetta. New York, Basil Blackwell**:** 94-107.

Lunt, P. and S. Livingstone (1996). "Rethinking the focus group in media and communications-research." Journal of Communications. **46**(2): 79-98.

Mackey, S. (2002). The Saudis: Inside the Desert Kingdom, London: Norton.

Madar Research Group (2014). Saudi Arabia Transition to Knowledge Society 2014.

Majlis Ash-Shura. (2015). "Royal Speeches." Retrieved 27/01/2015, from http://www.shura.gov.sa/wps/wcm/connect/ShuraArabic/internet/Home/.

Marcus, A. and E. W. Gould (2000). "Crosscurrents: cultural dimensions and global Web user-interface design." Interactions **7**(4): 32–46.

Marr, N. and G. Prendergast (1991). "human tellers: who needs tehm?" International Journal of Bank Marketing **8**(2): 32-39.

Marshall, J. and L. Heslop (1988). "Technology acceptance in Canadian retail banking: a study of consumer motivation and use of ATMs." International Journal of Bank Marketing **6**(4): 31-41.

Martin, P. Y. and B. A. Turner (1986). "Grounded Theory and Organizational Research." The Journal of Applied Behavioural Science **22**(2): 141- 157.

Martins, J. (2007). "Household Budgets as a Social Indicator of Poverty and Inequality in South Africa." Social Indicators Research **81**: 203--221.

Mathiasen, N. R. and S. Bodker (2011). Experiencing Security in Interaction Design. SIGCHI Conference on Human Factors in Computing Systems, CHI '11, Vancouver, BC, Canada, ACM, New York, NY, USA.

McKinsey Global Institute (2015). The Power of Parity: How Advacing Women's Equality can Add $12 Trillion to Global Growth., McKinsey Global Institute,.

Meidan, A. (1996). Marketing Financial Services. London, Macmillan.

Meier, J. D., A. Mackman, M. Dunner, S. Vasireddy, R. Escamilla and A. Murukan. (2003a). "Chater 2: Threats and Countermeasures." Improving Web Application Security: Threats and Countermeasures Retrieved 4/4/2017, from http://msdn.microsoft.com/en-us/library/aa302419.aspx - c03618429_011.

Meier, J. D., A. Mackman, M. Dunner, S. Vasireddy, R. Escamilla and A. Murukan. (2003b). "Chater 3: Threat Modeling." Improving Web Application Security: Threats and Countermeasures Retrieved 4/4/2017, from http://msdn.microsoft.com/en-us/library/aa302419.aspx - c03618429_011.

Ministry of Higher Education. (2012). "Higher Education Indicators in Saudi Arabia 2011." Retrieved 03/02/2015, from http://www.mohe.gov.sa/ar/docs/Doc1/VDMPI022.pdf.

Mirza, A. (2008). "Students perceived barriers to in-class participation in a distributed and gender segregated educational environment." The Electronic Journal of Information Systems in Developing Countries **35**(7): 1--7.

Moaddel, M. (2006). "THE SAUDI PUBLIC SPEAKS: RELIGION, GENDER, AND POLITICS." International Journal of Middle East Studies **38**(01): 79--108.

Möckel, C. and A. Abdallah (2010). Threat Modeling Approaches and Tols for Securing Architectural Designs of an E-banking Application. Sixth International Conference on Information Assurance and Security.

Moftah, L. (2015). "'Gay Parties' Raided In Saudi Arabia; Religious Police Arrest Several People On Suspicion Of Homosexuality." International Business Times, , from http://www.ibtimes.com/gay-parties-raided-saudi-arabia-religious-police-arrest-several-people-suspicion-1968038.

Mokhlis, S. (2006). "The effect of religiosity on shopping orientation: an exploratory study in Malaysia." Journal of American Academy of Business **9**(1): 64-74.

Morgan, D. L. (1998). Planning Focus Groups, Thousand Oake.

Morgan, M. (1996). "Qualitative research: a package deal?" The Psychologist **9**(1): 31-32.

Norman, D. A. (1998). The Invisible Computer. Cambridge, Mass, MIT Press.

Obeidat, B. Y., R. O. Shannak and I. M. Al-Jarrah (2012). "Toward better understanding for Arabian culture: implications based on Hofstede's cultural model." European Journal of Social Sciences **28**(4): 512–522.

Olson, J. S., J. Grudin and E. Horvitz (2005). A Study of Preferences for Sharing and Privacy. CHI EA '05, Portland, OR, USA, ACM.

Oruh, J. (2014). "Three-Factor Authentication for Automated Teller Machine System." International Journal of Computer Science and Information Technology & Security (IJCSITS) **4**(6).

Palen, L. and P. Dourish (2003). Unpacking "privacy" for a networked world. Human factors in computing systems, Florida, USA, ACM Press.

Palen, L. and M. Salzman (2002). Voice-mail diary studies for naturalistic data capture under mobile conditions. ACM conference on Computer supported cooperative work. New Orleans, USA, ACM.

Peak, M. H. (1997). "Back to the future of phones." Management Review **86**(6): 9.

Peevers, G., G. Douglas, D. Marshall and M. Jack (2011). "On the role of SMS for transaction confirmation with IVR telephone banking." International Journal of Bank Marketing **29**(3).

Pew Research Center. (2009). "Mapping the Global Muslim Population." Retrieved Accessed: 25/2/2016, from http://www.pewforum.org/files/2009/10/Muslimpopulation.pdf.

Prasath, V. (2010). "Modeling the Evaluation Criteria for Security Patterns in Web Service Discovery." International Journal of Computer Applications **1**: 53-60.

Preece, J., Y. Rogers, H. Sharp, D. Benyon, S. Holland and T. Carey (1994). Human-Computer Interaction, Harlow : Addison-Wesley.

Puchta, C. and J. Potter (2004). Focus group practice. London, SAGE

Ranjan, R. (2000). "Poverty and expenditure pattern of households in Pakistan and South Africa: a comparative study." Journal of International Development **12**(2): 241--254.

Renaud, K. (2004). "Quantifying the quality of web authentication mechanisms: a usability perspective." Journal of Web Engineering **3**: 95-123.

Renaud, K. (2005). Evaluating authentication mechanisms. Security and Usability: Designing Secure Systems that People Can Use. L. F. Cranor and S. Garfinkel. Sebastopol, CA, O'Reilly**:** 103-128.

Rieman, J. (1993). The Diary Study: A Workplace-Oriented Research Tool to Guide Laboratory Efforts. INTERACT '93 and CHI '93 Conference on Human Factors in Computing Systems, New York, ACM.

Riyad Bank. ""Contactless Payment"." from https://www.riyadbank.com/en/personal-banking/debit-card.

Rubin, H. and I. Rubin (1995). Qualitative Interviewing: The Art of Hearing Data, SAGE.

Saldana, J. (2011). The Coding Manual for Qualitative Researchers, Sage Publications, London & Thousand Oaks, California. .

SAMA. (2010). "Saudi Arabian Monetary Agency, Electronic Banking Rules." Retrieved Accessed: 25/2/2017, from http://www.sama.gov.sa/RulesRegulation/Rules/Pages/E_banking_Rules.pdf.

SAMA. (2012). "Saudi Arabian Monetary Agency, Rules Governing the Opening of Bank Accounts & General Operational Guidelines in Saudi Arabia." 16/9/2016, from http://www.sama.gov.sa/en-US/Laws/BankingRules/Rules_Governing_the_Opening_of_Bank_Accounts_ver4.pdf.

SAMA. (2013). "Saudi Arabian Monetary Agency, Consumer Protection Principles." Retrieved Accessed: 25/2/2017, from http://www.sama.gov.sa/RulesRegulationsandCirculars/ConsumerProtection/Documents/ConsumerProtection.pdf.

Sasse, M. A., S. Brostoff and D. Weirich (2001). "Transforming the 'weakest link': a human-computer interaction approach to
usable and effective security." BT Technical Journal **19**: 122-131.

Sasse, M. A. and I. Flechais (2005). Usable security: Why do we need it? How do we get it? Security and Usability: Designing Secure Systems that People Can Use. L. F. Cranor and S. Garfinkel, O'Reilly**:** 13--30.

Sathye, M. (1999). "Adoption of internet banking by Australian consumer: an empirical investigation." International Journal of Bank Marketing **17**(7): 324–334.

Saudi Arabia Ministry of Labor. (2015). "The Labor Code (Arabic resource)." Retrieved 17/6/2017, from https://portal.mol.gov.sa/ar/ProgramsAndInitiatives/Pages/%D9%86%D8%B8%D8%A7%D9%85%D8%A7%D9%84%D8%B9%D9%85%D9%84%D8%A7%D9%84%D8%AC%D8%AF%D9%8A%D8%AF%D8%A7%D9%84%D9%86%D8%B3%D8%AE%D8%A9%D8%A7%D9%84%D9%85%D8%B9%D8%AA%D9%85%D8%AF%D8%A9_v3.0.pdf.

Saudi Arabian Monetary Agency (1999). Development and restructuring of the Saudi banking system. BANK RESTRUCTURING IN PRACTICE. Basel, Switzerland, Bank for International Settlements Information, Press & Library Services**:** 183-196.

Saudi Hollandi Bank. "History." Retrieved Accessed: 25/2/2016, from http://shb.com.sa/en/about/AboutSHB/History.aspx.

Saudi Vision (2016). Saudi Vision 2030.

Schneier, B. (1996). Applied Cryptography. New York, John Wiley & Sons.

Schneier, B. (2000). Secrets and lies: Digital security in a networked world. New York, John Wiley & Sons.

Schneier, B. and A. Shostack (1999). Breaking Up Is Hard to Do: Modeling Security Threats for Smart Cards. USENIX Workshop on Smart Card Technology, USENIX Press**:** 175-185.

Scott, J. (2006). DIARY. The SAGE Dictionary of Social Research Methods. V. Jupp. London, SAGE.

Shaari, J. A. N. and N. S. M. Afirin (2010). "Dimension of halal purchase intention: a preliminary
study." International Review of Business Research Papers **6**(4): 444-456.

Sieger, H. and S. Moller (2012). Gender Differences in the Perception of Security of Mobile Phones. MobileHCI'12. San Francisco, USA.

Singh, S. (1997). Marriage Money: The Social Shaping of Money in Marriage and Banking. Studies in society, Allen & Unwin.

Singh, S. (2006). "The Social Dimensions of the Security of Internet banking." JTAER **1**(2): 72-78.

Singh, S. (2008). "Secure shared passwords: The social and cultural centered design of banking." journal of financial transformation **23**: 110-114.

Singh, S., A. Cabraal, C. Demosthenous, G. Astbrink and M. Furlong (2007a). Password sharing: implications for security design based on social practice. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, San Jose, California, USA, ACM.

Singh, S., A. Cabraal, C. Demosthenous, G. Astbrink and M. Furlong (2007b). Security design based on social and cultural practice: Sharing of passwords. HCI International Conference on Usability and Inter- nationalization, UI-HCII '07, SpringerLink**:** 476–485.

Singh, S., A. Cabraal, C. Demosthenous, G. Astbrink and M. Furlong (2007b). Security Design Based on Social and Cultural Practice: Sharing of Passwords. Proceedings of the HCI International Conference on Usability and Internationalization, Beijing, China, SpringerLink.

Singh, S., A. Cabraal and G. Hermansson (2006). What is your husband's name?: sociological dimensions of internet banking authentication, Sydney, Australia, ACM.

Singh, S. and K. Cassar-Bartolo (2004). The privacy of money and health. OZCHI. Wollongong.

Singh, S., M. Jackson, J. Beekhuyzen and A. Cabraal (2006). The Bank and I: Privacy, Banking and Life Stage. CHI 2006 Workshop on Privacy-Enhanced Personalization, National Science Foundation.

Singh, S. and C. Slegers (1997). Trust and electronic money. Melbourne, Centre for International Research on Communication and Information Technologies.

Sjoberg, L. E. (2009). Gender and international security: feminist perspectives, Routledge.

Sloman, M. (1994). "Policy Driven Management for Distributed Systems." Journal of Network and Systems Management **2**(4): 333-360.

Smith, W. R. (1903). KINSHIP AND MARRIAGE IN EARLY ARABIA, London: Adams and Chas. Black.

Snowden, M. (2015). "Use of diaries in research." Nursing Standard **29**(44): 36-41.

Sohail, M. and I. Al-Jabri (2014). "Attitudes towards mobile banking: are there any differences between users and non-users?" Behaviour & Information Technology **33**(4): 335–344.

Souiden, N. and M. Rani (2015). "Consumer attitudes and purchase intentions toward Islamic banks: the influence of religiosity." International Journal of Bank Marketing **33**(2): 143-161.

SPA, S. P. A. (2015). "Royal Speeches 2013." Retrieved 72/01/2015, from http://www.spa.gov.sa/awamer.php?pg=4&lite=.

Statista. (2016). "Number of smartphone users in Saudi Arabia from 2014 to 2021." Retrieved 8/1/2017, from https://www.statista.com/statistics/494616/smartphone-users-in-saudi-arabia/.

Statista. (2017). "Saudi Arabia: Average age of the population from 1950 to 2050 (median age in years)." from https://www.statista.com/statistics/262482/median-age-of-the-population-in-saudi-arabia/.

Strauss, A. and J. Corbin (1990). Basics of qualitative research: grounded theory procedures and techniques. Newbury Park, Sage.

Strauss, A. and J. M. Corbin (1998). Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory, SAGA Publications.

Sundarraj, R. and J. Wu (2005). "Using information-systems constructs to study online- and telephone-banking technologies." Electronic Commerce Research and Applications **4**(4): 427-443.

Thakefni. (2016). "Requiring intermediate and high schoolgirls issuing of national ID card." from http://www.thaqfny.com/97524/%D8%A7%D8%B3%D8%AA%D8%AE%D8%B1%D8%A7%D8%AC-%D8%A8%D8%B7%D8%A7%D9%82%D8%A9-%D8%A7%D9%84%D9%87%D9%88%D9%8A%D8%A9-%D8%A7%D9%84%D9%88%D8%B7%D9%86%D9%8A%D8%A9-%D9%84%D9%84%D8%B7%D8%A7%D9%84%D8%A8%D8%A7/.

The Saudi Investment Bank. ""Urgent Cash"." from https://www.saib.com.sa/en/content/emergency-cash-service.

The South Asian Times (2011). Saudi Arabia among Top 10 nations in terms of density of ultra-wealthy households, HT Media Ltd.

Timewell, S. (2014). "Banks start to close the gender divide in Saudi Arabia." from http://www.thebanker.com/World/Banks-start-to-close-the-gender-divide-in-Saudi-Arabia.

Tiwari, R., S. Buse and C. Herstatt (2007). Mobile services in banking sector. The role of innovative business solutions in generating competitive advantage. 8th International Research Conference on Quality, Innovation and Knowledge Management, New Delhi.

Tognazzini, B. (2005). Design for usability. Security and Usability: Designing Secure Systems that People Can Use. L. F. Cranor and S. Garfinkel, O'Reilly**:** 31-46.

UNESCO (2014). UNESCO intitute for statistics, Saudi Arabia.

Villalba, J. and E. Lleida (2010). Speaker verification performance degradation against spoofing and tampering attacks. FALA 10 workshop**:** 131–134.

Vyas, H. (2003). Sewa Bank's Savings and Credit Groups and Their Influence on Women's Financial Decision Making Within the Households, UMI.

Wajcman, J. (2010). "Feminist theories of technology." Cambridge journal of economics **34**(1): 143-152.

Wan, W., C. Luk and C. Chow (2005). "Customers' adoption of banking channels in Hong Kong." International
Journal of Bank Marketing **23**(3): 255 – 272.

Webb, P. and J. Young (2005). "Perhaps It's Time for a Fresh Approach to ICT Gender Research?" Journal of Research and Practice in Information Technology **37**(2).

Weir, C., G. Douglas, M. Carruthers and M. Jack (2009). "User perceptions of security, convenience and usability for eBanking authentication tokens." Computers and Security **28**: 47-62.

Weirich, D. and M. A. Sasse (2001). Pretty good persuasion: a first step towards effective password security in the real world. Proceedings of the 2001 workshop on New security paradigms, Cloudcroft, New Mexico, ACM.

Whitaker, B. (2016). Transgender issues in the Middle East.

Whitman, M. E. and A. B. Woszczynski (2004). The Handbook of Information Systems Research, Idea Group Pub.

Whitteker, W. (2014). Point of Sale (POS) Systems and Security, SANS Institute.

Whitworth, B. and A. Ahmad (2013). Socio-Technical System Design. The Encyclopedia of Human-Computer Interaction. M. Soegaard and R. F. Dam, Aarhus, Denmark: The Interaction Design Foundation.

Wibben, A. (2011). Feminist Security Studies: A narrative approach, Routledge.

Williamson, O. (1993). "Calculativeness, Trust, and Economic Organization." The Journal of Law & Economics **36**(1): 453-486.

Wright, M. (2002). "Patterns of purchase loyalty for retail payment methods." The International Journal of Bank Marketing **20**(7): 311-316.

Xin, T. and B. Xiaofang (2014). "Online Banking Security Analysis based on STRIDE Threat Model." International Journal of Security and Its Applications
8(2): 271-282.

Yamami, M. (1996). Feminism and Islam: Legal and Literary Perspectives., New York: New York University Press.

Yanagisako, S. (1979). "Family and Household: The Analysis of Domestic Groups." Annual Review of Anthropology **8**(5): 161--207.

Yee, K. (2004). "Aligning Security and Usability." IEEE Security and Privacy **2**(5): 48-55.

Zetter, K. (2011). More than 93,000 Sony customers affected in new breach. Wired. San Francisco, Clifornia.

Zimmerman, D. H. and D. L. Wieder (1977). "The diary: diary-interview method." Urban Life **5**(4): 479-498.

Zurko, M. E. and R. T. Simon (1997). User-Centered Security. New Security Paradigms Workshop.